Nathalie DE GROVE-VALDEYRON
Claire BORIES
Directrices scientifiques

Claire BORIES
Coordinatrice

Bulletin de l'EDiHL

European Digital Health Law

ACTUALITÉ DU DROIT EUROPÉEN DU NUMÉRIQUE EN SANTÉ

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

TROIS ANNÉES DE VEILLE SUR

DROIT DE L'UNION EUROPÉENNE

EHDS • IA en santé • Stratégie pour l'Union des données • TEHDaS 1 & 2 • Dispositifs médicaux numériques

DROITS NATIONAUX

France • Belgique • Espagne • Irlande • Italie • Suède

Télémédecine • Télésurveillance médicale • Accès aux données de santé • Dématérialisation de la carte Vitale

JURISPRUDENCE EUROPÉENNE ET NATIONALE

Protection des données à caractère personnel • Vente en ligne de médicaments • Accès au dossier médical partagé

RECUEIL DES BULLETINS DE L'EDiHL

2023-2026

Volumes 1 à 3

ÉCOLE de DROIT de TOULOUSE RECHERCHE | IRDEIC

Cofinancé par l'Union européenne

Financé par l'Union européenne.

Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables

Funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

Cofinancé par
l'Union européenne

ÉDITORIAL

Nathalie DE GROVE-VALDEYRON
Professeure de droit public
Chaire Jean Monnet (2017-2023) et (2023 - 2026)
Université Toulouse Capitole – IRDEIC

Le bulletin de la Chaire EDiHL (*European Digital Health Law*) est un des livrables de la Chaire Jean Monnet en droit européen du numérique en santé de Nathalie De Grove Valdeyron dont le site est hébergé par l'Université Toulouse Capitole, et en son sein, par l'IRDEIC (Institut de recherche en droit européen, international et comparé). L'objet de ce bulletin est d'accompagner la construction de cette discipline naissante (non enseignée en tant que telle lors de l'attribution de la chaire en France), au cours des 3 années de la chaire (2023-2026). Il est en réalité formé de 3 bulletins réalisés annuellement, et qui ont, pour chacun d'entre eux, fait l'objet d'une parution distincte sur le site de la chaire EDIHL. Il s'agit concrètement de retracer l'évolution majeure intervenue au cours de ces trois années, dans le domaine du numérique européen en santé, sous l'angle de l'activité principalement législative, mais aussi, le cas échéant, contentieuse.

Bulletin de l'EDiHL
European Digital Health Law

Le premier bulletin, qui couvre la période juin 2023 à juin 2024, fait état des textes en cours d'adoption au niveau européen, qu'il s'agisse de textes contraignants ou non contraignants (Guidelines/lignes directrices, orientations, recommandations…). Il s'agit aussi, dès 2023, de s'intéresser aux contextes juridiques nationaux au sein desquels les textes européens adoptés, ou en cours d'adoption, devront s'intégrer. Il convient en effet de garder à l'esprit que les États restent responsables, conformément à l'article 168 §7 du TFUE, de tout ce qui relève de l'organisation de leur système de soins de santé, et que des adaptations s'avèreront nécessaires pour permettre le déploiement du numérique en santé au sein des États membres. N'oublions pas non plus que le RGPD (règlement général sur la protection des données) accorde aux États membres une marge de manœuvre dans le domaine des données de santé à l'origine d'une « fragmentation » de ces mêmes données, justifiant (entre autres motifs) l'adoption du règlement sur l'espace européen des données de santé pour y remédier. Le premier bulletin s'attache donc, notamment, à mettre en évidence certaines des difficultés qu'il s'agira de lever dans la mise en œuvre du règlement, alors à l'état de proposition, en France.

Le deuxième bulletin (période 2024-2025) couvre une période particulièrement riche caractérisée d'une part, par l'adoption du règlement sur l'Espace européen des données de santé (« EEDS », ou « EHDS » selon l'acronyme anglais) (Règlement (UE) 2025 /327) du 11 février 2025), mais aussi par l'adoption du règlement sur l'IA « AI ACT » (règlement (UE) 2024/1689 du 13 juin 2024), dont les implications dans le domaine de la santé seront également importantes, certains produits de santé (et notamment les dispositifs médicaux faisant l'objet d'une évaluation de leur conformité par un « organisme notifié ») étant soumis à l'application dudit règlement. Par ailleurs il sera désormais possible, avec la création de l'Espace européen des données de santé, de constituer de vastes bases de données auxquelles des systèmes d'IA pourront être appliqués, ce qui offre de nouvelles perspectives, notamment, dans le cadre de la recherche médicale et du développement d'une médecine de plus en plus personnalisée.

Le règlement « EEDS », et dans une certaine mesure, le Règlement IA, constituent ainsi une première

manifestation opérationnelle de l'émergence de ce nouveau droit.

Les enjeux sont immenses et les défis non moins importants comme l'a montré le colloque international organisé à Toulouse en juin 2024 et dont les actes ont été publiés « Le droit européen de la santé numérique, un droit en construction » (dir. N. DE GROVE -VALDEYRON), Bruylant, juin 2025 et « Espace européen des données de santé et IA : enjeux juridiques et défis de mise en œuvre », Presses de Toulouse, 2025 accessible en open édition.

Ce deuxième bulletin ne néglige pas la dimension nationale et des incursions en droit français, espagnol et belge sont réalisées.

Enfin, le dernier bulletin (2025-2026) témoigne, notamment par son volume (200 pages), de la place importante prise par le droit européen du numérique en santé. Ce bulletin comporte notamment l'analyse synthétique de nombreuses guidelines, encore en consultation publique, de l'action conjointe TEHDaS2, mais aussi de l'EMA ainsi que des arrêts importants sur les données de santé dont les implications pourront être significatives. Une incursion dans le droit français (principes applicables par la CNEDIMTS) et dans le droit suédois permet d'avoir une idée des différences de mode de prise en charge des dispositifs médicaux numériques. Par ailleurs une étude réalisée en droit italien et en droit irlandais montre comment ces Etats se préparent à l'intégration du numérique en santé, pour ne citer ici que quelques exemples des textes commentés.

Le bulletin de la Chaire EDIHL n'aurait pu voir le jour sans la coordination efficace, rigoureuse et extrêmement précieuse de Claire BORIES, ancienne doctorante, docteure en droit de l'Université de Toulouse, aujourd'hui en poste au Ministère de la santé. Ce bulletin lui doit beaucoup tant au niveau de la coordination scientifique que de la conception et de la réalisation matérielle. Merci infiniment Claire ! D'autres doctorants ou (anciens) doctorants ont été de fidèles contributeurs tout au long de ces trois années (Sarah, Noémie, Lisa, Valentine, Winnie…), je ne peux que les en remercier encore vivement. Enfin, ce bulletin est aussi celui des étudiants de niveau Master 1 (droit de la santé et droit du numérique IA de l'École de droit de Toulouse) mais aussi du Master 2 Juriste européen, droit international et comparé et du Master 2 Droit de la santé, qui se sont succédés au cours de ces trois années.

Ce bulletin, chers contributeurs, est le vôtre et j'espère que vous avez pris autant de plaisir à y contribuer que j'en ai pris à le concevoir, à susciter votre intérêt, et à vous lire.

Merci à tous pour votre confiance et votre participation et bonne lecture à tous ceux qui souhaitent s'informer sur les récents développements de ce droit naissant.

SOMMAIRE GÉNÉRAL

RECUEIL DES BULLETINS DE L'EDiHL

Volume 1 à 3

BULLETIN DE L'EDiHL N° 1 6

1ère année – Bulletin annuel
Juin 2023 – Juin 2024

BULLETIN DE L'EDiHL N° 2 93

2ème année – Bulletin annuel
Juin 2024 – Juin 2025

BULLETIN DE L'EDiHL N° 3 204

3ème année – Bulletin annuel
Juin 2025 – Juin 2026

LISTE DES CONTRIBUTEURS 2023-2026 406-407

Nathalie DE GROVE-VALDEYRON
Claire BORIES
Directrices scientifiques
Claire BORIES
Coordinatrice

Bulletin de l'EDiHL

European Digital Health Law

ACTUALITÉ DU DROIT EUROPÉEN DU NUMÉRIQUE EN SANTÉ
Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

À LA UNE

ESPACE EUROPÉEN DES DONNÉES DE SANTÉ

Résolution législative du Parlement européen du 24 avril 2024 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (*COM(2022)* 0197 final – C9-0167/2022 – 2022/0140(COD))

par Lisa FERIOL

GOUVERNANCE DES DONNÉES DE SANTÉ

Rapport d'information sur les données de santé en France : une clarification nécessaire du cadre actuel

Catherine DEROCHE, *Rapport d'information au nom de la commission des affaires sociales sur les données de santé*, Session extraordinaire de 2022-2023, Sénat n° 873

par Nino ESCUDIER

ACCÈS AUX DONNÉES DE SANTÉ

La reconnaissance pour les patients d'un accès gratuit à la première copie de leur dossier médical

CJUE, 26 octobre 2023, *FT c. DW*, aff. C-307/22, ECLI:EU:C:2023:811

par Sarah BISTER

N° 1

1ère année – Bulletin annuel
Juin 2023-Juin 2024

ÉDITORIAL

Nathalie DE GROVE-VALDEYRON
Professeure de droit public
Chaire Jean Monnet (2017-2023) et (2023 - 2026)
Université Toulouse Capitole – IRDEIC

Dans le cadre de la construction en cours d'un « marché unique des données », qui relève de la stratégie numérique de l'Union pour les 10 années à venir, les données de santé occupent une place essentielle compte tenu des enjeux qu'elles recèlent. En tant que données personnelles, elles jouissent à ce titre d'une protection juridique renforcée, garantie par le Règlement général sur la protection des données, mais elles peuvent aussi, à certaines conditions, être mises à disposition et partagées dans un contexte transfrontalier afin, d'une part, de permettre une meilleure prise en charge des patients et la continuité des soins, mais aussi, d'autre part, de favoriser l'innovation et la recherche en santé, de développer une médecine de plus en plus personnalisée et plus précise, grâce à l'exploitation de vastes bases de données auxquelles des systèmes d'IA pourront être appliqués.

On perçoit d'emblée les enjeux en présence, tant juridiques qu'éthiques, et l'équilibre à trouver entre « intérêt privé » (le citoyen veut avoir le contrôle sur ses données de santé et décider s'il veut les partager, avec qui et à quelles conditions) et « intérêt général » (pour la recherche scientifique dans le domaine des activités de santé et de soin notamment).

C'est à cet équilibre que tend le règlement sur l'Espace européen des données de santé (ci-après EHDS), premier des espaces communs dont l'Union entend se doter et qui soulève un grand nombre de défis, notamment, au premier chef, celui de concilier la compétence de l'Union avec celle des États membres dans le domaine du numérique en santé, mais aussi celui de trouver une place cohérente au sein de tout un arsenal de textes juridiques touchant au numérique (règlement sur la gouvernance des données, règlement sur les données, règlement sur l'intelligence artificielle, règlement sur la cybersécurité, règlements sur les dispositifs médicaux, directive NIS 2 ….).

Le règlement sur l'Intelligence artificielle, récemment adopté, ouvre également de nouvelles perspectives dans son application au domaine de la santé et, ici aussi, son articulation avec d'autres règlements (EHDS, règlements sur les dispositifs médicaux, règlement sur la surveillance des marchés…) suscite nombre de questionnements.

L'objet de ce bulletin est de suivre, au cours des 3 années de la chaire EDIHL dont je suis titulaire, l'activité principalement législative, mais aussi le cas échéant contentieuse (même si à ce jour, ce qui semble logique, elle apparaît beaucoup plus marginale), dans ce domaine en construction du droit européen du numérique en santé.

Cette discipline étant naissante, il s'agit de commenter les textes en cours d'adoption, qu'ils soient contraignants ou qu'ils prennent la forme de Guidelines, d'orientations, de recommandations, au niveau européen. Il s'agit aussi, plus largement, de s'intéresser aux contextes juridiques nationaux avec lesquels les textes européens adoptés ou en cours d'adoption devront s'articuler car il convient de garder à l'esprit que les États restent responsables, conformément à l'article 168 §7 du TFUE, de tout ce qui relève de l'organisation de leur système de soins de santé, et que le RGPD leur accorde aussi une marge de manœuvre dans le domaine des données de santé. Cette dernière, ce qui peut paraître à certains égards paradoxal, est à l'origine d'une « fragmentation » de ces mêmes données, à laquelle le règlement EHDS tente de remédier.

Le premier bulletin s'intéresse donc aussi subsidiairement au contexte national français mais les prochains bulletins auront vocation à prendre aussi en compte les cadres juridiques nationaux d'autres États membres afin de mettre en évidence les difficultés à lever dans la mise en œuvre du règlement EHDS.

Ce premier bulletin, coordonné et réalisé par Claire Bories, docteure en droit, a associé des doctorants et des étudiants de Master 2 juriste européen (promotion 2023-2024). Qu'ils soient tous chaleureusement remerciés.

Bulletin de l'EDiHL
European Digital Health Law

SOMMAIRE

N°1 /
1ère année – Bulletin annuel
Juin 2023-Juin 2024

VEILLE LÉGISLATIVE

L'INTELLIGENCE ARTIFICIELLE EN SANTÉ 6

Aperçu général sur l'IA Act 6

European Commission, Living guidelines on the Responsible use of generative AI in research. ERA Forum Stakeholders' document, First Version, coll. , « EU Publications », March 2024
par Noémie DUBRUEL **9**

STRATÉGIE GLOBALE SUR LE BIG DATA – EMA 15

Note sous EMA, *Big Data Steering Group (BDSG) : 2023 Report*, 18 January 2024 et *Multi-annual AI workplan 2023-2028. HMA-EMA Big Data Steering Group*, November 2023
par Valentine DURAND **15**

EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, 13 July 2023
par Noémie DUBRUEL **19**

ESPACE EUROPÉEN DES DONNÉES DE SANTÉ 23

Résolution législative du Parlement européen du 24 avril 2024 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))
par Lisa FERIOL **23**

E-HEALTH NETWORK 42

Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, Hospital Discharge Report, Release 1.0, November 2023
par Sarah BISTER **42**

Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, Medical imaging studies and reports, Release 1.0, November 2023.
par Sarah BISTER **44**

ACTION CONJOINTE TEHDaS 45

Options for the services and services architecture and infrastructure for secondary use of data in the EHDS, 4 July 2023

Compilation of perspectives on multi-country data access applications, mutual recognition and cross- border applications through a workshop approach, 5 July 2023

Kalliola Markus et al., Advancing data sharing to improve health for all in Europe. Main findings of joint action Towards the European Health Data Space 2021–2023, Septembre 2023

Guidelines document for multi-country data access applications, including mutual

recognition and cross-border applications, 22 September 2023

Recommendations on a Data Quality Framework for the European Health Data Space for secondary use, 26 September 2023

Sustainability Plan for Secondary Use of Health Data in the European Health Data Space, 29 September 2023

Report on lessons learned to be applied and recommendations for data altruism practices in the implementation of construction of national and European health data spaces (including broad consent), 29 September 2023

ACCÈS ET CONTRÔLE DES PATIENTS DE LEURS DONNÉES DE SANTÉ 46

Arrêté du 26 octobre 2023 fixant les règles de gestion des droits d'accès au dossier médical partagé des professionnels mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 du code de la santé publique, JORF n°0252 du 29 octobre 2023
par Sarah BISTER **46**

GOUVERNANCE DES DONNÉES DE SANTÉ 47

Rapport d'information sur les données de santé en France : une clarification nécessaire du cadre actuel
DEROCHE Catherine, *Rapport d'information au nom de la commission des affaires sociales sur les données de santé*, Session extraordinaire de 2022-2023, Sénat n° 873
par Nino ESCUDIER **47**

DEROCHE Catherine, *Rapport d'information au nom de la commission des affaires sociales (1) sur la proposition de résolution européenne au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé - COM(2022) 197 final*, Session extraordinaire 2022-20223, Sénat n° 874

UTILISATION SECONDAIRE DES DONNEES DE SANTE 53

MARCHAND-ARVIER Jérôme et *al.*, Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé, 5 décembre 2023
par Shana LEVI **53**

HÉBERGEMENT DES DONNÉES DE SANTÉ 56

Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel, JORF n°0113 du 16 mai 2024

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1), *JORF* n° 0117 du 22 mai 2024

« MON ESPACE SANTÉ » FRANCE – ACTUALITÉS 58

Arrêté du 23 octobre 2023 modifiant l'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, JORF n°0253 du 31 octobre 2023

TÉLÉCONSULTATION 60

Loi de financement de la sécurité sociale pour 2024. Focus sur certaines dispositions

Loi n° 2023-1250 du 26 décembre 2023 de financement de la sécurité sociale pour 2024, *JORF* n° 0299 du 27 décembre 2023
par Sarah BISTER 60

La reconnaissance des sociétés de téléconsultation en droit français comme véritables opérateurs de santé ?
Décret n°2024-164 du 29 février 2024 relatif aux sociétés de téléconsultation, *JORF* n° 0051 du 1er mars 2024
par Sarah BISTER 65

PRESCRIPTION ÉLECTRONIQUE – TÉLÉMATIQUE 70

Décret n° 2023-1222 du 20 décembre 2023 relatif à la mise en œuvre de la prescription électronique, JORF n° 0295 du 21 décembre 2023 70

Arrêté royal fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux praticiens de l'art dentaire pour l'utilisation de la télématique et pour la gestion des dossiers médicaux en 2023, *M.B.* du 27 décembre 2023 72

ACCÈS AUX THÉRAPIES NUMÉRIQUES 73

EFPIA, *Improving access to digital therapeutics in Europe*, June 2023
par Dorianne CATTOEN 73

VEILLE CONTENTIEUSE

ACCÈS DES PATIENTS À LEURS DONNÉES DE SANTÉ 79

La reconnaissance pour les patients d'un accès gratuit à la première copie de leur dossier médical
CJUE, 26 octobre 2023, *FT c. DW*, aff. C-307/22, ECLI:EU:C:2023:811
par Sarah BISTER 79

VENTE EN LIGNE DE MÉDICAMENTS 85

Vente en ligne de médicaments via la plateforme Doctipharma : la Cour de justice précise les interdictions que peut prononcer un État membre
CJUE, 29 février 2024, *Doctipharma*, aff. C-606/21, ECLI:EU:C:2023:585
par Claire BORIES 85

Aperçu général sur l'IA Act[1]



La Commission a proposé un encadrement de l'IA en présentant une proposition de règlement[2], le 21 avril 2021. L'objectif annoncé est d'établir un cadre juridique uniforme pour le développement, la commercialisation, l'utilisation et l'adoption de l'intelligence artificielle (IA) dans le marché intérieur, conformément aux valeurs de l'Union.

EN SAVOIR PLUS

Ce cadre juridique doit garantir un niveau de protection élevé et cohérent, dans l'ensemble de l'Union, des intérêts publics comme la santé, la sécurité et la protection des droits fondamentaux, tels qu'ils sont reconnus et protégés par le droit de l'Union. Soulignant qu'il est dans l'intérêt de l'Union « d'être un leader mondial dans le développement d'une intelligence artificielle centrée sur l'humain, durable, sûre, éthique et digne de confiance », la proposition présentée se situe dans le prolongement d'un livre blanc sur l'IA « Une approche européenne de l'excellence et de la confiance[3] ». Elle répond aussi à une résolution du Parlement européen portant sur un cadre d'aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes[4] qui recommandait expressément à la Commission « de proposer des mesures législatives pour exploiter les opportunités et les avantages de l'IA, mais aussi d'assurer la protection des principes éthiques ».

Les **principes** sur lesquels reposent la proposition de 2021 peuvent être brièvement rappelés : il s'agit de :

« - garantir que les systèmes d'IA mis sur le marché de l'Union et utilisés sont sûrs et respectent le droit existant en matière de droits fondamentaux et les valeurs de l'Union ;

- assurer la sécurité juridique pour faciliter l'investissement et l'innovation dans l'IA ;

- renforcer la gouvernance et l'application effective de la législation existante sur les droits fondamentaux et les exigences de sécurité applicables aux systèmes d'IA ;

- faciliter le développement d'un marché unique pour les applications d'IA légales, sûres et dignes de confiance et prévenir la fragmentation du marché ».

Afin d'atteindre ces objectifs la Commission propose une approche harmonisée fondée et proportionnée au risque. Elle établit ainsi une distinction selon que le risque est « inacceptable » « élevé » ou « faible ». Relèvent de la première catégorie « les systèmes d'IA [qui sont] considérés comme une menace manifeste pour la sécurité, les moyens de subsistance et les droits des personnes ». De

[1] L'IA Act dans ses applications au domaine de la santé sera commenté dans le prochain bulletin. Sur la proposition, voir DE GROVE -VALDEYRON Nathalie, « Une union protectrice fondée sur des valeurs, réflexions liminaires sur l'IA appliquée à la santé », *RUE*, 2021 n°653.
[2] *COM(2021)* 206 final du 21 avril 2021.
[3] *COM(2020)* 65 final du 19 février 2020.
[4] T90275/2020, 20 octobre 2020.

tels systèmes sont interdits. Les « systèmes d'IA à haut risque » (risque élevé) au titre desquels figurent, notamment, « les composants de sécurité des produits (par exemple, l'application de l'IA dans la chirurgie assistée par robot), ou de façon générale, les produits de santé relevant de la législation sectorielle visés en annexe du règlement (les DM soumis à évaluation de leur conformité par un tiers) ». Pour ceux -ci, le respect d'exigences spécifiques établies par le règlement s'impose. Elles se traduisent, notamment, par des systèmes d'atténuation des risques, la qualité des ensembles de données utilisés, l'enregistrement des activités ; la documentation détaillée ; la fourniture d'informations claires à l'utilisateur ; le contrôle humain ainsi qu'un niveau élevé de performances en matière de robustesse, d'exactitude et de cybersécurité. Enfin, les « systèmes d'IA à risque limité ou faible », ce qui recouvre la grande majorité des systèmes d'IA, sont exemptés de toute obligation car ils ne présentent qu'un risque minime ou nul pour les droits ou la sécurité des citoyens. Les entreprises pourront néanmoins, de manière volontaire, s'engager à adopter des codes de conduite supplémentaires.

Le Parlement européen a présenté sa position en première lecture le 14 juin 2023[5]. Il insiste sur le respect des valeurs de l'Union. Pour encourager l'innovation en matière d'IA et soutenir les PME, les députés ont ajouté des exceptions pour les activités de recherche et les composants d'IA fournis dans le cadre de licences libres. La nouvelle législation encourage ce que l'on appelle les « bacs à sable réglementaires pour l'IA », ou les environnements de mise en situation, mis en place par les autorités publiques pour tester l'IA avant son déploiement.

Un certain nombre de principes généraux doivent être respectés lors du développement ou l'utilisation de systèmes d'IA ou de systèmes d'IA à finalité générale. Sont ainsi énumérés : « i) «facteur humain et contrôle humain»; ii) «solidité technique et sécurité»; iii) «protection de la vie privée et gouvernance des données»; iv) «transparence»; v) «diversité, non-discrimination et équité»; vi) «bien-être social et environnemental» ».

Les députés ont par ailleurs élargi la liste des pratiques interdites pour inclure des interdictions des utilisations intrusives et discriminatoires de l'IA. Les systèmes d'IA générative basés sur des modèles tels que ChatGPT devraient respecter les exigences en matière de transparence (mentionner que le contenu est généré par l'IA, aider également à distinguer les fausses images des vraies en cas d'hypertrucage) et offrir des garanties contre la génération de contenus illicites. Des résumés détaillés des données protégées par le droit d'auteur utilisées pour la formation des IA devront également être rendus public.

La proposition établit le bureau de l'IA (bureau européen de l'IA[6]) qui devrait être un organe indépendant de l'Union (siège situé à Bruxelles). Il aura notamment comme tâche de soutenir, conseiller les États membres, les autorités de surveillance nationales, la Commission et les autres institutions, organes ou organismes de l'Union et coopérer avec eux en ce qui concerne la mise en œuvre du règlement.
Les personnes physiques ou les groupes de personnes physiques auraient le droit d'introduire une réclamation auprès d'une autorité de contrôle nationale s'ils considèrent que le système d'IA les concernant viole le règlement. Enfin, les

[5] T9-0236/2023.

[6] Le bureau européen de l'IA a été créé par une décision de la Commission du 24 janvier 2024, voir ci -après.

députés veulent renforcer le droit des citoyens à recevoir des explications sur les décisions fondées sur des systèmes d'IA à haut risque qui ont une incidence significative sur leur santé, leur sécurité, leurs droits fondamentaux, et leur bien-être socioéconomique.

Après 1ère lecture du Parlement européen, le règlement a été adopté par le Conseil (en 1ère lecture) le 21 mai 2024 et l'acte final a été signé le 13 juin 2024.

Un bureau européen de l'intelligence artificielle [7] a été créé, comme précédemment mentionné, par la décision de la Commission du 24 janvier 2024, au sein de la Commission européenne, dans le cadre de la structure administrative et du plan de gestion annuel de la direction générale des réseaux de communication, du contenu et des technologies. Il répond au besoin de se doter de mesures supplémentaires « pour tenter de mieux comprendre les capacités, les tendances et les risques potentiels en matière d'IA et pour soutenir le développement et l'utilisation sûrs de ces technologies dans l'Union » (considérant 6). On relèvera que ce bureau a été créé, de façon anticipée, suite à l'accord politique des colégislateurs conclu le 8 décembre 2023. La décision pourra être révisée après adoption du règlement. Les missions de ce bureau, trop nombreuses pour pouvoir être toutes reprises ici, figurent à l'article 3 de la décision. On notera notamment qu'il sera « chargé d'assister la Commission dans l'élaboration d'orientations et de lignes directrices visant à soutenir la mise en œuvre pratique du futur règlement, ainsi que de mettre au point des outils de soutien, tels que des protocoles normalisés et des bonnes pratiques, en concertation avec les services de la Commission et organes et organismes de l'Union compétents; ou encore « d'assister la Commission dans la préparation des demandes de normalisation,

Il y a lieu de créer les bases d'un système de gouvernance unique pour l'IA dans l'Union en créant une structure qui soit chargée de surveiller les progrès des modèles d'intelligence artificielle, notamment les modèles d'IA à usage général, ainsi que l'interaction avec la communauté scientifique, et qui ait une vocation mondiale et joue un rôle clé en matière d'enquêtes, d'essais et d'application de la législation sur l'IA. En conséquence, un Bureau européen de l'Intelligence artificielle devrait être crée au sein de la Commission, dans le cadre de la structure administrative et du plan de gestion annuel de la direction des réseaux de communication, de contenu et des technologies.

EN SAVOIR PLUS

dans l'évaluation des normes existantes et dans l'élaboration de spécifications communes pour la mise en œuvre du futur règlement ».

Ce rôle s'avère particulièrement important au regard des nouvelles obligations qui pèsent désormais, avec l'IA Act, sur les différents opérateurs, des producteurs aux déployeurs des systèmes d'IA jugés à haut risque, en termes de sécurité, de santé et de droits fondamentaux. Le nombre considérable d'actes d'exécution qui devront être adoptés pour rendre le règlement opérationnel, permet d'apprécier les enjeux en présence.

On pense tout particulièrement aux normes techniques qui devront être adoptées pour garantir, à titre d'exemple, dans le domaine de la santé, que les dispositifs médicaux connectés, contenant de l'IA (intégrant ou fonctionnant à l'aide d'IA), répondront aux exigences essentielles de sécurité visées par le règlement 2017/745 sur les dispositifs médicaux et respecteront les droits fondamentaux (IA act). Ceux-ci devront être intégrés dans les systèmes d'IA, en tant qu'exigences essentielles, selon les règles désormais bien connues de la « nouvelle approche » de l'harmonisation technique, au même titre que les exigences plus habituelles en matière de santé et de

[7] Décision n° C /2024/1459 du 24 janvier 2024, *JOUE* du 14 février 2024.

sécurité, afin de pouvoir accéder au marché intérieur et bénéficier du marquage CE. Le respect de cette nouvelle exigence ne va pas aller de soi[8] et nécessitera la plus grande vigilance des organisations de la société civile, des académiques et des experts en plus des ingénieurs chargés de les élaborer afin de mettre au point des normes techniques répondant aux exigences imposées par la règlementation européenne.

European Commission, *Living guidelines on the Responsible use of generative AI in research. ERA Forum Stakeholders' document,* First Version, coll. , « EU Publications », March 2024

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Introduction

Le 20 mars dernier, la Commission européenne a publié des lignes directrices pour une utilisation responsable des Intelligences Artificielles (IA) génératives[9]. Ce document a été élaboré par les membres du Forum ERA (*European Research Area*), ainsi que par plusieurs parties prenantes, notamment associées au programme Horizon Europe[10]. Plus précisément, le Forum ERA est une plateforme de l'Espace européen de la recherche créée en 2022, dans le but de permettre le dialogue et la coopération entre la Commission européenne, les gouvernements des Etats membres et les différents acteurs de la recherche et de l'innovation[11]. Ce forum joue un rôle dans l'accompagnement de l'élaboration et de la mise en œuvre de textes contraignants, de programmes de recherche ou d'initiatives politiques qui peuvent avoir un impact sur l'amélioration du déploiement des technologies, de l'innovation et de la recherche[12]. La définition de ce rôle explique que le Forum ERA soit l'auteur des lignes directrices, objet de notre analyse.

Ces dernières s'inscrivent dans une volonté européenne d'accompagner le déploiement de méthodes innovantes dans la recherche tout en apportant les premières pierres à l'édifice d'un encadrement adapté[13]. Pour cela, ces lignes directrices sont directement adressées à trois catégories de professionnels : les chercheurs, les organismes de recherche (qu'ils soient publics ou privés) et les financeurs de la

[8] LEWKOWICZ Gregory, « Règlement sur l'IA : une victoire pour les droits fondamentaux ? », *JDE,* 2024/2, n°306, 15 février 2024.

[9] European Commission, « Living guidelines on the responsible use of generative AI in research », ERA Forum Stakeholders' document, Fisrt Version, March 2024, 18p.

[10] Résolution législative du Parlement européen du 17 avril 2019 sur la proposition de règlement du Parlement européen et du Conseil portant établissement du programme-cadre pour la recherche et l'innovation « Horizon Europe » et définissant ses règles de participation et de diffusion (COM(2018)0435-C8-0252/2018-2018/0224(COD)), Établissement du programme-cadre « Horizon Europe »x – définition de ses règles de participation et de diffusion, P8-TA(2019)0395, 2014-2019.

[11] « European Research Area Platform », site de la Commission européenne (Consulté le 03/06/2024).

[12] European Commission, Directorate A – ERA and Innovation, « Informal Commission Expert Group 'ERA Forum'. Terms of reference », Brussels, February 2023, p.01.

[13] « Living guidelines on the responsible use of generative AI in research », *op. cit.,* p.11.

recherche[14]. En outre, elles concernent spécifiquement les IA génératives sans pour autant en apporter de définitions explicites[15]. Les intelligences artificielles dites génératives sont largement entendues comme des systèmes algorithmiques capables de générer du contenu unique[16]. Plusieurs applications émergent ainsi dans notre environnement quotidien, dont le plus célèbre est ChatGPT[17]. D'autres peuvent également être identifiées telles que Midjourney[18] ou bien encore QuillBot[19]. Ces types d'IA se développent rapidement, accessibles à tous, faciles d'utilisation et donc déployées dans toutes les sphères de la société. Le domaine de la science est alors particulièrement impacté par le déploiement de ces nouveaux outils, aptes à produire de nouvelles formes d'informations[20]. Suivant une évolution un peu plus récente, le domaine de la recherche n'a, lui aussi, pas échappé à l'émergence de cette innovation[21]. En effet, l'IA - et le numérique de manière générale - sont de réels atouts pour l'optimisation de la recherche. Depuis plusieurs années, le traitement de données de masse, les outils numériques et informatiques et, depuis peu l'IA, se développent de plus en plus pour diverses finalités. De la découverte de médicaments aux différentes étapes de la recherche scientifique et en santé, ces innovations présentent des intérêts flagrants. Dans le domaine de la recherche clinique par exemple, l'IA et le numérique sont de réels outils pour l'élaboration de design complexes d'essais[22], pour l'identification des populations à inclure dans un essai[23], pour la dématérialisation ou encore la décentralisation des essais cliniques[24].

Plus largement dans l'ensemble du spectre de la recherche, ces innovations favorisent l'accès et le partage des connaissances, permettent d'identifier des sujets de recherche, aident aux traductions mais également à la rédaction d'articles scientifiques[25]. C'est dans ce panel d'utilisations possibles que les IA génératives jouent un rôle particulièrement intéressant, pour la production de textes, de documentations de la recherche ou bien encore de références directement utilisées dans la recherche[26].

Si le recours, de plus en plus facilité, aux IA génératives garantit une simplification de certaines étapes de la recherche et ainsi son accélération, ces lignes directrices insistent sur l'importance d'encadrer leurs utilisations afin de garantir une fiabilité et une loyauté essentielles à la validité de la recherche.

---

[14] *Ibid.*, p. 6-9.
[15] *Ibid.,* p. 3.
[16] LAMRI Jérémy et *al.*, « Chapitre 1. Comprendre les IA génératives et leur portée », *in* LAMRI Jérémy (dir.), *Travailler à l'ère des IA génératives*, éd. EMS Editions, coll. « Questions de société », 2023, p. 23-67.
[17] ChatGPT est une IA générative développée par Open AI accessible au grand public, [Accessible en ligne].
[18] Midjourney est une IA générative développée par une entreprise privée du même nom, capable de développer des images à partir d'algorithmes qui analysent des mots-clés, [Accessible en ligne].
[19] QuillBot est un outil d'IA générative permettant de rédiger des documents ou article en proposant une réécriture à partir de mots clés, [Accessible en ligne].
[20] European Commission, Group of Chief Scientific Advisors, « Successful and timely uptake of Artificial Intelligence in science in the EU », *Scientific Advice Mechanism*, *Scientific Opinion*, n° 15, March 2024.
[21] « Living guidelines on the responsible use of generative AI in research », *op. cit.,* p. 3-4.
[22] BATOOL Maria et *al.*, « A Structure-Based Drug Discovery Paradigm », *Int J Mol Sci*, vol. 20, n°11, June 2019.
[23] DUGUET Anne-Marie., « The place of digital and artificial intelligence in Medical research », *in* ZIMA Thomas et WEISSTUB Nicolas D. (dirs..), *Medical research ethics: challenges in the 21st century*, Editors Philosophy and medicine, vol. 132 Springer, January 2023, p. 476.
[24] LEEM « Essais cliniques 2030 », Étude réalisée par IQVIA auprès d'experts français et internationaux, 10/03/2022, 97p.
[25] LUND B.D et *al.*, « ChatGPT and a New Academic Reality: Artificial Intelligence-Written Research Papers and the Ethics of the Large Language Models in Scholarly Publishing », *Journal of the Association for Information Science and Technology*, Vol. 74, n° 5, 2023, p. 570-581.
[26] « Living guidelines on the responsible use of generative AI in research », *op. cit.,*p. 4.

I. PENSER ET ENCADRER LES RISQUES POUR UNE UTILISATION RESPONSABLE DES IA GENERATIVES DANS LA RECHERCHE

Ces lignes directrices prônent un accompagnement des différents acteurs de la recherche afin de garantir une utilisation responsable des IA génératives. A travers cette volonté, la Commission européenne souhaite favoriser l'innovation permise par le recours aux IA tout en limitant tout risque de mésusage pouvant s'avérer dramatique pour la qualité de la recherche en Europe. En effet, les IA génératives présentent des risques qui sont propres à leur mode de fonctionnement. Plus précisément, ces algorithmes fonctionnent sur des modèles d'apprentissages autonomes, le plus souvent sous la forme de boîtes noires, qui ne garantissent pas un contrôle suffisant des sources utilisées et des modalités d'apprentissages du système[27]. Il n'est ainsi pas toujours possible pour l'humain d'expliquer le raisonnement de l'algorithme qui lui permet d'arriver à un résultat donné. Cette absence de contrôle et d'explicabilité laisse la porte ouverte à des biais et informations erronées voire totalement inventées. Les auteurs des lignes directrices parlent alors des « hallucinations »[28] des IA génératives qui créent des informations fausses pouvant sembler être vraies. En outre, l'appropriation par l'IA d'informations dont elle est nourrie, ne tient pas compte des enjeux de propriété intellectuelle. En d'autres mots, les IA génératives peuvent retranscrire des éléments d'informations issus d'une production intellectuelle humaine sans en préciser l'appartenance. Dans le domaine de la recherche, de tels risques peuvent véritablement fausser et faire perdre toute substance au travail du chercheur. C'est en considérant cela que la Commission européenne insiste sur l'importance de mener une recherche responsable.

Pour ce faire, les recommandations émises auprès des acteurs de la recherche reposent sur deux documents essentiels. Le premier est le code de conduite pour l'intégrité de la recherche[29]. Ce document, revisité en 2023, pose des principes essentiels d'honnêteté, de loyauté et de fiabilité de la recherche, garants de sa qualité[30]. De plus, la responsabilité de la recherche est notamment considérée au regard de son impact sociétal[31]. Enfin, la notion de respect, que cela soit des autres chercheurs, du patrimoine de la recherche ou bien encore de l'ensemble de son écosystème[32] est une garantie essentielle. En parallèle, ce code de conduite édicte des pratiques qualifiées d'inacceptables telles que la création de faux, la falsification de la recherche et le plagiat[33]. Or, au regard des risques inhérents aux IA génératives, nous constatons que ces pratiques peuvent assez aisément être induites en ayant recours à ces innovations sans même que le chercheur en ait conscience.

Face à ce constat, la responsabilisation des acteurs de la recherche n'apparaît pas suffisante. Il importe que les systèmes d'IA qui sont mis à la disposition de la communauté scientifique, soient conformes aux exigences d'intégrité exigées par l'Union européenne. En ce sens, les lignes directrices pour une utilisation responsable des IA génératives dans la recherche sont également fondées sur des principes pour « une IA digne de confiance », dont les premières versions ont été établis en 2018

[27] LOUBES Jean-Michel et RISSER Laurent, « Intelligence Artificielle de confiance : biais et explicabilité en IA », CNRS Formation, 21 mars 2023.
[28] « Living guidelines on the responsible use of generative AI in research », *op. cit.*,p. 6 et note de bas de page n°14.
[29] All European Academies (Allea), « The European Code of Conduct for Research Integrity", Revised edition, Berlin, June 2023.
[30] *Ibid.*, p. 3.
[31] *Ibid.*, p. 4.
[32] *Ibid.*, p. 5.
[33] *Ibid.*, p.10.

par un groupe d'expert[34]. Ces premières lignes directrices, qui illustrent les prémices de la prise de position de l'Union européenne en matière d'IA, insistent sur l'importance de ne déployer que des IA robustes, éthiques, respectueuses de la législation et la réglementation en vigueur mais aussi et surtout conformes aux valeurs de l'Union européenne de protection des individus et de leurs droits fondamentaux[35].

Ce panel de principes et de notions phares orientent les recommandations émises auprès des acteurs de la recherche directement visés par ces nouvelles lignes directrices.

II. L'IMPORTANCE DU SOUTIEN DES ACTEURS DE LA RECHERCHE DANS L'UTILISATION DES IA GENERATIVES

La Commission européenne s'appuie sur des principes existants afin de promulguer des recommandations auprès des différents acteurs de la recherche identifiés. La volonté première de la Commission s'inscrit dans une logique de sensibilisation des usages et limites des IA génératives pour parvenir à un changement culturel d'appropriation de l'IA par la communauté de la recherche. En second lieu, la Commission prône une réelle responsabilisation des acteurs pour établir un environnement sûr pour la recherche. La volonté européenne est alors claire : favoriser l'exploitation du potentiel de l'IA dans la recherche sans porter atteinte à son intégrité ni à celle du chercheur et sans mettre à mal la confiance des citoyens dans la recherche[36].

Concrètement, ces lignes directrices permettent l'identification de points d'actions à mettre en œuvre, adressés aux trois catégories d'acteurs concernés[37]. Pour les chercheurs, les recommandations portent sur une responsabilisation et une transparence dans les usages et production de l'IA. L'accent est mis sur le respect de la vie privée, de la confidentialité ainsi que des droits de propriété intellectuelle lors du partage des informations dans les outils d'IA, le tout conformément aux législations nationale, européenne et internationale en vigueur[38].

En parallèle, les organismes de recherche se voient adresser des exigences de promotion et de soutien des utilisations qui peuvent être faites des IA aux seins de leurs organisations[39]. Par ailleurs, dans une optique de limitation des biais, il est recommandé aux organismes de mettre en œuvre des IA génératives hébergées localement ou basées sur un cloud qu'ils gouvernent eux-mêmes chaque fois que cela est possible[40]. Ces recommandations spécifiques sont adressées de façon à harmoniser des actions « individuelles » mises en œuvre dans divers établissements de recherche, dans le but de contrôler et d'encadrer, autant que faire cepeut, le recours aux IA génératives. L'Union européenne souhaite ainsi apporter un accompagnement qui laisse une marge de manœuvre suffisante à chaque organisme de recherche tout en harmonisant les différentes actions mises en œuvre[41].

Enfin, les financeurs de la recherche sont également visés par des recommandations qui leurs sont spécifiques. Ils sont désignés comme devant montrer la voie par un examen minutieux de l'utilisation des IA génératives au sein de

[34] Groupe d'experts de haut niveau sur l'intelligence artificielle, « Lignes directrices en matière d'éthique pour une IA digne de confiance », Avril 2019.
[35] Groupe d'experts de haut niveau sur l'intelligence artificielle, « Lignes directrices en matière d'éthique pour une IA digne de confiance », Avril 2019., p. 11-12.
[36] « La Commission et la communauté de la recherche élaborent des lignes directrices sur l'utilisation responsable de l'intelligence artificielle générative dans la recherche », *Press Release*, 20 mars 2024.
[37] « Living guidelines on the responsible use of generative AI in research », *op. cit.*,p. 6-9.
[38] *Ibid.*, p. 7.
[39] *Ibid.*, p. 8.
[40] *Ibid.*
[41] *Ibid.*, p. 8.

leurs processus internes ainsi qu'en attendant de la communauté des chercheurs un maximum de transparence sur le recours aux IA dans leurs travaux[42]. Nous soulignons qu'il est particulièrement intéressant que les financeurs soient concernés par ces lignes directrices, particularité qui illustre le rôle important dans la promotion et le soutien de la recherche.

Conclusion

Par l'élaboration de ces lignes directrices, le Forum ERA et la Commission européenne ont allié leurs voix afin de sensibiliser et de responsabiliser les divers acteurs de la recherche concernés par le déploiement des IA génératives qui bouleversent tous les pans de notre société.

Afin d'être au plus près des attentes des acteurs et, surtout, de suivre les évolutions constantes et rapides des technologies, ces lignes directrices ont été pensées sous la forme de « lignes directrices vivantes »[43]. Cette considération originale présente ainsi une forme particulière d'engagement des acteurs concernés par un appel à commentaires permanent. Des mises à jour régulières – selon une temporalité encore inconnue - seront pensées et mises en œuvre au fur et à mesure des commentaires qui seront adressés via une page spécifiquement dédiée[44].

Nous espérons alors que les divers commentaires qui ont été et seront adressés à la Commission européenne sur ce document permettront sa révision. En effet, si cette initiative est à saluer, certains points mériteraient d'être approfondis. De manière générale, au regard des risques que ces innovations renforcent ou font émerger dans le domaine de la recherche, il est important d'insister sur le besoin d'un réel engagement des chercheurs et organismes de recherches dans l'usage des IA génératives. Si ces exigences sont importantes elles ne doivent pas pour autant entraver la liberté du chercheur[45]. En outre, l'usage responsable des IA génératives pousse à repenser les relations qu'entretiennent les organismes de recherche avec leurs chercheurs. Nous pouvons également nous interroger sur les capacités des organismes de recherche à évaluer la fiabilité des données et des systèmes d'IA utilisés ainsi qu'à former leurs chercheurs considérant que tous les organismes de recherche européens ne disposent pas des mêmes moyens à cet effet[46].

En outre, nous nous inquiétons des utilisations des IA génératives qualifiées de prohibées dans cette première version des lignes directrices, identifiées comme des « utilisations substantielles »[47] qui semblent n'encadrer que des actions volontaires de l'individu. Or, particulièrement dans le cas des IA génératives, un algorithme peut perdre en qualité et en confiance, et produire des résultats erronés ou des hallucinations, notamment s'il est alimenté par des données biaisées ou non-représentatives[48]. Ces points d'attentions obligent à distinguer la dimension éthique de l'objet (de l'IA) de la dimension éthique du comportement (individuel)[49].

Enfin, si ces lignes directrices visent à accompagner l'utilisation des IA génératives dans la recherche vers des démarches responsables, elles font alors inévitablement peser de nouvelles responsabilités sur les chercheurs et les

[42] *Ibid.*

[43] *Ibid.* [Notre traduction de « living guidelines »].

[44] Les commentaires des parties prenantes peuvent être déposées via un formulaire en ligne.

[45] Extrait de la réponse de l'appel à consultation du groupe « Ethique du numérique, de la robotique et de l'IA » de la Chaire UNESCO Ethique, science et société déposée le 31 mai 2024.

[46] *Ibid.*

[47] « Living guidelines on the responsible use of generative AI in research », *op. cit.,* p. 9 et note de bas de page 22.

[48] LOUBES Jean-Michel et RISSER Laurent, « Intelligence Artificielle de confiance : biais et explicabilité en IA », *op. cit.*

[49] Extrait de la réponse de l'appel à consultation du groupe « Ethique du numérique, de la robotique et de l'IA » de la Chaire UNESCO Ethique, science et société déposée le 31 mai 2024.

organismes de recherche. La responsabilisation accrue des chercheurs peut alors faire oublier celle des autres acteurs impliqués dans l'IA et notamment des développeurs et créateurs des IA génératives. De même, si l'ensemble des documents qui couvrent actuellement les différents pans de la responsabilité en matière d'IA sont évoqués dans ces lignes directrices[50], le manque d'une hiérarchie entre les documents applicables est déploré : l'IA Act pose en premier lieu des règles juridiques contraignantes en matière d'IA[51], associées aux diverses obligations de qualité à destination des développeurs des IA pour la mise sur le marché d'innovation de confiance qui doivent prévaloir sur les présentes guidelines à destination des utilisateurs.

Penser le déploiement des IA génératives dans le domaine de la recherche oblige à reconsidérer les risques qui pourraient mettre à mal un domaine dont la loyauté et l'exactitude sont des principes essentiels. En outre, ces innovations emportent une question plus large encore sur ce que signifie faire de la recherche aujourd'hui : quels impacts ces innovations ont-elles sur le temps de la recherche et sur le sens même de la recherche ? Par ailleurs, une non considération des disparités d'accès à ces innovations, qu'elles soient directes ou induites, ne risque-t-elle par de modifier l'environnement européen actuel en créant une recherche « à deux vitesse » ?

[50] « Living guidelines on the responsible use of generative AI in research », *op. cit.,* p.18.

[51] Parlement européen, Amendements du Parlement européen, adoptés le 14 juin 2023, à la 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 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2023)0236.

Note sous EMA, *Big Data Steering Group (BDSG) : 2023 Report*, 18 January 2024 et *Multi-annual AI workplan 2023-2028. HMA-EMA Big Data Steering Group*, November 2023

par Valentine DURAND

Doctorante en Droit public, IRDEIC Université Toulouse Capitole

Dans le domaine pharmaceutique, le régulateur européen suit avec assiduité l'avancée des technologies numériques. Ces technologies présentent un fort potentiel dans ce secteur, qui concentre une quantité importante et croissante de données. Nous pouvons noter deux grands axes d'intérêts pour le régulateur : l'utilisation des technologies numériques pour soutenir le développement de produits de santé, et l'usage réglementaire.

D'une part, le secteur pharmaceutique est un secteur à la fois très innovant et fortement réglementé. Les acteurs de la recherche et du développement pharmaceutique utilisent de plus en plus de technologies numériques ; utilisation que le régulateur doit ensuite analyser pour assurer le maintien de la santé publique. Or, les acteurs cherchent à mobiliser l'intégralité des données à leur disposition et sont demandeurs d'un cadre réglementaire précis et dument motivé qui permettrait de comprendre quelles sont les données mobilisables, dans quel contexte et par quels moyens.

D'autre part, de plus en plus de données sont échangées entre le régulateur et le titulaire, ou potentiel titulaire, d'une autorisation de mise sur le marché d'un médicament. Les possibilités d'échanges d'informations sécurisés et à bas-coût créent de nouvelles interactions pour assurer un niveau toujours plus élevé de qualité, d'efficacité et de sécurité des produits pharmaceutiques. Ces échanges donnent au régulateur un accès à des quantités toujours plus grandes de données. Étudier ces données pourrait permettre d'améliorer la science réglementaire, c'est-à-dire l'ensemble des « activités scientifiques d'évaluation qui participe de la prise de mesures juridiques visant à encadrer activités et produits industriels (autorisation, retrait, fixation de seuils de présence ou d'exposition, étiquetage de médicaments (…), etc. »[52].

Ces éléments contribuent à expliquer la forte volonté du régulateur de développer une règlementation basée sur les données et notamment sur les données massives et les systèmes d'intelligence artificielle.

Le potentiel de l'utilisation des données massives, '*Big Data'*, pour la création de données probantes peut avoir un impact majeur sur la capacité d'innovation pharmaceutique du territoire et sur le maintien et l'amélioration de la santé publique. Les régulateurs européens du médicament seront de plus en plus amenés à se baser sur les données massives pour déterminer le rapport bénéfice-risque du médicament aux différentes étapes de son cycle de vie. Cet usage des données massives pourra optimiser l'utilisation des médicaments, afin de la rendre plus sûre et efficace.

Dès décembre 2019, l'ambition politique du groupe de travail sur les données massives, 'Big Data TaskForce', formé par l'Agence européenne du

[52] BORRAZ Olivier et *al.*, *Dictionnaire critique de l'expertise. Santé, travail, environnement*, Presses de Sciences Po, Coll. « Référence (Presses de Sciences Po) », 2015, pp.279 – 285.

médicament (EMA[53]) et les agences nationales compétentes (HMA[54]), est clairement énoncée : se positionner comme une référence internationale en matière de prise de décision réglementaire basée sur les données[55]. Pour ce faire, l'analyse des possibilités offertes par les données massives se concentre sur les données reçues, analysées ou qui font l'objet de conseil de la part de Réseau européen de réglementation du médicament (en anglais, EMRN). Ce groupe de travail a produit un rapport final en deux phases. La phase I recommande dix chantiers prioritaires afin de développer l'usage des données massives[56] tandis que la phase II, plus détaillée, précise les étapes de réalisation de ces objectifs et établit un plan de priorisation des actions afin de « réaliser le potentiel des données massives »[57].

Faisant suite à ce rapport final, un second groupe de travail, nommé groupe de pilotage conjoint HMA-EMA sur les données massives, le 'Big Data Steering Group' (BDSG)[58], a été instauré afin de conseiller l'EMA et la HMA sur la hiérarchisation et la planification des actions à mettre en place pour suivre les recommandations du rapport. Le BDSG a mis en place un plan d'action[59] qui s'inscrit dans la Stratégie du réseau des agences européennes des médicaments pour 2025[60].

Ce plan d'action décrit onze initiatives et les délivrables qui y sont associés. Le BDSG, en parallèle de la mise à jour régulière du plan d'action, produit des rapports annuels afin de détailler l'avancée des différents chantiers.

Sur le rapport 2023[61] :

L'année 2023 a été productive : les onze initiatives présentées semblent presque toutes progresser. Afin de décrire ces initiatives, nous les classerons en quatre catégories : les initiatives portant sur les données et leurs caractéristiques (**1**), les initiatives portant sur le réseau réglementaire, ses capacités et son cadre de gouvernance (**2**), les initiatives portant sur la collaboration avec les parties prenantes (**3**) et enfin les initiatives vétérinaires (**4**).

1. S'agissant des initiatives sur les données et leurs caractéristiques

Le centre de coordination DARWIN EU fête son premier anniversaire. Cette initiative comporte aujourd'hui vingt partenaires actifs et mène, ou a mené, dix-huit études basées sur des données de vie réelle[62]. Ce centre permet, en parallèle de la mobilisation des données de vie réelle pour l'intérêt général, de créer des standards d'analyse pour ce type de données[63].

S'agissant de la qualité des données, 2023 a vu la publication du cadre de qualité

[53] L'Agence européenne des médicaments (EMA) est une agence décentralisée de l'Union européenne (UE) chargée de l'évaluation scientifique, de la supervision et du contrôle de la sécurité des médicaments dans l'UE.

[54] Le réseau des Chefs des agences du médicament (Heads of Medecines Agencies, HMA) est le réseau des directeurs des agences nationales, compétentes en matière de réglementation des médicaments et des produits de santé à usage humain et vétérinaire au sein de l'espace économique européen.

[55] HMA-EMA Joint Big Data Taskforce, Phase II report: 'Evolving Data-Driven Regulation', EMA/584203/2019, Janvier 2020, page 5.

[56] HMA-EMA Joint Big Data Taskforce, Phase I report: Priority Recommendations of the HMA-EMA joint Big Data Task Force, 2019.

[57] HMA-EMA Joint Big Data Taskforce, Phase II report: 'Evolving Data-Driven Regulation', EMA/584203/2019, Janvier 2020.

[58] HMA – EMA, Joint HMA-EMA Big Data Steering Group, Mandate, EMA/96120/2023, 12 juin 2023.

[59] HMA/EMA joint Big Data Steering Group, Big Data Workplan 2023-2025, version 1.4, Juin 2024.

[60] EMA, European medicines agencies network strategy to 2025, EMA/85501/2020, 2020.

[61] Big Data Steering Group (BDSG), Rapport 2023, EMA/569310/2023, 18 janvier 2024.

[62] Le terme donné de vie réelle est « un terme générique désignant les données relatives aux effets des interventions de santé qui ne sont pas collectées dans le cadre d'essais cliniques randomisés hautement contrôlés ». - Horizon Europe, Work Programme 2021-2022, 4. Health (European Commission Decision C(2022)2975 of 10 May 2022) Part 4, p.145 (Disponible sur ec.europa.eu).

[63] DARWIN EU, Standardised Analytics, Site du centre de coordination Darwin EU [en ligne] (consulté le 25 avril 2024).

des données pour la réglementation européenne sur les médicaments[64]. En effet, les données ne sont utilisables que si elles correspondent à une situation réelle. Elles doivent représenter, le plus fidèlement possible, l'élément qu'elles décrivent. Avoir des standards de qualité permet de déterminer la force probatoire des données utilisées.

Enfin, sur l'accessibilité des données, le rapport présente 2023 comme une année de transition. Après des avancées en 2022, plusieurs délivrables sont attendus pour 2024 (accord sur les métadonnées à utiliser, développement des catalogues de données de vie réelle, etc.). Ces initiatives visent à découvrir de nouvelles sources de données et à les rendre accessibles aux chercheurs.

2. S'agissant des initiatives portant sur le réseau, ses capacités et son cadre de gouvernance

Développer les compétences du réseau européen passe par la formation. D'une part, des curricula portant sur les données massives ont été préparés et les deux premiers modules, relatifs à la pharmaco-épidémiologie et aux preuves de vie réelle ont été déployés. D'autre part, pour que l'EMA ait la capacité de conseiller les développeurs de médicaments dans leurs usages des données massives, plusieurs projets devraient aboutir en 2024, tel qu'un document de réflexion sur l'utilisation des données de vie réelle pour générer des preuves de vie réelle dans les études non-interventionnelles ou une feuille de route pour l'élaboration de lignes directrices sur les preuves de vie réelle.

Afin de développer les processus autour de l'utilisation des données de vie réelle et des preuves fondées sur ces données, l'EMA a produit un rapport portant sur l'expérience acquise dans le cadre des études menées par les régulateurs entre septembre 2021 et février 2023[65]. Ce partage de cas d'usage et de bonnes pratiques devrait servir de base de développement des capacités d'analyse du réseau européen.

S'agissant de la gouvernance, 2023 a permis de mettre à jour le mandat du BDSG, clarifiant ces missions, notamment vis-à-vis de l'intelligence artificielle, et ajoutant à ces membres des représentants de l'Espace européen des données de santé ou encore des payeurs[66].

S'agissant de la capacité du réseau à analyser les données massives, trois thématiques sont abordées : les données brutes ("*raw data*") issues ou non d'essais cliniques, les systèmes d'intelligence artificielle et les initiatives autres en matière d'analyse. Parmi les délivrables, un plan de travail multi-annuel sur l'IA[67]. Étant donné que l'IA est une technologie très consommatrice de données, il est logique de réfléchir son utilisation dans le cadre des données massives. Beaucoup plus succinct que le plan sur les données massives, il ne comporte que quatre catégories d'actions. La première catégorie vise à développer des lignes directrices pour apporter un support au développement et à l'évaluation des systèmes d'IA dans le cycle de vie des médicaments. Ensuite, la stratégie se penche sur la question des outils et technologies d'IA, notamment pour assurer la conformité avec le RGPD[68] mais

[64] EMA, Data Analytics and Methods Task Force, Data Quality Framework for EU medicines regulation, EMA/326985/2023, 30 October 2023.

[65] HMA – EMA, Real-world evidence framework to support EU regulatory decision-making, EMA/289699/2023, 2023.

[66] Le terme « payeur » est défini dans la stratégie des agences européennes du médicament pour 2025 comme les « autorités responsables des décisions de prix et remboursement au niveau national », EMA, *European medicines agencies network strategy to 2025*, EMA/85501/2020, 2020, 48 p.

[67] HMA-EMA BDSG, Multi-annual AI workplan 2023-2028, Novembre 2023.

[68] Règlement n° 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la

aussi pour développer un usage commun dans l'ensemble du réseau réglementaire pour favoriser la prise de décision réglementaire. En parallèle, des objectifs de collaboration et de gestion du changement sont établis pour développer les capacités et les compétences du réseau, des partenaires et des parties prenantes. Enfin, la stratégie cherche à favoriser l'expérimentation, dont il reconnaît le rôle fondamental dans l'accélération de l'apprentissage et l'acquisition de nouvelles connaissances. En organisant des cycles d'expérimentation de six mois, et en mettant en place des cadres précis, la stratégie cherche à établir une approche structurée de l'expérimentation dans l'ensemble du réseau. Le régulateur européen reconnait la rapide évolution des systèmes d'IA et promeut une adaptation continue. Pour ce faire, le plan d'action propose principalement des actions qui s'inscrivent dans le temps long (d'un à quatre ans).

3. S'agissant des initiatives portant sur la collaboration avec les parties prenantes

Le BDSG fait le bilan d'une année d'initiatives internationales et de mobilisation des parties prenantes. S'agissant des initiatives internationales, le BDSG fait état de nombreux projets relatifs aux données de vie réelle et notamment portant sur l'harmonisation des terminologies, des métadonnées, des grands principes d'évaluation réglementaire ainsi que les bonnes pratiques d'enregistrement des résultats et protocoles d'études.

Pour mobiliser les parties prenantes, le BDSG crée des opportunités d'échanges, à travers des ateliers de travail, des forums, des réunions avec les acteurs industriels ou encore des bulletins d'information par courrier électronique. Ces échanges permettent un partage d'information avec l'ensemble des parties informées qui souhaitent intervenir et vise à terme à adapter les évolutions réglementaires aux besoins des parties prenantes.

4. Sur les initiatives vétérinaires

En parallèle des actions et recommandations pour l'utilisation des données massives pour les médicaments à usage humain, le domaine vétérinaire entame lui aussi sa transformation stratégique. Pour ce faire, des échanges interdisciplinaires ainsi qu'un forum des parties prenantes ont été instaurés afin de définir les cas d'usage des données massives dans le domaine vétérinaire, les besoins futurs et les challenges à venir. Une étude cartographiant le paysage des données mobilisables pour l'utilisation des données massives dans le cadre posé par le règlement sur les médicaments vétérinaires[69] a été lancée en 2023.

Il est intéressant de noter que les domaines vétérinaire et humain partagent probablement assez de points communs dans leurs usages de données pour que chacun profite des progrès de l'autre.

Ce rapport confirme les ambitions européennes quant à l'utilisation des données dans le domaine pharmaceutique. La stratégie de prendre le virage technologique le plus tôt possible afin de se positionner comme référence internationale en matière de prise de décision réglementaire fondée sur les données pourrait s'avérer payante. Le régulateur européen semble, du moins, se donner les moyens organisationnels de ses ambitions. **À suivre.**

protection des données), *JOUE* n° L 119, du 4 mai 2016, p. 1–88.

[69] Règlement n° 2019/6/UE du Parlement européen et du Conseil du 11 décembre 2018 relatif aux médicaments vétérinaires, PE/45/2018/REV/1, JOUE n° L 4, du 7 janvier 2019, p. 43–167.

EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, 13 July 2023

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Le 19 juillet 2023, l'Agence européenne du médicament (ci-après « EMA ») a rendu public un papier de réflexion sur l'utilisation de l'Intelligence Artificielle (IA) dans le cycle de vie des médicaments à usage humain et vétérinaire[70]. Ce document a été développé en liaison entre le comité des médicaments à usage humain (CHMP)[71] de l'EMA et son comité des médicaments vétérinaires (CVMP). Ce travail s'inscrit dans les initiatives conjointes du groupe de pilotage *Big Data* (BDSG) HMA-EMA qui vise à développer la capacité du réseau européen de réglementation des médicaments en matière de réglementation basée sur les données[72]. Plus largement, il transparaît de cette initiative la volonté politique européenne claire de rendre disponible des produits de santé sûrs et efficaces[73].

Cette première version de ce papier de réflexion a été ouverte à consultation publique de juillet 2023 à décembre 2023, dans le but de bénéficier des commentaires des différentes parties prenantes concernées par ce sujet ainsi que de l'ensemble des citoyens. Ce processus, assez fréquent au niveau européen, garantit une réelle transparence des différentes actions et volontés européennes. Plus précisément ici, le processus de consultation publique relève d'une réelle volonté d'ouvrir un dialogue avec les développeurs des systèmes algorithmiques, les universitaires et l'ensemble des régulateurs[74]. De plus, le point essentiel de la réflexion à ce stade réside dans l'identification des utilisations qui peuvent être faites de l'IA dans ce domaine, mais également des opportunités et risques qui en découlent[75]. En complément, deux ateliers de réflexion ont été organisés les 20 et 21 novembre 2023 afin de préciser les enjeux soulevés dans ce document[76].

En parallèle, les actions de l'EMA en la matière reflètent celles qui ont été entreprises Outre-manche par la *Food and Drug Administration* (FDA). En effet, l'autorité américaine a initié en 2023 deux documents de discussion pour le recours à l'IA, l'un dans la fabrication de médicament[77] et l'autre dans le développement des médicaments et des produits biologiques[78], suivi d'une

[70] European Medicines Agency, « Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle », EMA/CHMP/CVMP /83833/2023, July 2023, 17p.
[71] Site de l'Agence Européenne du Médicament (EMA), (Consulté le 05/06/2024).
[72] HMA-EMA, Big Data Steering Group, « Big Data Workplan 2022-2023 », Adopted in July 2022, 9p.
[73] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 25 novembre 2020 relative à la Stratégie pharmaceutique pour l'Europe, *COM(2020)* 761 final, 29 p.
[74] « Reflection paper on the use of artificial intelligence in the lifecycle of medicines », EMA, News, 19 July 2023, (Consulté le 05/06/2024).
[75] *Ibid.*
[76] *Ibid.*
[77] FDA, Center for Drug evaluation and research, « Artificial Intelligence in Drug Manufacturing », Discussion Paper 2023, 17p.
[78] FDA, « Using Artificial Intelligence & Machine Learning in the Development of Drug & Biological Products », Discussion Paper ad Request for Feedback, 2023, 33p.

consultation à ce sujet, ouverte de mai à août 2023[79].

Fort du constat des avantages que l'IA peut apporter pour optimiser le cycle de vie du médicament en permettant l'obtention de données probantes, l'EMA contribue activement à l'élaboration d'un encadrement suffisant pour le déploiement de ces méthodes comme l'illustre ce premier travail.

Nous soulignons que l'EMA établit une définition de l'IA, qualifiée de « systèmes qui affichent un comportement intelligent en analysant leur environnement et en prenant des mesures –avec un certain degré d'autonomie- pour atteindre des objectifs spécifiques »[80], qui diffère de celle qui avait été établie dans la proposition de règlement sur l'Intelligence Artificielle (*AI Act*)[81].

Ainsi, dans ce papier, l'EMA aborde une approche par le risque qui est pensée par étape. Ces premières réflexions concernent alors les technologies d'IA utilisées, les contextes d'utilisation ainsi que le degré d'influence de l'innovation, et ce, tout au long du cycle de vie du médicament[82]. Les utilisations qui peuvent en être faites sont nombreuses. En effet, l'IA apparaît être un réel outil prometteur pour le développement non clinique d'une molécule utilisée par exemple pour approfondir les connaissances sur la toxicité ; accélérer la découverte et la sélection de molécules ; identifier des biomarqueurs ou bien encore raffiner, réduire et remplacer le recours aux animaux[83]. La recherche clinique pour le développement des médicaments à usage humain bénéficie également de ces méthodes pour sélectionner des participants aux essais cliniques ; créer de cohortes virtuelles ; aider à la prise de décision en adaptant le dosage, le design voire les paramètres cliniques d'un essai[84]. L'obtention d'informations est alors accélérée par le recours à l'IA qui apporte un soutien dans les dossiers de demande d'autorisation de mise sur le marché des produits. Enfin, l'IA est également utile lors des phases post-autorisation en permettant la mise en place d'outils de suivis performants[85].

À travers la prise en compte des différentes utilisations de l'IA dans le cycle de vie du médicament et du risque associé à celles-ci, l'EMA identifie des interactions réglementaires inévitables entre les règles en vigueur pour la recherche et le développement pharmaceutique, celles encadrant les technologies numériques ou bien encore les procédures d'avis scientifiques concernant les nouvelles méthodologies pour le développement de

[79] *Op. cit.,* p 1.

[80] « Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle », *op. cit.,* [Notre traduction] : « systems displaying intelligent behaviour by analysing data and 47 taking actions with some degree of autonomy to achieve specific goals – », lignes 47-48.

[81] Il s'agit d'un « 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 » (au sens de « système d'intelligence artificielle »), v. amendements du Parlement européen adoptés le 14 juin 2023 à la 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 (*COM(2021)*0206 – C9-0146/2021 –2021/0106(COD)), P9_TA(2023)0236, spéc. amendement 3 (1).

[82] « Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle », *op. cit.,* lignes 117-187.

[83] FABRE Isabelle, « Les méthodes substitutives à l'expérimentation animale », *Bulletin de l'Académie Vétérinaire de France*, n°8, 2009, p 1783-1791.

[84] BAJARD Agathe *et al.,* « An in silico approach helped to identify the best experimental design, population, and outcome for future randomized clinical trials », *Journal of Clinical Epidemiology*, 2015.

[85] DUGUET Anne-Marie, « The place of digital and artificial intelligence in Medical research », *in* ZIMA Thomas et WEISSTUB David N. (dirs.), *Medical research ethics: challenges in the 21st century*, Editors Philosophy and medicine, vol. 132, Springer, January 2023, p.476.

médicaments à usage humain[86]. En outre, la gouvernance des données[87], leur protection[88], les aspects liés à l'intégrité des données et de la recherche[89] ainsi que les aspects éthiques[90] du déploiement d'une IA digne de confiance[91] doivent obligatoirement être pensés. En effet, le déploiement de l'IA nécessite le traitement d'un grand nombre de données, accentuant les risques pour leur protection et celle de la vie privée[92]. En outre, un grand nombre de chercheurs s'accordent sur les biais et erreurs induits par l'IA[93], qui pourraient alors se répercuter sur la recherche. Le recours à l'IA dans le développement des médicaments doit ainsi être pensé de manière responsable et large, en partant des données utilisées pour l'élaboration des systèmes d'IA, jusqu'aux aux conséquences que ces nouvelles méthodes peuvent avoir sur la recherche ; et ce en gardant notamment à l'esprit les principes bioéthiques fondamentaux que sont la bienfaisance, la non malfaisance, la justice et l'équité[94]. De même, des aspects techniques sont considérés tels que les modalités de développement du modèle d'IA, l'évaluation de ses performances dans un contexte d'utilisation précis, l'interprétabilité et l'explicabilité de l'IA ainsi que les conditions de déploiement du modèle[95]. Le modèle d'IA développé doit être robuste et approprié à l'étape pour laquelle il est utilisé.

Par ailleurs, les risques associés aux modèles d'IA peuvent particulièrement être induits par le jeu de données qui l'alimente. Dès lors, il importe de contrôler les modalités d'acquisition et d'augmentation des données afin de prévenir de biais potentiels[96].

Finalement, même s'il est possible de s'interroger sur la réelle compétence de l'EMA en ce qui concerne certains aspects de ce document, notamment la dimension éthique de l'utilisation de l'IA dans le cycle de vie du médicament[97], l'Agence participe ici au déploiement de réflexions essentielles pour penser une utilisation de l'IA adaptée aux objectifs de sûreté et d'efficacité des médicaments dans l'Union. L'EMA aborde aussi la question de l'articulation des diverses normes éthiques, techniques, scientifiques et réglementaires applicables. L'enjeu de ces premières réflexions devrait alors être l'élaboration de futures orientations réglementaires qui nécessiteront cependant de faire appel à des experts qualifiés afin de garantir une interaction réglementaire et un accompagnement suffisant pour l'utilisation de l'IA dans le cycle de vie du médicament. De plus, la collaboration apparaît être un élément essentiel, non seulement pour permettre l'accès aux données mais également pour couvrir les différents éléments d'attention d'une utilisation acceptable de l'IA. En effet, d'autres acteurs -différents de ceux de la

[86] « Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle », *op. cit.,* lignes 233-254.
[87] *Ibid.*, lignes 358-362.
[88] *Ibid.*, lignes 363-381.
[89] *Ibid.*
[90] *Ibid.*
[91] Groupe d'experts de haut niveau sur l'intelligence artificielle, « Lignes directrices en matière d'éthique pour une IA digne de confiance », Avril 2019.
[92] RIAL-SEBBAG Emmanuelle, « CHAPITRE 4 : La gouvernance des big data utilisées en santé, un enjeu national et international », *in Journal international de bioéthique et d'éthique des sciences. Données de masse en santé*, éd. Alexandre Lacassagne, coll. « Diffusion ESKA », vol. 28, n°3, Septembre 2017, p.45.
[93] ZUIDERVEEN BORGESUIS Frederik, *Discrimination, intelligence artificielle et décisions,* Conseil de l'Europe, 2018.
[94] BEAUCHAMP Tom L. et CHILDRESS James F., *Principles of Biomedical Ethics*, Oxford University Press, New York, 1994.
[95] « Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle », *op. cit.,* lignes 297-357.
[96] *Ibid.*, lignes 255-296.
[97] Extrait des commentaires de l'appel à consultation adressés par le groupe « Éthique du numérique, de la robotique et de l'IA » de la Chaire UNESCO « Ethique, science et société », déposés le 29 décembre 2023.

recherche - apparaissent essentiels pour l'élaboration, l'utilisation, le contrôle et la vérification de l'IA dans les différentes étapes de développement des médicaments. Ces inévitables collaborations vont certainement mener à un élargissement des acteurs de la recherche. De même, les Comités d'éthique de la recherche seront amenés à penser différemment le processus d'élaboration et d'évaluation de la recherche – étape essentielle dans le cycle de vie du médicament à usage humain. Or, ces derniers ne sont pas mentionnés dans cette première version du papier de réflexion.

Reste à voir quelles seront les prochaines étapes et échéances de ce document qui devrait avoir intégré les différents commentaires formulés auparavant. L'EMA, tout comme la Commission européenne, doivent ainsi considérer l'ensemble de ces nouveaux enjeux, autant que faire se peut, afin de garantir un déploiement sûr et acceptable de l'innovation dans le domaine sensible du médicament.

Résolution législative du Parlement européen du 24 avril 2024 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))

par Lisa FERIOL

Doctorante CIFRE, Ekitia et Equipe BIOETHICS, CERPOP UMR1295
Inserm et Université Toulouse Paul Sabatier

Introduction

La stratégie européenne pour les données présentée par la Commission européenne en février 2020[98] a permis de structurer les actions de l'Union européenne afin d'améliorer la circulation des données au sein du marché européen de manière conforme aux valeurs de l'Union européenne, notamment pour lutter contre les modèles développés par les géants du web. Cette stratégie ambitionne de créer, à travers différents règlements européens[99], un cadre de gouvernance harmonisé permettant de faciliter l'accès et le partage de différents types de données, personnelles comme non-personnelles, entre les Etats membres et au-delà de l'Union selon les règles fixées par ces textes. Cette approche transsectorielle dite « horizontale » est complétée par une approche sectorielle visant à créer onze espaces communs de données dans des secteurs d'activité identifiés comme clés par la Commission européenne (mobilité, énergie, culture, industrie…)[100]. L'objectif est ici de faciliter l'accès aux données pour les citoyens, permettre la réutilisation des données pour bénéficier de leur potentiel et encadrer et harmoniser ces échanges dans le respect des règles européennes en matière de protection des données et de droit de la concurrence. Dans ce contexte, la santé a été identifiée comme secteur prioritaire et fera l'objet de la création du premier espace européen commun de données. La création de l'Espace européen des données de santé (EEDS)[101] participe à l'ambition plus large affichée par l'Union européenne de créer une véritable « Union européenne de la santé »[102], notamment en s'appuyant sur les possibilités offertes par le numérique en matière de santé pour renforcer la

[98] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2022 portant sur « Une stratégie européenne pour les données », *COM(2020)* 66 final. V. aussi, site de la Commission européenne, « Stratégie européenne pour les données de santé ».

[99] Comme notamment le *Data Governance Act* (v. règlement n° 2022/868/UE du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement n° 2018/1724/UE (règlement sur la gouvernance des données), *JOUE* n° L 152 du 3 juin 2022), l'*Artificial Intelligence Act* (v. proposition de règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, *COM(2021)* 206 final -), le *Digital Markets Act* (règlement n° 2022/1925/UE du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives n°s 2019/1937/UE et /UE (règlement sur les marchés numériques), *JOUE* n° L 265 du 12 octobre 2022) ou encore le *Digital Services Act* (v. règlement n° 2022/2065/UE du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive n° 2000/31/CE (règlement sur les services numériques), *JOUE* n° L 277 du 27 octobre 2022).

[100] « Espaces européens communs de données », site de la Commission européenne.

[101] Souvent également désigné par « European Health Data Space » ou l'acronyme « EHDS »

[102] « Union européenne de la santé : protéger notre santé ensemble », site de la Commission européenne.

souveraineté de l'Union en matière de numérique en santé, du fait de l'accélération à l'échelle mondiale de ce marché et des importants enjeux économiques que ce domaine représente.

À ce sujet, le futur règlement sur l'Espace européen des données de santé affiche trois grands objectifs :

- poursuivre les efforts pour permettre la circulation des données de santé au sein de l'Union européenne au service des citoyens et patients européens en donnant le contrôle à ces derniers sur leurs données de santé (utilisation primaire) ;
- promouvoir un véritable marché unique des systèmes de dossiers médicaux électroniques ;
- faciliter l'accès aux données de santé existantes au profit de finalités encadrées (utilisation secondaire) grâce à l'élaboration d'un système cohérent, fiable et efficace[103].

Les motivations à la création de cet Espace européen des données de santé sont multiples : la crise de la Covid-19 a bien mis en lumière les obstacles existants à la coopération des États membres et à l'accès aux données de santé pertinentes ; les objectifs fixés par la directive de 2011 sur les soins transfrontaliers[104] n'ont pas été atteints rendant nécessaire une harmonisation des règles afin de pouvoir offrir aux citoyens européens une continuité des soins au sein de l'Union européenne ; les données de santé et ce qu'elles impliquent représentent une réelle opportunité pour le marché européen du fait du potentiel économique immense qu'elles représentent ; les modèles du géant du web posent de véritables interrogations en matière de préservation des droits, libertés et intérêts des citoyens européens alors que les données de santé sont des données sensibles.

L'accès et le partage des données de santé étaient jusque-là principalement encadrés par les dispositions du Règlement Général sur la Protection des Données (RGPD)[105] complétées par les lois nationales. Le RGPD définit les données de santé comme appartenant à la catégorie des données à caractère personnel particulières[106], prévoyant un principe d'interdiction de traitement auquel des exceptions sont prévues. Le futur règlement sur l'Espace européen des données de santé (EEDS)[107] vient préciser et compléter les modalités d'accès et de partage des données de santé, ainsi que les droits individuels prévus par le RGPD, en matière d'utilisation primaire et secondaire des données de santé électroniques personnelles[108]. Là où le RGPD concentrait son approche sur la protection des données personnelles en organisant leur circulation, le futur règlement semble se concentrer sur la valorisation du potentiel des données de santé existantes et disponibles au sein de l'Union européenne tout en assurant leur protection, et ceci au profit du soin et de la recherche. Il est intéressant de souligner que le périmètre du règlement est plus large que celui du RGPD puisqu'il couvre les données de santé électroniques à caractère personnel[109], ainsi que les données de santé

[103] « Espace européen des données de santé », site de la Commission européenne.
[104] Directive n° 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* n° L 88 du 4 avril 2011.
[105] Règlement n° 2016/679/UE 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 n° 95/46/CE (règlement général sur la protection des données, ci-après « RGPD »), *JOUE* n° L° 119 du 4 mai 2016.
[106] Article 9, paragraphe, RGPD, *op. cit.*
[107] Résolution législative du Parlement européen du 24 avril 2024 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), ci-après « REEDS ».V. aussi, position du Parlement européen arrêtée en première lecture le 24 avril 2024 en vue de l'adoption du règlement n° 2024/… du Parlement européen et du Conseil relatif à l'espace européen des données de santé, P9_TC1-COD(2022)0140.
[108] Article 1, paragraphe 2, sous a), REEDS, *op. cit.*
[109] *Ibid.*

électroniques non-personnelles[110] (données anonymisées). Les bénéfices attendus par ce règlement doivent autant concerner les patients et citoyens que les professionnels concernés (professionnels de santé, chercheurs, industriels…). Quant à sa base juridique, il s'appuie sur l'article 16 du Traité sur le Fonctionnement de l'UE (TFUE) (protection des données à caractère personnel) et l'article 114 du TFUE (fonctionnement du marché intérieur). On notera que l'article 168 du TFUE, base juridique « Santé publique » n'a pas été ici mobilisé.

Le règlement prévoit des règles communes, des standards, des infrastructures et un cadre de gouvernance visant à faciliter l'accès aux données de santé électroniques à des fins d'utilisation primaire et secondaire[111]. Il introduit de nouvelles qualifications pour les acteurs du domaine de la santé emportant de nouvelles obligations (utilisateurs de données de santé, détenteurs de données de santé), et crée de nouveaux organes de gouvernance afin de structurer les mécanismes prévus par ce futur règlement (organisme d'accès aux données de santé, EHDS Board, forum des parties prenantes…). Ce cadre doit permettre de favoriser la confiance des différentes parties prenantes à cette stratégie – confiance décrite comme facteur fondamental du succès de l'Espace européen des données de santé[112].

Ce commentaire vise à présenter les mécanismes prévus par le futur règlement sur l'Espace européen des données de santé (REEDS) afin d'améliorer l'utilisation primaire et secondaire des données de santé au sein de l'Union européenne[113].

I. LES DISPOSITIONS DU FUTUR RÈGLEMENT EN MATIÈRE D'UTILISATION PRIMAIRE DES DONNÉES DE SANTÉ (CHAPITRE II DU FUTUR RÈGLEMENT)

Afin d'atteindre les objectifs en matière d'utilisation primaire des données, le futur règlement vient préciser les données de santé visées par cet objectif (**A**), les droits associés des personnes concernées (**B**) ainsi que la gouvernance des mécanismes prévus au niveau européen et national (**C**).

A. Données de santé concernées par l'utilisation primaire

Le futur règlement prévoit des catégories prioritaires de données personnelles de santé pour l'utilisation primaire, comme notamment les comptes rendus médicaux, les prescriptions électroniques, les imageries médicales, ou encore les résultats d'examens médicaux. Les Etats membres pourront prévoir d'ajouter des catégories de données concernées par les dispositions sur l'utilisation primaire[114]. Afin de garantir l'interopérabilité des dossiers médicaux électroniques assurant l'accès aux données de santé nécessaires dans le cadre de l'utilisation primaire, des règles sont prévues sur l'enregistrement des données de santé dans un format électronique interopérable[115]. En effet, l'article 6 du futur règlement prévoit l'établissement par la Commission européenne d'un format européen d'échange de dossiers de santé électroniques afin de fixer des standards d'interopérabilité en la matière permettant la circulation de ces dossiers.

B. Droits des personnes concernées quant à l'utilisation primaire de leurs données

Le futur règlement prévoit un droit d'accès des personnes physiques à certaines de leurs

[110] *Ibid.*, article 2, paragraphe 2, sous b).
[111] *Ibid.*, article 1, paragraphe 1, sous 1).
[112] « Espace européen des données de santé », site de la Commission européenne.
[113] Ce commentaire se base sur la version votée par le Parlement européen le 24 avril 2024[113], les références sont donc susceptibles d'être modifiées. Le texte final sera prochainement voté par le Conseil de l'Union européenne.
[114] Article 5, paragraphe 1, REEDS, *op. cit.*
[115] *Ibid.*, article 7, REEDS.

données de santé[116] dans un format facilement lisible et accessible. Ce droit d'accès comprend en fait pour les personnes physiques concernées ou leurs représentants le droit de télécharger une copie électronique des données *a minima,* désignées comme « prioritaires ». Les Etats membres peuvent restreindre la portée de ce droit lorsque cela est nécessaire pour la protection des personnes physiques (sécurité des patients, motifs éthiques), jusqu'à ce qu'un professionnel de santé puisse communiquer et expliquer de manière adaptée à la personne physique concernée les informations susceptibles d'avoir un impact significatif sur sa santé[117]. De même, le futur règlement impose aux Etats membres de veiller à ce qu'un ou plusieurs services gratuits d'accès aux données électroniques de santé pour les personnes physiques et leurs représentants soient mis en place au niveau national, régional ou local, pour permettre aux personnes d'accéder à leurs données de santé et d'exercer leurs droits prévus par le règlement. Ces services d'accès devront veiller à être accessibles aux personnes handicapées, aux groupes vulnérables ou aux personnes ayant une faible culture numérique.

Les personnes physiques pourront également insérer des informations dans leur propre dossier médical électronique[118] par l'intermédiaire des services d'accès ou à travers des applications liées à ces services – à l'instar de ce qui est prévu pour « Mon Espace Santé » en France. Les informations directement insérées par les personnes physiques ou leurs représentants sont clairement identifiées et les personnes ne peuvent modifier les informations insérées par les professionnels de santé. Cependant, il est prévu que les personnes pourront rectifier les données de santé en vertu de l'application de l'article 16 du RGPD, auprès des services d'accès prévus par les Etats membres, sous réserve de vérification par un professionnel de santé compétent[119]. Le futur règlement vient aussi préciser et spécifier pour l'utilisation primaire des données les dispositions en matière de droit à la portabilité prévues par le RGPD, lequel limite ce droit aux données traitées sur la base du consentement ou du contrat)[120]. Notamment, les personnes physiques peuvent demander à un prestataire de soins de santé de transmettre tout ou partie de leurs données de santé à un autre prestataire de leur choix, immédiatement et gratuitement, et ceci même si les prestataires de soins de santé sont situés dans des États membres différents en prenant appui sur l'infrastructure transfrontalière « MaSanté@UE ». Cette transmission peut être demandée et envoyée auprès de la Sécurité sociale ou des services de remboursement. La précision des dispositions sur le droit à la portabilité des données est donc concentrée sur l'utilisation primaire des données, il aurait pu être intéressant de préciser ces dispositions pour l'utilisation secondaire et notamment en ce qui concerne l'altruisme en matière des données[121].

Le futur règlement ouvre la possibilité pour les personnes physiques de restreindre l'accès à des professionnels de santé et des prestataires de soin de santé à tout ou partie de leurs données électroniques de santé concernées par l'utilisation primaire, en étant informées des incidences que cela peut

[116] Article 8b, REEDS, *op. cit.*
[117] *Ibid.*
[118] *Ibid.*
[119] *Ibid.*, article 8c.
[120] *Ibid*, article 8d.
[121] L'altruisme en matière de données est une notion introduite par le *Data Governance Act* à son chapitre V et qui est défini par l'article 2, point 16, comme étant « : le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel 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 (…) par exemple les soins de santé (…) ou la recherche scientifique dans l'intérêt général. »

avoir sur leur prise en charge médicale[122]. Il est également prévu un droit d'obtenir des informations sur l'accès aux données (personnes ayant eu accès aux données, date et heure d'accès, données de santé auxquelles la personne a accédé) de manière gratuite et sans délai par l'intermédiaire des services d'accès électronique aux données de santé, pendant au moins 3 ans après chaque accès aux données[123].

Les États membres pourront prévoir la possibilité pour les personnes physiques de s'opposer, dans leur droit national et de manière réversible, à l'accès à leurs données de santé enregistrées dans un dossier médical électronique par l'intermédiaire des services d'accès aux données de santé prévus par le futur règlement. En tout état de cause, il sera toujours possible que les prestataires de soins ou professionnels de soins accèdent aux données de santé concernées pour protéger les intérêts vitaux de la personne en question ou d'une autre personne physique[124].

Le règlement précise les règles concernant l'accès des professionnels de santé aux données de santé[125], ainsi que des règles sur la gestion de l'identification des personnes utilisant les services d'accès aux données de santé, en s'appuyant sur ce qui est prévu par l'article 6 du règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE[126].

Concernant la compensation pour la mise à disposition des données de santé disponibles, le prestataire destinataire ne sera pas tenu de rémunérer le prestataire de soins de santé. Il est également prévu que ne pourront être demandés par un prestataire de soins de santé ou un tiers aux personnes concernées une redevance, une compensation ou des frais pour le partage ou l'accès aux données[127].

C. Gouvernance de l'utilisation primaire

Afin d'organiser la gouvernance des modalités de circulation des données de santé au profit du soin à l'échelle de l'Union, le futur règlement impose la désignation d'autorités au niveau des États membres (**1**) ainsi que la participation obligatoire à l'infrastructure européenne « MaSanté@UE » coordonnant les différentes autorités nationales (**2**).

1. Désignation par les États membres d'une ou plusieurs autorités de santé numérique

Afin de pouvoir coordonner à l'échelle nationale la mise en place de ces mécanismes d'utilisation primaire des données, chaque État membre devra désigner une ou plusieurs autorités de santé numérique[128], déclarées à la Commission européenne. De manière générale, ces autorités de santé numérique devront contribuer au développement, à l'échelon local, régional et national, de solutions techniques pour les infrastructures et renforcer les capacités nationales de mise en œuvre de l'interopérabilité et de la sécurité de l'utilisation primaire de manière collaborative avec les différentes parties prenantes concernées (comprenant notamment les représentants des patients, les prestataires de soins de santé ou encore les représentants des professionnels de santé). Ces autorités de santé numérique devront agir dans l'intérêt public et en toute indépendance. Elles devront rendre un rapport d'activité bisannuel[129] contenant un aperçu complet de leurs activités – comprenant notamment la description des mesures prises pour mettre en place le règlement, le pourcentage de personnes physiques ayant eu accès aux données de

[122] Article 8e, REEDS, *op. cit.*
[123] *Ibid.*, article 8f.
[124] *Ibid.*, article 8h. S
[125] *Ibid.*, articles 9a et 9b.
[126] *JOUE* n° L 267/73 du 28 août 2014.
[127] Article 9a, REEDS, *op. cit.*
[128] *Ibid.*, article 10.
[129] *Ibid.*, article 10a.

santé visées par le règlement, ou encore les volumes de données de santé partagées à travers les frontières par l'intermédiaire de « MaSanté@UE ». Ces autorités de santé numérique pourront également recevoir des plaintes formulées par les personnes physiques de manière individuelle ou collective concernant l'éventuelle méconnaissance de leurs droits prévus par le règlement en matière d'utilisation primaire des données. Une coopération entre les États membres sera prévue en cas de plainte liée à l'échange transfrontalier de données de santé[130]. A noter que les autorités de contrôle prévues par le RGPD restent compétentes pour le suivi et l'exécution des dispositions conférant des droits aux individus en matière d'utilisation primaire des données de santé[131].

2. Infrastructure transfrontalière pour l'utilisation primaire des données de santé électroniques : « MaSanté@EU » (« MyHealth@EU)

Afin de permettre, d'une part, la coordination des différentes autorités de santé numérique désignées comme point de contact national par chaque État membre à l'échelle de l'Union européenne, et d'autre part, la circulation des données de santé entre les États membres, une participation des autorités de santé numérique à l'infrastructure transfrontalière MaSanté@UE (MyHealth@EU) est rendue obligatoire pour l'utilisation primaire des données personnelles de santé. Le futur règlement va donc plus loin que ce qui avait été prévu par la Directive 2011 sur les soins transfrontaliers[132]. Cette infrastructure déjà existante et mise en place par la Commission européenne vise à fournir des services destinés à soutenir et à faciliter l'échange de données personnelles de santé entre les différents points de contacts nationaux. La Commission européenne adoptera, au moyen d'actes d'exécution, les mesures nécessaires au développement technique de MyHealth@EU (règles concernant la sécurité, confidentialité et la protection des données électroniques de santé à caractère personnel, conditions des contrôles de conformité nécessaires pour participer à MyHealth@EU, exigences en matière de cybersécurité, interopérabilité technique, sémantique, etc.). Dans ce cadre, les États membres ont la responsabilité de vérifier que les différents acteurs concernés par cette plateforme puissent s'y connecter et accéder aux fonctionnalités (prestataires de soins de santé, fournisseurs de soins de santé connectés) et que les pharmacies opérant sur le territoire soient en mesure de délivrer des prescriptions électroniques émises par d'autres États, auxquelles elles accèdent par l'intermédiaire de MyHealth@EU. Conformément à ce qui a été défini par la Commission européenne dans les actes d'exécution prochainement adoptés[133], les États membres pourront décider de fournir, par l'intermédiaire de cette plateforme, des services supplémentaires (comme par exemple la télémédecine, les applications de santé, les services de traduction des données de santé, …).

Par ailleurs, au-delà des points de contact nationaux en matière de santé numérique, d'autres infrastructures pourront devenir des participants autorisés à MyHealth@EU dans les conditions définies par la Commission et les États membres (comme par exemple les systèmes de gestion clinique des patients (CPMS), ou autres services ou infrastructures dans les domaines de la santé, des soins ou de la sécurité sociale). Un point de contact national d'un pays tiers ou un système établi au niveau international pourront devenir un participant autorisé à MyHealth@EU, à condition de respecter les exigences imposées par le futur règlement, en particulier les exigences fixées par le

[130] *Ibid*., article 11.
[131] *Ibid.*
[132] Directive n° 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *op. cit*.
[133] Article 13, REEDS, *op. cit.*

chapitre V du RGPD relatif aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales[134].

II. LES DISPOSITIONS EN MATIÈRE DE SYSTÈMES DE DOSSIERS MÉDICAUX ÉLECTRONIQUES (DME) ET APPLICATIONS DE BIEN-ÊTRE (CHAPITRE III DU FUTUR RÈGLEMENT)

L'objectif du règlement sur ce point est de créer un marché des dossiers médicaux électroniques (DME) avec un premier niveau d'harmonisation autour de deux axes d'exigences : interopérabilité et traçabilité des accès[135] (**A**). Les exigences en matière d'applications de bien-être sont également mentionnées dans ces dispositions (**B**) ; ce qui permettra de créer une base de données européenne des DME et applications de bien-être conformes au règlement (**C**).

A. Dispositions relatives aux dossiers médicaux électroniques (DME)

1. Obligations des opérateurs économiques en ce qui concerne l'interopérabilité et la traçabilité de l'accès au système de DME

Les fabricants de systèmes de DME pourront accéder au marché de l'Union si leur produit respecte les exigences d'interopérabilité et de traçabilité des accès[136] et les obligations fixées par le futur règlement[137]. Des dispositions spécifiques sont prévues pour les importateurs de systèmes de DME en matière de mise sur le marché de ces derniers[138], ainsi que pour les distributeurs qui souhaitent mettre à disposition un système de DME sur le marché[139].

Les fabricants devront établir une documentation technique[140] avant la mise sur le marché ou la mise en service du DME et la tenir à jour afin de pouvoir démontrer que le système de DME satisfait aux exigences essentielles. Toutes les informations nécessaires permettant d'évaluer la conformité du système de DME devront être fournies aux autorités de surveillance du marché.

La conformité est vérifiée par une procédure d'auto-certification des logiciels de DME, dispositifs médicaux et d'IA connectés à ces DME sur la base de plusieurs exigences : transparence à la charge des industriels (publication de documentation), obligation de recourir à un environnement de test numérique européen[141] mis en place par la Commission européenne (logiciel mis en open-source), publication des résultats et contrôle par une autorité de surveillance du marché. Le fabricant démontre à travers une déclaration de conformité de l'UE[142] (modèle uniforme établi par la Commission) qu'il respecte les exigences essentielles fixées en la matière[143]. En établissant cette déclaration de conformité, le fabricant assume la responsabilité de la conformité du système de DME aux exigences fixées par le futur règlement lors de la mise sur le marché ou de sa mise en service[144]. Un marquage « CE » est apposé avant la mise sur le marché du système de DME[145].

2. Exigences nationales en matière de DME

Au-delà des exigences harmonisées en partie par l'Union (interopérabilité et traçabilité des accès), les Etats membres

[134] Chapitre V Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, RGPD, *op. cit*
[135] Article 13a, REEDS, *op. cit.*
[136] *Ibid.*, article 13b.
[137] *Ibid.*, article 17.
[138] *Ibid.*, article 19.
[139] *Ibid.*, article 20.
[140] *Ibid.*, article 24.
[141] *Ibid.*, article 26.
[142] *Ibid.*
[143] *Ibid.*, Annexe sur les « Exigences essentielles pour les composants harmonisés des systèmes de DSE et les produits revendiquant l'interopérabilité avec les systèmes de DME ».
[144] *Ibid.*, article 26, paragraphe 4.
[145] *Ibid.*, article 27.

pourront introduire des exigences nationales pour les systèmes de DME ainsi que des dispositions sur l'évaluation de leur conformité à ces règles nationales (par exemple les règles relatives à la sécurité ou à l'éthique). Les États membres en informeront la Commission européenne[146].

3. Surveillance du marché des systèmes de DME

En outre, le règlement n° 2019/1020/UE relatif à la surveillance du marché et la conformité des produits[147] s'applique aux systèmes de DME au regard des exigences fixées par le futur règlement et les risques qu'ils présentent. En la matière, les Etats membres désignent la ou les autorités de surveillance du marché chargées de la surveillance des DME, qui peuvent être les autorités de santé numérique prévues par le futur règlement en veillant à éviter tout conflit d'intérêt[148]. Un partage des compétences avec les autres autorités de surveillance est prévu pour notamment les systèmes d'IA à haut risque ou encore les dispositifs médicaux de diagnostics in vitro[149]. Le futur règlement envisage des dispositions sur le traitement des risques posés par les systèmes de DME, des incidents graves[150] et des cas de non-conformité[151].

B. Dispositions relatives aux applications de bien-être

Un étiquetage (label) des applications de bien-être sera prévu pour les cas où un fabricant d'une application de bien-être revendiquerait l'interopérabilité avec un système de DME en ce qui concerne les composants harmonisés des systèmes de DME établis par le futur règlement[152]. Il s'agit d'une procédure d'auto-labellisation. La validité du label ne pourra excéder 3 ans. Les autorités de surveillance du marché vérifieront la conformité aux exigences fixées par le règlement à son annexe II.
Le partage ou la transmission des données du DME avec l'application de bien-être reconnue comme interopérable ne pourra se faire qu'avec le consentement de la personne physique concernée. Les fabricants devront laisser la possibilité à l'utilisateur de choisir les catégories de données de santé de l'application de bien-être qu'ils souhaitent insérer dans le système de DME et les circonstances de ce partage ou de cette transmission[153].

C. Base européenne de données des DME et applications de bien-être conformes au règlement

Une base de données à l'échelle de l'UE accessible au public est prévue afin de répertorier les informations sur les systèmes de DME pour lesquels une déclaration UE de conformité a été délivrée ainsi que celles sur les applications de bien-être labellisées[154]. Les systèmes de DME doivent être enregistrés dans cette base de données avant leur mise sur le marché ou en service.

III. DISPOSITIONS SUR L'UTILISATION

[146] *Ibid.*, article 27a.
[147] Règlement n° 2019/1020/UE du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive n° 2004/42/CE, et les règlements n°s 765/2008/CE et n° 305/2011/UE, *JOUE* n° L°169/1 du 25 juin 2019.
[148] Article 28, paragraphe 3, REEDS
[149] Article 93 du règlement n° 2017/745/UE du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive n° 2001/83/CE, le règlement n° 178/2002/CE et le règlement n° 1223/2009/CE et abrogeant les directives du Conseil n°s 90/385/CEE et 93/42/CEE (*JOUE* n° L 117 du 5 mai 2017), article 88 du règlement n° 2017/746/UE du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive n° 98/79/CE et la décision n] 2010/227/UE de la Commission (*JOUE* n° L 117 du 5 mai 2017), et article 59 de la proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'Intelligence Artificielle (COM/2021/206).
[150] Article 29, REEDS, *op. cit.*
[151] *Ibid.*, article 30.
[152] *Ibid.*, article 31.
[153] *Ibid.*, article 31a.
[154] *Ibid.*, article 32.

SECONDAIRE DES DONNÉES ÉLECTRONIQUES DE SANTÉ

Afin de favoriser l'utilisation des données de santé existantes pour des finalités autres que celles qui ont justifié leur collecte ou leur production[155] (désigné par l'expression d'« utilisation secondaire » ou « réutilisation des données de santé »), le futur règlement sur l'EEDS désigne les données concernées par cette utilisation secondaire ainsi que les finalités autorisées et interdites (**A**). Il introduit de nouveaux statuts pour les acteurs du numérique en santé ainsi que de nouvelles obligations pour les organismes d'accès aux données de santé[156], les détenteurs de données de santé[157] et les utilisateurs de données de santé[158] (**B**). Un système de gouvernance spécifique a dû être mis en place à cet effet (**C**).

A. Conditions générales relatives à l'utilisation secondaire des données électroniques de santé

1. Catégories de données de santé concernées par l'utilisation secondaire

Concernant les détenteurs de données de santé dont sont exclus les chercheurs individuels et les personnes physiques ainsi que les micro-entreprises (sauf dispositions contraires prévues par le droit national)[159], une obligation de mise à disposition des données de santé visées par le futur règlement[160] est prévue[161]. Sont visées des catégories minimales de données électroniques destinées à un usage secondaire, qui sont finalement particulièrement larges. On y trouve de manière non-exhaustive les données électroniques de santé provenant des DME, les données sur les facteurs ayant un impact sur la santé, y compris les facteurs socio-économiques, environnementaux et sociaux, ainsi que les déterminants comportementaux de la santé, les données administratives relatives aux soins de santé, les données génétiques, épigénomiques et génomiques humaines ou encore les données provenant d'application de bien-être. Sans oublier les registres de données de santé basés sur la population (registres de santé publique), les registres de mortalité ou encore les données provenant des dispositifs médicaux, les données de cohortes de recherche… ; catégories pouvant être complétées par des lois nationales. Il est intéressant de souligner que pour les données génétiques, épigénomiques et génomiques, les données moléculaires humaines (données omiques comme les protéomiques, transcriptomiques ou métabolomiques), les données provenant d'application de bien-être, les données de santé provenant de biobanques et les bases de données associées, les Etats membres pourront, après notification à la Commission européenne, introduire des mesures plus strictes et des garanties supplémentaires dans leur droit national du fait de la sensibilité particulière de ces données[162], comme notamment le recueil du consentement des personnes concernées.

2. Propriété intellectuelle et secrets

La mise à disposition des données devra se faire dans le respect des éventuels droits de propriété intellectuelle[163], des secrets commerciaux ou des dispositions règlementaires applicables en matière de médicaments applicables aux jeux de données visés. Ce sont les organismes d'accès aux données de santé (ci-après désignés par HDAB pour *Health Data Access Bodies*), qui prennent les mesures spécifiques, appropriées et proportionnées,

[155] *Ibid.*, article 2, paragraphe 2, sous e).
[156] *Ibid.*, article 36.
[157] *Ibid.*, article 2, paragraphe 2, sous y).
[158] *Ibid.*, article 2, paragraphe 2, sous z).
[159] *Ibid.*, article 32a.
[160] *Ibid.*, article 33.
[161] *Ibid.*, article 41.
[162] *Ibid.*, article 33, paragraphe 8, sous b).
[163] *Ibid.*, article 33a.

comprenant les mesures juridiques, organisationnelles et techniques jugées nécessaires (comme par exemple le requis d'accords contractuels entre les détenteurs et utilisateurs de données de santé). Ces dispositions ont fait l'objet de débat lors de la discussion du texte par le Parlement européen et le Conseil de l'UE qui sont venus détailler les conditions, là où la proposition de règlement de la Commission européenne ne prévoyait pas de modalités particulières à ce sujet.

3. Finalités autorisées pour l'utilisation secondaire des données de santé

Les finalités pour lesquelles les données de santé visées par le règlement peuvent être réutilisées sont fixées par l'article 34 du futur règlement. Elles comprennent de manière non exhaustive l'intérêt public dans le domaine de la santé publique et de la santé au travail, les politiques publiques, les statistiques, ou encore la recherche scientifique liée aux secteurs de la santé ou des soins. Les discussions sur le texte ont rattaché à la finalité de la recherche scientifique les finalités de développement et d'innovation de produits ou de services ainsi que la formation, le test et l'évaluation d'algorithmes (y compris dans les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro, les systèmes d'IA et les applications de santé numérique).

4. Finalités d'utilisation secondaire interdites

Le futur règlement considère également comme interdites certaines finalités d'utilisation secondaire[164] comme par exemple le fait de prendre des décisions préjudiciables à une personne physique ou à un groupe de personnes physiques ; d'offrir des conditions moins favorables pour la fourniture de biens ou de services (y compris les exclure de contrat d'assurance ou crédit) ; ou encore les activités contraires aux dispositions éthiques prévues par le droit national.

B. Les nouvelles qualifications introduites par le futur règlement en matière d'utilisation secondaire

1. Les organismes d'accès aux données de santé (ou HDAB pour « Health Data Access Bodies »)

Afin de pouvoir coordonner les actions et mécanismes imposés par le futur règlement à l'échelle des États membres, ces derniers devront désigner un ou plusieurs organismes d'accès aux données de santé (HDAB) (auquel cas un organisme coordinateur devra être nommé)[165]. Il est attendu de ces HDAB qu'ils coopèrent entre eux, avec la Commission, ainsi qu'avec les représentants des parties prenantes concernées telles que les autorités de contrôle compétentes en matière de protection des données. Les États membres devront assurer que ces organismes disposent des ressources humaines, financières et techniques, mais aussi de l'expertise, des locaux et des infrastructures nécessaires à l'accomplissement des tâches qui leur incombent. Tout conflit d'intérêt dans la répartition de ces tâches devra être évité. Le personnel, de son côté, sera tenu d'agir dans l'intérêt public et en tout indépendance[166] [167].

Les principales tâches de ces HDAB sont énumérées à l'article 37 de la proposition de règlement et comprennent le fait de statuer sur les demandes d'accès, d'autoriser et de délivrer les permis d'accès aux données. L'accès aux données de santé est permis dans un environnement de traitement sécurisé[168]. Le HDAB contrôlera et supervisera le respect des exigences qui pèse sur les utilisateurs et détenteurs de données de santé, et demandera aux détenteurs de données de santé l'accès aux données de santé visées par l'autorisation de données ou la demande de données

[164] *Ibid.*, article 35.
[165] *Ibid.*, article 36.
[166] *Ibid.*, article 36, paragraphe 3, sous a).
[167] *Ibid.*, article 36, paragraphe 3.
[168] *Ibid.*, article 50.

accordée. Ces organismes devront également prendre toutes les mesures nécessaires pour préserver la confidentialité des droits de propriété intellectuelle, la protection réglementaire des données, la confidentialité des secrets commerciaux en tenant compte des droits pertinents du détenteur et de l'utilisateur des données relatives à la santé[169].

Un article est dédié aux obligations des HDAB envers les personnes physiques concernées par le traitement de leurs données[170] : ils devront rendre de manière publique et accessible les conditions dans lesquelles les données de santé sont mises à disposition pour un usage secondaire en tenant compte de différentes informations imposées par le règlement[171].

Les HDAB devront aussi faciliter l'accès transfrontalier aux données de santé par l'intermédiaire de la plateforme HealthData@EU mais aussi coopérer au niveau de l'Union et au niveau national pour définir des normes communes, des exigences techniques et des mesures appropriées. Des mesures de transparence sont imposées aux HDAB, comme notamment l'obligation de rendre public par des moyens électroniques un catalogue national de l'ensemble des données concernées par le futur règlement qui sont mobilisables, les demandes et requêtes de données de santé, les autorisations données.

Les HDAB auront également des obligations de coopération de divers ordres[172] : coopération avec les autorités de contrôle mises en place par le RGPD et le comité de l'EEDS concernant les données personnelles, coopération avec les différentes parties prenantes (associations de patients, représentants des personnes physiques, professionnels de santé, comités éthiques…), coopération avec d'autres organismes nationaux compétents notamment ceux prévus par le *Data Governance Act*[173] ou le règlement sur l'IA[174].

Afin d'assurer un système de réutilisation des données de santé transparent, il incombera aux HDAB de publier selon un modèle harmonisé un rapport d'activité bisannuel, notamment sur son site internet de manière accessible au grand public[175]. Ce rapport doit notamment contenir les informations concernant les demandes reçues, les potentielles amendes administratives imposées, les informations sur le traitement des demandes formulées par des personnes physiques concernant l'exercice de leurs droits en matière de protection des données, une description de ses activités en matière d'engagement et de consultation des parties prenantes concernées de même que les informations concernant les publications de recherche ou les produits et services de santé numériques ayant mobilisés des données accessibles via l'EEDS.

Les HDAB seront dotés de missions de contrôle et de surveillance et auront, dans ce cadre, le droit de demander et recevoir toutes les informations nécessaires auprès des détenteurs et utilisateurs des données de santé pour vérifier le respect des dispositions prévues par le règlement[176]. En cas de non-respect constaté des dispositions prévues par le règlement, le HDAB pourra sanctionner l'utilisateur ou le détenteur de données de santé en l'excluant jusqu'à 5 ans, de tout accès pour une utilisation secondaire des données de santé au sein de l'EEDS. Les HDAB seront également habilités à infliger des amendes administratives proportionnées et

[169] *Ibid.*, article 37, paragraphe 1, sous f).
[170] *Ibid.*, article 37a.
[171] Comme par exemple les mesures techniques organisationnelles mises en place pour protéger les droits des personnes physiques ou encore les droits applicables aux personnes physiques en la matière et les modalités pour les exercer, ainsi que l'identité et les coordonnées du HDAB.
[172] *Ibid.*, article 37, paragraphe 2.
[173] Règlement sur la gouvernance des données, *op. ci.*
[174] Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), *op. cit.*
[175] Article 39, REEDS, *op. cit.*
[176] *Ibid.*, article 43.

dissuasives dont le montant sera fixé par le droit national au regard des dispositions prévues par le futur règlement[177]. En matière de manquement impliquant des données personnelles, les autorités de contrôle prévues par le RGPD resteront compétentes pour imposer des amendes administratives selon les dispositions prévues par le RGPD[178].

2. Les détenteurs de données de santé

Une qualification centrale introduite par la proposition de règlement est celle de « détenteurs de données de santé ». Ces derniers sont définis par la proposition de règlement comme étant « *toute personne physique ou morale, toute autorité publique, toute agence ou tout autre organisme du secteur de la santé ou des soins, y compris les services de remboursement le cas échéant, ainsi que toute personne physique ou morale qui développe des produits ou des services destinés aux secteurs de la santé, des soins ou des soins, qui développe ou fabrique des applications de bien-être, qui effectue des recherches en rapport avec les secteurs de la santé ou des soins ou qui fait office de registre de mortalité, ainsi que toute institution ou tout organisme de l'Union ou une agence qui a soit le droit ou l'obligation conformément au droit de l'Union applicable ou à la législation nationale de traiter des données électroniques de santé à caractère personnel pour la prestation de soins de santé ou de soins ou à des fins de santé publique, de remboursement, de recherche d'innovation, d'élaboration de politiques, de statistiques officielles, de sécurité des patients ou de réglementation, en sa qualité de responsable du traitement ou de coresponsable de traitement ou la capacité de mettre à disposition, y compris d'enregistrer, de fournir, de restreindre l'accès ou d'échanger des données électroniques non personnelles sur la santé, grâce au contrôle de la conception technique d'un produit ou des services connexes* ». On comprend alors que les acteurs qui seront concernés par cette qualification sont particulièrement nombreux allant des industriels, aux hôpitaux, aux cliniques, ou encore aux instituts de recherche.

La qualification des acteurs en tant que détenteurs de données de santé est loin d'être sans conséquence puisqu'il en découlera des obligations[179] de mise à disposition des données de santé pertinentes couvertes par le futur règlement sur demande du HDAB. Les données seront mises à disposition par le détenteur auprès du HDAB dans un délai de trois mois à compter de la réception de la demande du HDAB – avec possibilité de prolonger ce délai. Au-delà de cette obligation de mise à disposition, les détenteurs de données devront communiquer au HDAB, en la mettant à jour, une description de l'ensemble des données couvertes par le futur règlement qu'il détient. Concernant les données non-personnelles de santé, il est attendu des détenteurs de données qu'ils garantissent l'accès à ces données par l'intermédiaire de bases de données ouvertes fiables de manière illimitée.

3. Le détenteur de données de santé de confiance (DDSC) (« trusted health data holder »)

En sus, les discussions sur le texte ont introduit dans l'accord inter-institutionnel adopté par le Parlement une nouvelle catégorie d'acteurs qui est celle de détenteur de données de santé de confiance (DDSC)[180], pour laquelle est prévue une procédure simplifiée d'accès aux données qu'il détient, seulement dans le cas où la demande d'accès aux données ou la demande de données ne portent que sur les données de santé qu'il détient. Il appartiendra aux États membres d'établir une procédure permettant à des détenteurs de données de santé d'être reconnus DDSC. Cette procédure devra réunir, selon le règlement, plusieurs conditions comme le

[177] *Ibid.*, article 43a.
[178] *Ibid.*, article 43b.
[179] *Ibid.*, article 21.
[180] *Ibid.*, article 49.

fait de pouvoir donner accès aux données de santé dans un environnement de traitement sécurisé conforme aux exigences du futur règlement, de disposer de l'expertise nécessaire pour évaluer des demandes d'accès aux données de santé et des demandes de données de santé et de fournir les garanties nécessaires pour assurer le respect du règlement. La demande formulée uniquement à destination d'un détenteur de données de santé de confiance restera adressée au HDAB de l'Etat membre concerné ; ce dernier la transmettra au DDSC qui évaluera la demande au regard des critères fixés par le règlement et soumettra son évaluation ainsi qu'une proposition de décision à l'HDAB. Dans les deux mois suivants la réception de cette proposition, le HDAB prendra une décision sans être lié par la proposition formulée par le DDSC. En fonction de ce qui a sera décidé par le HDAB, le DDSC mettra à disposition les données dans l'environnement de traitement sécurisé qu'il détient ou fournira le résultat de la demande de données formulée. Les DDSC devraient permettre une simplification de l'accès aux données mais on ne saisit pas bien dans les dispositions du texte en quoi cela allège la charge qui pèse sur les HDAB.

4. Les utilisateurs de données de santé

Les utilisateurs de données de santé sont, quant à eux, définis comme « *toute personne physique ou morale comprenant les institutions, les organes ou agences de l'Union, à qui a été accordée un accès à des données de santé en vue d'une utilisation secondaire* »[181]. Cette qualification est assortie de devoirs[182] comme par exemple le fait de donner accès aux données uniquement aux personnes autorisées, de ne pas chercher à réidentifier les personnes concernées par les données de santé, de rendre publics les résultats sous format anonyme de l'utilisation secondaire des données de santé dans les délais impartis ou encore d'informer les HDAB de toute découverte importante concernant la santé de la personne physique concernées par les données auxquelles l'utilisateur a eu accès.

C. Gouvernance et mécanismes pour l'utilisation secondaire des données électroniques sur la santé

1. Les modalités d'accès aux données de santé pour une utilisation secondaire

Principe de minimisation et de limitation des finalités – Le futur règlement rappelle le principe de minimisation et de limitation des finalités qui consiste pour le HDAB à veiller à ce que l'accès aux données de santé soit adéquat, pertinent et limité à ce qui est nécessaire au regard de la finalité de traitement indiquée par l'utilisateur des données de santé[183] . Celle-ci consiste à privilégier, quand cela est possible, de fournir l'accès à des données de santé sous un format anonymisé.

Deux modalités d'accès prévues par le futur règlement : la demande d'accès aux données de santé[184] et la demande de données de santé[185] – *La demande d'accès aux données* consiste à demander à avoir accès à des données référencées dans le catalogue du HDAB concerné sous réserve de fournir les informations mentionnées par le futur règlement[186]. En cas de demande d'accès auprès de détenteurs de données de

[181] *Ibid.*, article 2, paragraphe 2, sous z).
[182] *Ibid.*, article 41a.
[183] Article 44 REEDS
[184] *Ibid.*, article 45.
[185] *Ibid.*, article 47.
[186] *Ibid.*, article 45, paragraphe 2 : notamment l'identité du demandeur, une explication détaillée de l'utilisation prévue et des avantages attendus de cette utilisation, une description des données de santé demandées, le format anonymisé ou pseudonymisé des données attendu, si applicable une description des données de santé détenues par l'utilisateur au sein de l'environnement de traitement sécurisé, une description des garanties proportionnées aux risques prévus pour prévenir toute utilisation abusive des données de santé ainsi que pour protéger les droits et intérêts du titulaire des données de santé y compris pour empêcher toute réidentification des individus concernés, etc.).

santé établis dans plusieurs États membres, une demande unique d'accès aux données devra être déposée auprès du HDAB de l'établissement principal du demandeur, celui de l'un des détenteurs de données ou par l'intermédiaire de l'infrastructure transfrontalière HealthData@EU[187]. Cette demande sera ensuite automatiquement transmise aux HDAB des Etats membres dans lesquels sont établis les détenteurs de données de santé concernés par la demande d'accès[188].

Une autorisation de traitement des données peut être délivrée par les HDAB lorsque les critères cumulatifs fixés par le futur règlement sont réunis[189]. A noter qu'en cas de demande d'accès aux données concernant différents États membres, une autorisation de traitement de données délivrée par un HDAB pourra bénéficier d'une reconnaissance mutuelle par les autres HDAB concernés. Le futur règlement établit à ce titre les éléments devant figurer dans l'autorisation de traitement des données. Ainsi, après la délivrance de ladite autorisation, le HDAB demandera immédiatement les données de santé au détenteur de données qui les mettra à la disposition de l'utilisateur dans un délai de deux mois au sein de l'espace de traitement sécurisé prévu par le HDAB. L'autorisation de traitement des données de santé sera délivrée pour la durée nécessaire à la réalisation des finalités demandées ; qui ne pourra excéder dix ans.

La demande de données de santé consiste pour sa part à la demande soumise à un HDAB d'obtenir une réponse sous forme de statistiques anonymes. Les informations à fournir par le demandeur seront naturellement moindre en comparaison à ce qui est exigé pour la demande d'accès aux données de santé (principalement l'identité du demandeur, explication détaillée de l'utilisation prévue de ces données, description des garanties prévues pour empêcher toute utilisation abusive des données de santé concernées). L'utilisateur n'aura pas accès aux données ayant permis de fournir ces résultats. Le HDAB évaluera la demande dans un délai de trois mois et fournira le résultat dans un délai de trois mois également. La Commission européenne définira au moyen d'actes d'exécution, les modèles de la demande d'accès aux données, ceux de l'autorisation de traitement des données et de demande de données de santé.

Redevances – Par ailleurs, une question qui a largement été discutée lors des négociations sur le texte est celle des redevances pour l'accès aux données de santé. En se conformant à la proposition de règlement, les HDAB (comprenant les services d'accès aux données de l'Union européenne ou les « détenteurs de données de santé de confiance ») pourront facturer des redevances pour la mise à disposition des données de santé électroniques en vue d'une utilisation secondaire[190]. Ces redevances devront être proportionnelles au coût de la mise à disposition des données, transparentes, et ne devront pas restreindre la concurrence, ni être discriminantes. Ce sont notamment les éléments pris en compte dans le calcul de ces redevances qui ont été discutés. L'accord inter-institutionnel[191] prévoit alors que ces redevances couvrent tout ou partie des coûts liés à la procédure d'évaluation d'une demande d'accès aux données ou demande de données, comprenant les coûts liés à la consolidation, la préparation, l'anonymisation, la pseudonymisation et la mise à disposition des données de santé. Des redevances réduites pourront être établies par les Etats

[187] *Ibid.*, article 52.
[188] *Ibid.*, article 45, paragraphe 3.
[189] *Ibid.*, article 46 : comprenant notamment l'adéquation aux finalités d'utilisation secondaire des données de santé prévues par le futur règlement, les données demandées sont nécessaires, adéquates et proportionnées aux finalités envisagées, le demandeur est qualifié au regard des finalités envisagées, des mesures techniques et organisationnelles suffisantes sont prévues, les requis éthiques fixés éventuellement par le droit national applicable sont vérifiés.
[190] *Ibid.*, article 42.
[191] *Ibid.*

membres pour certains types d'utilisateurs de données comme les organismes du secteur public, les organismes opérant dans le secteur de la santé publique, les chercheurs universitaires ou les micro-entreprises. Le détenteur des données fournira une estimation de ces coûts au HDAB ; ce dernier lui versera la partie des frais liés aux coûts pesants sur le détenteur de données de santé.

L'environnement de traitement sécurisé – L'accès aux données de santé ne sera donné par les HDAB que dans un environnement de traitement sécurisé répondant à des exigences en matière de sécurité et d'interopérabilité fixées par les dispositions du futur règlement[192]. Il s'agira ainsi par exemple de limiter l'accès à l'environnement uniquement aux personnes autorisées par le permis d'accès ou réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données de santé grâce à des mesures techniques et organisationnelles de pointe. Les HDAB devront veiller à ce que les utilisateurs de données de santé ne puissent télécharger que des données de santé non-personnelles comprenant des données de santé sous forme de statistiques anonymes. Les espaces de traitement sécurisés seront, eux, soumis à des audits réguliers. Parallèlement, il est prévu que la Commission décrive, au moyen d'actes d'exécution, les exigences techniques, organisationnelles, de sécurité de l'information, de confidentialité, de protection des données et d'interopérabilité.

Responsabilité – En matière de responsabilité, il était prévu, dans le texte initial, une responsabilité conjointe des HDAB et des utilisateurs de données de santé dans l'accès aux données. L'accord inter-institutionnel détaille davantage les modalités applicables en matière de responsabilité et abandonne l'approche responsabilité conjointe initialement proposée. Chaque acteur désigné par le futur règlement (détenteur des données de santé, détenteur des données de santé de confiance, HDAB, utilisateur des données de santé) restera alors responsable des actions lui incombant au regard de ce qui est imposé par le futur règlement[193].

2. Droit des personnes physiques de s'opposer au traitement des données de santé en vue d'une utilisation secondaire

Le sujet de la préservation de l'autonomie des individus concernés par le traitement de leurs données de santé dans le contexte de l'utilisation secondaire a mêmement été au centre des discussions sur le texte. Là où la Commission européenne ne prévoyait aucun mécanisme de préservation de l'autonomie des individus dans sa proposition de texte[194], le Parlement européen et le Conseil de l'Union sont parvenus à un accord sur l'introduction d'un droit d'opposition (*opt-out*) des individus concernés au traitement des données de santé personnelles en vue de leur utilisation secondaire, et ce, à tout moment sans indication de motif et de manière réversible[195]. Ce droit d'opposition devra être permis à travers un mécanisme d'opposition facilement compréhensible, qui sera mis en place par les Etats membres. L'exercice de ce droit n'affectera pas le traitement des données de santé personnelles concernant cette personne pour des traitements ayant été autorisés antérieurement à l'expression de cette opposition. Les États membres pourront prévoir un mécanisme permettant de passer outre l'expression de cette opposition dans des conditions précises et cumulatives que sont :

- la demande d'accès aux données est formulée par un organisme du secteur public ou une institution de l'Union mandatée dans le domaine de la santé publique pour des finalités d'intérêt public en matière de santé, de politiques publiques ou bien de statistiques dans le domaine de la santé, ou bien de

[192] *Ibid.*, article 50.
[193] *Ibid.*, article 51.
[194] *Ibid.*, article 33, paragraphe 5.
[195] *Ibid.*, article 48a.

recherche scientifique pour des raisons importantes d'intérêt public, ;
- les données ne peuvent pas être obtenues par d'autres moyens en temps utile et de manière efficace.

La législation nationale prévoyant un tel mécanisme devra contenir les mesures spécifiques et appropriées pour protéger les droits fondamentaux et les données personnelles des personnes physiques.

Ces dispositions ont notamment été introduites pour trouver un équilibre entre la préservation de l'exercice de l'autonomie des individus quant à la réutilisation de leurs données d'une part, et le fait de pouvoir garantir la complétude des données dans certaines situations d'autre part.

3. Gouvernance de l'utilisation secondaire des données de santé

Infrastructure transfrontalière pour l'utilisation secondaire des données de santé (HealthData@EU) – Le futur règlement instaure une infrastructure dédiée à l'utilisation secondaire des données de santé afin de connecter les différents points de contact nationaux (HDAB référents dans chaque État membre)[196] identifiés auprès de la Commission européenne. Le futur règlement décrit les points de contact nationaux comme étant des passerelles organisationnelles et techniques qui permettent et sont responsables de la mise à disposition des données de santé en vue d'une utilisation secondaire dans un contexte transfrontalier. Au-delà des HDAB des États membres, d'autres participants pourront être autorisés à participer à HealthData@EU, comme les infrastructures de recherche liées à la santé ou d'autres structures similaires dont le fonctionnement est fondé sur le droit de l'Union et qui soutiennent l'utilisation de données de santé à des fins de recherche, d'élaboration de politiques, de statistiques, de sécurité des patients. Quant aux pays tiers et organisations internationales, ils pourront également devenir participants agréés à travers un acte d'exécution de la Commission sous réserve du respect du chapitre V du RGPD. De manière complémentaire, la Commission développe, déploie et exploite une plateforme centrale pour l'infrastructure HealthData@EU en fournissant les services informatiques nécessaires pour soutenir et faciliter l'échange transfrontalier d'informations entre les HDAB. A la demande de deux points de contacts nationaux ou plus, la Commission pourra fournir un environnement de traitement sécurisé pour des données provenant de plusieurs États membres. HealthData@EU devra être interopérable avec les futurs autres espaces de données prévus par la stratégie européenne pour les données.

Le développement de l'infrastructure HealthData@EU est déjà en cours grâce à un projet pilote lancé en octobre 2022 qui rassemble 17 partenaires autour de différents cas d'usage. La Plateforme française des données de santé (Health Data Hub) en est la coordinatrice[197]. Ce projet pilote a pour objectif de livrer une première version de cette infrastructure dédiée à l'utilisation secondaire.

Catalogues européen et nationaux des données de santé disponibles pour l'utilisation secondaire – Afin d'améliorer la visibilité des données existantes au sein de l'Union européenne, le HDAB fournira un catalogue de données accessible au public sous forme de métadonnées sur l'ensemble des données disponibles et leurs caractéristiques (source, nature, conditions de mise à disposition…)[198]. Ces différents catalogues nationaux, ainsi que ceux des autres participants autorisés, seront réunis dans un catalogue d'ensemble de données de l'UE mis à disposition par la Commission européenne[199].

---

[196] *Ibid.*, article 52.

[197] « HealthData@EUPilot. Piloting an infrastructure for the secondary use of healthdata », site du projet pilote de l'infrastructure « MyHealthData@EU ».

[198] Article 55, REEDS, *op. cit.*

[199] *Ibid.*, article 57.

Qualité et utilité des données de santé pour une utilisation secondaire – Pour informer les utilisateurs de données sur la qualité des données de santé référencées dans le catalogue, un label de qualité et d'utilité des données de l'Union pourra être apposé par les détenteurs de données répondant à une liste de critères prévus par le futur règlement[200]. Les HDAB pourront évaluer si le jeu de données labellisé répond véritablement à ces critères et révoquer le label s'il ne répond pas à la qualité requise.

La Commission pourra, par des actes d'exécution, déterminer les spécifications minimales attendues d'ensembles de données à fort impact pour l'utilisation secondaire, lesquelles seront décrites comme étant des ensembles de données dont la réutilisation est associée à des avantages importants en raison de leur pertinence pour la recherche et la santé.

Stockage des données – Des dispositions sur les aspects liés au stockage des données de santé ont également été rajoutées à l'issue des discussions sur le texte. Qu'il s'agisse de l'utilisation primaire ou de l'utilisation secondaire (stockage et traitement des données de santé par les HDAB comprenant les environnements de traitement sécurisés), le stockage devra être situé dans l'Union européenne[201]. A titre exceptionnel, dans le cas de l'utilisation secondaire, le stockage peut pourra être effectué dans un pays tiers faisant l'objet d'une décision d'adéquation conformément aux dispositions du RGPD[202].

Transfert vers un pays tiers – De manière intéressante, les données non-personnelles de santé couvertes par le règlement seront considérées, dans le cadre de transfert vers un pays tiers, comme des données non-personnelles hautement sensibles. Cette qualification est prévue par le *Data Governance Act* dans le cas où leur transfert présenterait un risque de réidentification, compte tenu notamment du nombre limité de personnes physiques concernées par ces données, de leur dispersion géographique ou de l'évolution technologique attendue dans un proche avenir[203].

Comité européen de l'Espace européen des données de santé (EHDS Board)[204] – Par ailleurs, un comité de l'EHDS est institué pour faciliter la coopération et l'échange d'informations entre les États membres et la Commission, composé de deux représentants par État membre, d'un représentant de la Commission, d'un représentant pour l'utilisation primaire et d'un autre pour l'utilisation secondaire, les deux étant respectivement nommés par chaque État membre. Ledit comité devra agir dans l'intérêt public et de manière indépendante. Pourront aussi être invités à participer aux réunions, les autorités de surveillance du marché ou encore le Comité européen de la protection des données lorsque cela sera considéré comme pertinent par le Comité de l'EHDS. D'autres acteurs comme les autorités nationales, des experts, des observateurs, d'autres institutions de l'Union, des infrastructures de recherche pourront aussi être invités. Il est attendu que ce comité coopère avec les autres organes, entités et experts compétents comme le Comité européen de la protection des données instauré par le RGPD[205], ou le Conseil européen de l'innovation en matière de données prévu par le *Data Governance Act*[206].

Les tâches du comité de l'EEDS[207] seront réparties au regard de l'utilisation primaire et de l'utilisation secondaire. Le comité aidera les Etats membres à coordonner les pratiques des autorités chargées de la santé numérique, à publier des contributions écrites et à échanger les meilleures pratiques liées à la mise en œuvre du présent règlement en tenant compte du niveau régional et local ou

[200] *Ibid.*, article 56, paragraphe 3.
[201] *Ibid.*, articles 60a et 60aa.
[202] *Ibid.*, article 60aa.
[203] *Ibid.*, article 61.
[204] *Ibid.*, article 64.
[205] Règlement n° 2016/679/UE, *op. cit.*
[206] Règlement n° 2022/868/UE, *op. cit.*
[207] Article 65, REEDS.

encore à coopérer avec le forum des parties prenantes et partager des informations sur les risques et incidents.

Forum des parties prenantes[208] – Il est intéressant de noter que les discussions sur le texte ont amené à considérer l'importance de mettre en place un forum des parties prenantes pour faciliter l'échange d'informations et promouvoir la coopération avec les parties prenantes dans le cadre de la mise en œuvre du présent règlement. Les parties prenantes devront être représentatives des intérêts concernés par les questions d'utilisation primaire et secondaire des données de santé dans le cadre de l'EEDS. Elles comprendront notamment les représentants d'organisation de patients, de professionnels de santé, de l'industrie, d'organisations de consommateurs, de chercheurs scientifiques et d'universitaires. Les membres du forum seront nommés par la Commission à la suite d'un appel public à manifestation d'intérêt et d'une procédure de sélection transparente. Des réunions régulières seront prévues dans les dispositions du règlement et un rapport annuel d'activités devra être rendu. Néanmoins, à la lecture des dispositions, on ne saisit pas encore véritablement comment les positions exprimées par ce forum seront prises en considération dans la gouvernance de l'EEDS.

Groupes de pilotage – La gouvernance de l'EEDS sera complétée par deux groupes de pilotage des infrastructures MyHealth@EU et HealthData@EU, chacun composé d'un représentant par État membre des points de contact nationaux respectifs. L'objectif sera de prendre des décisions opérationnelles concernant le développement et l'exploitation des deux infrastructures transfrontalières. D'autres participants pourront être invités à échanger des informations et points de vue sur certaines questions, comme notamment les représentants des patients, des professionnels de santé, des consommateurs ou de l'industrie.

Formation des professionnels de santé[209]**.** À la suite des discussions sur le texte initial, des dispositions ont été rajoutées afin de souligner l'importance de la formation et de l'information des professionnels de santé incombant aux États membres d'élaborer et mettre en œuvre des programmes de formation pour les professionnels de santé pour les aider à comprendre et exercer efficacement leur rôle dans l'utilisation primaire des données.

Culture numérique en matière de santé[210] – De plus, au-delà des professionnels de santé, c'est la culture numérique en matière de santé et l'accès à la santé numérique qui devra être promue par les États membres à travers des campagnes de sensibilisation visant à informer les patients et le grand public de l'utilisation primaire et secondaire des données de santé dans le cadre de l'Espace européen des données de santé, y compris des droits qui en découlent, ainsi que des avantages, des risques et des bénéfices potentiels pour la science et la société.

Conclusion

La mise en œuvre du règlement sur l'Espace européen des données de santé demandera aux États d'importants efforts en interne pour parvenir à structurer et permettre une collaboration entre les acteurs concernés par ledit règlement. Les modalités d'opérationnalisation de ce règlement seront largement précisées grâce aux actes d'exécution attendus de la part de la Commission européenne. A ce sujet, l'entrée en vigueur du règlement est prévue à l'automne 2024 pour une application échelonnée sur plusieurs années : l'adoption des actes d'exécution par la Commission européenne est différée de 2 ans, l'entrée en application des dispositions sur l'utilisation primaire des données étant, elle, différée de 4 à 6 ans – 4 ans pour l'utilisation secondaire des données de

[208] *Ibid.*, article 64a.
[209] *Ibid.*, article 59a.
[210] *Ibid.*, article 59b.

santé. La procédure de certification des dossiers médicaux électroniques pourrait quant à elle entrer en application 6 ans après l'entrée en vigueur du règlement[211].

L'entrée en application du futur règlement supposera pour la France de procéder à certaines modifications dans la réglementation relative à l'accès aux données de santé (notamment en termes de délai d'accès aux données de santé), mais globalement, l'effort mis depuis maintenant plusieurs années sur la structuration de l'utilisation des données de santé disponibles à l'échelle nationale permettra une entrée en application du règlement facilitée. Le principal défi restera celui d'arriver à fédérer le riche écosystème des acteurs de la recherche français afin qu'ils perçoivent l'intérêt de cette structuration européenne et ne soient pas trop réfractaires aux nouvelles obligations qui s'imposeront à eux, notamment pour ceux qualifiés de détenteurs de données de santé par le futur règlement.

[211] Délégation du numérique en santé, Présentation Conférence de presse, 25 avril 2024, « Espace européen des données de santé »

Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, Hospital Discharge Report, Release 1.0, November 2023

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en droit public

L'eHealth Network a été établi conformément à l'article 14 de la directive 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers. Il s'agit d'un réseau volontaire qui relie les autorités nationales responsables de la santé en ligne désignées par les Etats membres. L'eHealth Network a pour ambition d'établir des lignes directrices visant à faciliter l'interopérabilité transfrontière des dossiers médicaux électroniques dans l'Union européenne.

En novembre 2023, eHealth Network publiait des lignes directrices sur l'échange électronique de données de santé en vertu de la directive 2011/24/UE plus précisément sur le rapport de sortie d'hôpital. Ces lignes directrices visent à soutenir l'échange de rapports de sortie d'hôpital pour la continuité des soins dans un cadre transfrontalier. En effet, les États membres ont des systèmes de santé de différents, une approche également différente dans les prestations de soins de santé et peuvent utiliser leur propre vocabulaire clinique. Tout cela peut entraîner des difficultés dans l'échange de données de santé des patients dans un contexte transfrontalier.

Le rapport de sortie d'hôpital comprend, en général, les documents cliniques générés durant le séjour du patient à l'hôpital : antécédents médicaux, diagnostics, traitements, résultats de tests, état de santé du patient au moment de sa sortie, plan de soins pour le traitement post-hospitalier…

La continuité des soins est une priorité dans une société où les citoyens européens travaillent, vivent et se déplacent entre les différents États membres. Ces lignes directrices proposent des moyens pour échanger les informations sur les sorties d'hôpital à travers l'Union, tout en préservant la confidentialité, l'intégrité et la disponibilité des informations des patients. Selon la législation et la pratique des États membres, le rapport de sortie d'hôpital est communiqué au patient à sa sortie et/ou envoyé aux professionnels de santé concernés. La communication transfrontalière de documents n'est réellement effective que s'il existe une certaine interopérabilité entre celui à l'origine de l'envoi du rapport et celui qui en est destinataire. Ces lignes directrices précisent la manière dont les opérateurs devraient s'organiser pour que le partage des rapports de sortie d'hôpital soit efficient : aspects organisationnels des structures, considérations sémantiques et techniques. Elles reviennent aussi sur l'ensemble des données que devraient contenir les rapports de sortie d'hôpital. Un exemple concret de rapport de sortie d'hôpital conclut ces lignes directrices.

Hospital discharge report

Creation date: 18.3.2023 v 08:15 | Version: 1

Expand menu Expand all

Patient: Ing. Jana Example, PhD. (Ž) ČP: 999999/9999 (VZP)

Gender	Female	**Address:**	
Maiden name	Dvořáková	Ulice 13a	
Date of birth	xx.xx.1935	150 00 Praha 5	
Place of birth	Žilina	**Lega guardiens:**	
Insurance number	9999999999	**JUDr. Eliáš Example**	
Health insurance house	Všeobecná zdravotní pojišťovna (111)	Ulice 1234	
Marital status	maried	516 00 Město	
Citizenship	Czech Republic	Mobile +420 600 000 111	
Communication languages	Czech Slovak, preferred	Phone (home) +420 222 222 222 Phone (work) +420 333 333 333	
Phone (home)	+420 216 200 100		
Mobile	+420 603 200 100		
Email	email@provider.cz		

Hospital encounter: Example hospital
In-patient encounter from 09.10.2022 to 17.10.2022

Example hospital
Rovná 345
550 00 Malá Obec, Středočeský kraj

Phone +420 613 111 222 0
Fax +420 201 201 201
info@nemprklad.cz
http://www.nemprklad.cz

Case number: Pn123456
Admission date and time: 09.05.2022, 10:46
Discharge date and time: 17.05.2022, 12:00

Contact person:
Prof. Jan Voštěp
Phone (work) +420 212 444 555

Allergies, Intolerances and Medical Allerts:

- Drug Allergy: Penicillin
- Permanent anticoagulant treatment in permanent atrial fibrillation, transient hemiparesis after discontinuation
- Repeated loss of blood in the stool

This is a sample discharge report containing fictitious information that does not represent any real case. The report illustrates the basic technical capabilities of the design.

Admission reason

Bleeding into the digestive system

Hospital stay

Diagnostic summary

Diagnosis / Problem description	Onset date	Resolution date	Category	Code
Treated conditions				
Angiectasia in ascending colon	10.05.2022	10.05.2022	POA	*K55.2*
Recurrent lossy hyposideremic anemia from angiectasia in the ascending colon	30.07.2016		POA	*D50.0*
Polyp of the sigmoid	10.05.2022		POA	
Transient ischemic attack (TIA) with transient left-sided hemiparesis	11.5.2022	11.5.2022	HAC	*G45.9*
Permanent atrial fibrillation	2011		POA	*I48.1*
Amiodarone hypothyroidism	2018		POA	*E03.2 Y52.2*
Other conditions (untreated)				
Stricture of the right ureter	2020			
Postmenopausal osteoporosis, stable finding	2018			*M81.0*
Varicose veins of the lower limbs	2014			*I83.9*
Isolated hypercholesterolemia				*E78.0*
Presbyacusis bilat.				*H91.1*

Surgeries and other "instrumental" interventions

Procedure Date	Description	Outcome	Complications
15.5.2022	Destruction of angiectasias in the ascending colon by argon plasmacoagulation via colonoscopy and polypectomy in the sigmoid colon	Successful	None

Medical devices and implants

No implants or medical devices

Other significant treatment

Fraxiparine 0.3 ml every 12 hours sc. (when discontinuing oral anticoagulation)

Results not yet delivered

Histology from a resected polyp in the colon.

Clinical synthesis

87-year-old patient treated with long-term (since 2016) parenteral iron replacement and repeated erythrocyte transfusions. However, at the beginning of March 2018, a drop of Hb of almost 40 g/l in less than 3 weeks was detected, therefore admitted to our clinic for blood transfusions and investigation of the etiology of the losses.

Gastrofibroscopy without evidence of bleeding, colonoscopy showed blood in the colon, but the source was not found, presumably in the small intestine.

Source of bleeding was not detected even by double balloon enteroscopy and repeat capsule enteroscopy (2022). In the following period, the hemoglobin value was above 100 g/L with a few exceptions.

Now electively admitted for an endoscopic examination of the terminal ileum by colonoscopy, which revealed angiectasias in the ascending colon (apparently covered by blood in the earlier acute colonoscopy) and a small polyp of the sigmoid colon (biopsy taken). After discontinuation of anticoagulant therapy, transient ischemic attack with left-sided hemiparesis occurred on May 11, 2022, which resolved spontaneously during transfer for brain CT scan.

Therefore, she was secured with heparin and switched to the lowest still effective dose of direct anticoagulant. Subsequently, destruction by argon plasmacoagulation via colonoscopy was performed without complications. Prior to dimission, i.v. iron was administered.

Status at discharge

Objective findings

unchanged since admission

Functional status

unchanged since admission

Recommendations

Social and health measures after discharge

-

Regime and dietary measures

existing regime, food saving

Medication summary

Status	Medicinal product	Administration	Dosage	Note
Stopped	Pradaxa 110 mg	2 x day	1 tbl	
Changed	none			
New	Eliquis 2,5 mg	2 x day	1 tbl	
Continuous	Euthyrox 75 ug	daily	1-0-0-0	
	Fludrokortizon tbl.	daily	1/4-1/4-0-0	
	Digoxin tbl. 0,125 mg	daily	1-0-0-0	
	Calcichew D3 tbl	daily	0-0-1-0	
	Cilkanol tbl.	daily	1-0-1-0	
	Ascorutin tbl.	daily	1-0-1-0	

Care plan

Recommended care

follow-up blood count and feraemia in one week, stool examination for occult bleeding in two weeks if haemoglobin drops - arranged by GP

Dates of check-ups

Check-up at the internal outpatient clinic (**after prior arrangement by phone on +420 123 456**)

Optional sections of the hosptital discharge letter

Patient history

Medical history

Past problems

Diagnosis / Problem	Onset date	Resolution date	Previous therapy	Clinical status
Permanent atrial fibrillation			Anticoagulant therapy with dabigatran and rate-control digoxin since 11/2011; paroxysmal fibrillation was first detected at about 55 years of age, first treated with propafenone, then amiodarone + beta-blockers (but these were discontinued immediately due to a tendency to hypotension), dronedarone administration was also tried. Negative coronary angiography in 2000.	Active
Amiodarone hypothyroidism			Euthyrox substitution therapy	Active
Recurrent states of weakness with hypotension			since 11/2011 treated with small doses of mineralocorticoids	
Isolated hypercholesterolemia	at about 55 years old		Hypolipidemic treatment in the past, then with satisfactory values without treatment.	Inactive
Perceptual hearing loss			Dispensed at the ENT clinic Dr. XXX YYYY	Active
Varicose veins of the lower limbs	for many years		Currently no problems, uses compression stockings and venotonics (Detralex)	Inactive
Postmenopausal osteoporosis	2000		Stable finding. Dispensed in ###, high fracture risk, initially anti-osteoresorptive treatment with risedronate, then discontinued due to relative contraindication p.o. aminobisphosphonate; followed by denosumab without Hospital Acquired Condition (HAC)s. DXA 10/2017: bone density is in the osteoporosis zone.	Inactive
Bilateral cataract	06.2017		right eye surgery 2010, vitreomacular traction sy bilat. in right surgery (posterior capsulectomy 6/2017)	Inactive
Recurrent anemia	2013		Repeated colonoscopy (2014 polyp in the lienal flexure – endoscopically removed, 2015 small ulcer on the opposite Bauhinian valve with a bloody base; 4/2016 recurrence of polyp c. transversum (approx. 6x4 mm). Permanent substitution of Fe i.v.	Inactive
Hydronephrosis l.dx. with transient dysfunction of the right kidney	04.2020		during ascending ureteropyelography, a long relative stricture of the ureter was detected at the level of the SI joint	Inactive
Left humerus fracture				Inactive

History of procedures

Date	Procedure	Reason
04.2020	Insertion of a stent into the right ureter	Hydronephrosis l.dx. with transient dysfunction of the right kidney

Devices and Implants

Start date	End date	Description	Location
04.2020		Ureteral stent	Right ureter

Vaccination

Vaccination date	Description
10.2020	Anti-flu

Family history

father +65 for myocardial infarction

Social history

old-age pensioner, widow, lives with her daughter in a 1st category apartment, 3rd floor with elevator

Admission evaluation

Objective findings

BP 108/74 mmHg, heart rate 85/min slightly irregular. deviations from the physiological findings: heart action slightly irregular, 2 sounds, quiet systolic murmur in the tip area 1-2/6, abdomen above niveau, numerous peristaltic sounds on auscultation, lower limbs without swelling only slightly soaked bilaterally, signs of chronic venous insufficiency.

Functional status

walking, self-sufficient

Selected findings

Laboratory findings

Sample collection date: 30.10.2022 7:00

Test name	Value	Units	Reference range	Interpretation
Blood count				
Leukocytes	8,8	10^9/L	4,0-10,0	*
Erythrocytes	3,47	10^{12}/L	3,80-5,20	-
Hemoglobin	104	g/L	120-160	--
Erythrocyte (MCV, mean volume)	93,4	fL	82,0-98,0	*
Platelets	229	10^9/L	150-400	*

+++ Critical high ++ Significantly high + High * Normal - Low -- Significantly low --- Critical low

Imaging findings

CT brain 11.5.2022:
Diffuse brain atrophy of medium degree, without signs of a focal lesion. Defect of the occipital bone paramedially on the right - dop. scintigraphic examination.

Other findings

Coloscopic examination 10.5.2022:
In the sigmoid, a small polyp about 4 mm in size - a biopsy was taken, there are several angiectasias in the ascending colon, which bleed slightly when touched with the colonoscope. Other parts of the colon are without pathological findings. The ileocecal valve and terminal ileum could not be intubated.

Coloscopic examination 15.5.2022:
Total colonoscopy with destruction of four angiodysplasias in the ascending colon by argon plasma coagulation; the procedure was performed without complications
Total colonoscopy with treatment of angiodysplasia in the right colon with argon plasma coagulation: performed argon plasma coagulation of 4 small angiectasias in the transverse and 3 in the ascendens.

Konzilia

ENT consultation:
subjective pain 0/10 NRS, hearing impairment, obj. OM bilat ear canals quiet, eardrums intact, gray, no retraction, middle ear air audio bilat perc. hearing loss 40-40-40-50-55-60-70 dB, tympanum low A bilat. Dr. presbyacusis bilat

In case of any question please contact: MUDr. Jan Pudr
Phone (work) +420 613 345 344

Signature: Prof. Jan Voštěp, 17. 9. 2022 11:25
MUDr. Jan Pudr, 17. 9. 2022 11:35

More information about this document

EXEMPLE D'UN RAPPORT DE SORTIE

Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, Medical imaging studies and reports, Release 1.0, November 2023.

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en droit public

Institué sur la base de l'article 14 de la directive 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers, l'eHealth Network relie les autorités nationales responsables de la santé en ligne désignées par les Etats membres. Ce réseau rédige des lignes directrices dont l'objectif premier est de faciliter l'interopérabilité transfrontière des dossiers médicaux électroniques dans l'Union européenne.

En novembre 2023, eHealth Network publiait des lignes directrices sur l'échange électronique transfrontière des études et rapports d'imagerie médicale. Ces lignes directrices tendent à permettre le transfert des études et rapports d'imagerie entre professionnels de santé dans un contexte transfrontalier quand cela est nécessaire pour la continuité de la prise en charge du patient. Elles précisent qu'elles n'ont pas vocation à s'appliquer uniquement dans un contexte transfrontalier mais qu'elles devraient également être suivies au sein même des Etats membres dans un cadre régional ou national.

Le transfert des informations médicales permet aux professionnels de santé impliqués de mieux prendre en charge le patient, de comparer les résultats, d'éviter des actes de soins non-nécessaires ou, par exemple, de réaliser à nouveau les mêmes actes ce qui serait préjudiciable, non seulement, en termes de coût mais également de temps dans la prise en charge du patient. Aussi, en transférant les rapports d'imagerie médicale, les professionnels de santé assurent la sécurité des patients en minimisant les irradiations médicales inutiles conformément à ce que prévoit la directive 2013/59/Euratom[212].

A l'instar des autres lignes directrices de l'eHealth Network, les présentes lignes directrices fournissent une liste d'exigences techniques pour une interopérabilité effective entre les Etats membres. C'est ainsi que ces lignes directrices confirment l'utilisation pour les études et rapports d'imagerie médicale du format européen d'échange de dossiers de santé électroniques (EEHRxF).

[212] Directive n° 2013/59/Euratom du Conseil du 5 décembre 2013 fixant les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants et abrogeant les directives n^os 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom, *JOUE* n° L 13 du 17 janvier 2014.

Lancée le 1er février 2021, l'action conjointe « Vers un espace européen des données de santé » (TEHDaS), cofinancée par la Commission européenne et ayant mobilisée la coopération de 25 États membres de l'Union, est arrivée à son terme le 31 juillet 2023. L'objectif de ce projet fut de développer et de promouvoir des concepts orientés sur le partage et l'utilisation secondaire des données de santé dans le cadre du futur Espace européen des données de santé, contribuant ce faisant à l'émergence du cadre opérationnel nécessaire à sa mise en œuvre. Parmi les recommandations majeures de TEHDaS figure la nécessité de veiller à une répartition claire des rôles et des responsabilités entre les détenteurs des données, les organismes responsables de l'accès aux données et les coordinateurs nationaux des organismes de l'accès aux données.

EN SAVOIR PLUS

Options for the services and services architecture and infrastructure for secondary use of data in the EHDS, 4 July 2023

Ce rapport analyse différentes options techniques permettant aux États membres de faciliter l'utilisation secondaire des données de santé dans le cadre du futur espace européen des données de santé (EHDS), détaillant pour chacune d'elles les avantages et les inconvénients.

EN SAVOIR PLUS

Compilation of perspectives on multi-country data access applications, mutual recognition and cross-border applications through workshop approach, 5 July 2023

TEHDaS présente une synthèse des meilleures pratiques et des points faibles en matière de partage transfrontalier des données de santé pour leur utilisation secondaire et, en même temps, formule des recommandations pour l'examen de cette question dans le cadre de l'espace européen des données de santé à venir.

EN SAVOIR PLUS

Markus Kalliola *et al.*, *Advancing data sharing to improve health for all in Europe. Main findings of joint action Towards the European Health Data Space 2021–2023*, September 2023

Un résumé des principales conclusions du projet TEHDaS relativement à l'utilisation des données de santé à des fins de recherche et d'innovation est présenté dans ce document, lequel est destiné aux acteurs européens des données santé et au public.

EN SAVOIR PLUS

Guidelines document for multi-country data access applications, including mutual recognition and cross-border applications, 22 September 2023

Ce rapport contient plusieurs recommandations visant à clarifier certaines dispositions du règlement sur l'EHDS présentée par la Commission en mai 2022, en vue d'améliorer et d'élargir les possibilités d'utiliser les données de santé dans le cadre de projets transfrontaliers ou multi-pays.

EN SAVOIR PLUS

Recommendations on a Data Quality Framework for the European Health Data Space for secondary use, 26 September 2023

TEHDaS a développé un cadre permettant de garantir la qualité et l'utilité des données dans l'EHDS et treize recommandations dans ce but.

EN SAVOIR PLUS

Sustainability Plan for Secondary Use of Health Data in the European Health Data Space, 29 September 2023

EN SAVOIR PLUS

Report on lessons learned to be applied and recommendations for data altruism practices in the implementation of construction of national and European health data spaces (including broad consent), 29 September 2023

Le TEHDaS souhaite encourager et, dans la mesure du possible, aider les États membres à permettre le partage volontaire des données à des fins d'intérêt général – l'altruisme des données ou *data altruism*), car ces données sont le principal vecteur de progression au profit de la recherche et de l'innovation.

EN SAVOIR PLUS

L'action conjointe TEHDaS2 a débuté en mai 2024, et se terminera en décembre 2026. Dans le prolongement du travail effectué dans le cadre du premier projet TEHDaS, cette deuxième action commune aura vocation à préparer concrètement les États membres à la mise en œuvre du règlement sur l'EHDS, élaborant ici et là des lignes directrices et des supports techniques pour leur permettre d'utiliser les données de santé de manière harmonisée.

EN SAVOIR PLUS

Arrêté du 26 octobre 2023 fixant les règles de gestion des droits d'accès au dossier médical partagé des professionnels mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 du code de la santé publique,

***JORF* n° 0252 du 29 octobre 2023**

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en droit public

Le présent arrêté précise les règles des droits d'accès aux documents du dossier médical partagé (« DMP ») des patients pour les professionnels des secteurs sanitaire, social et médico-social. Ces droits d'accès sont applicables de plein droit, sauf si le titulaire du DMP en décide autrement.
Seuls sont autorisés à accéder au DMP d'un patient les professionnels qui interviennent dans sa prise en charge. Ainsi, tout professionnel membre de l'équipe de soins du patient est réputé autorisé à accéder au DMP de ce dernier, sous réserve qu'il ne s'y soit pas opposé. Le consentement du patient n'est donc pas nécessaire dans ces cas précis. Au contraire, lorsque des professionnels non-membres de l'équipe de soins du patient souhaitent accéder au DMP, le consentement préalable du patient est obligatoire et doit être recueilli avant chaque consultation. La forme de recueil du consentement n'est pas imposée par le législateur : il peut se faire par tout moyen, y compris de manière dématérialisée.

Conformément à l'article L. 1110-12 du Code de la santé publique, appartiennent à l'équipe de soins l'ensemble des professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes.

L'arrêté du 26 octobre 2023 établit une matrice d'habilitations des professionnels : ceux-ci ne sont habilités à accéder qu'aux catégories de données prévues et, au sein de ces catégories, qu'aux seules données strictement nécessaires à la prise en charge du patient. Afin de s'assurer que ces règles sont respectées, toutes les actions et accès sur le DMP sont automatiquement tracés dans le système DMP. Le titulaire du DMP peut consulter ces traces à tout moment. Aussi, dès qu'un professionnel accède pour la première fois à son DMP, le patient est notifié par tout moyen.

Au total, ce sont dix-neuf professions et disciplines qui sont abordées dans cette matrice : tous les professionnels de santé médicaux et paramédicaux réglementés par le Code de la santé publique, les professionnels sanitaire, social et médico-social exerçant des fonctions de coordination et d'orientation, les assistants de service social ou assistants sociaux, ou encore notamment les professionnels du social et médico-social exerçant des fonctions d'accompagnement aux soins.
Pour chacun des professionnels, la liste exhaustive des documents auxquels ils sont susceptibles d'accéder est abordée : comptes-rendus, imagerie, prescriptions et dispensation, plans et protocoles de soins…

Le non-respect des conditions d'accès est susceptible de faire encourir à son auteur une amende et une peine d'emprisonnement, en sus d'éventuelles sanctions disciplinaires.

De la même auteure :
Rapport d'information au nom de la commission des affaires sociales (1) sur la proposition de résolution européenne au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé - COM(2022) 197 final, Session extraordinaire 2022-20223, Sénat n° 874

EN SAVOIR PLUS

Rapport d'information sur les données de santé en France : une clarification nécessaire du cadre actuel

Catherine DEROCHE, *Rapport d'information au nom de la commission des affaires sociales sur les données de santé*, Session extraordinaire de 2022-2023, Sénat n° 873

par Nino ESCUDIER

Étudiant en Master de droit européen
Université Toulouse Capitole

Publié en juillet 2023 à la suite d'une mission d'information de la commission des affaires sociales du Sénat, le rapport DEROCHE dresse le bilan des réformes successives concernant l'encadrement et le traitement des données de santé en France, et l'évolution du cadre actuel au regard du nouveau contexte européen. À l'issue de ce rapport, le Sénat adresse quinze recommandations afin d'atteindre les objectifs fixés par la loi, lesquels ne sont pour l'instant pas encore en mesure d'être atteints. Bien que salué sur certains aspects, le système français des données de santé nécessite une clarification et une adaptation dans le contexte de l'établissement d'un espace européen des données de santé.

Sous la présidence de Mme Catherine DEROCHE, la commission des affaires sociales du Sénat français a adopté le 12 juillet 2023 à l'unanimité des membres la composant le rapport d'information n°873 sur les données de santé[213]. Ce rapport sénatorial intervient dans le cadre d'une mission d'évaluation de la mise en œuvre de la loi santé de 2019[214]. Cette dernière portait alors plusieurs ambitions d'envergure : élargir le périmètre des données versées au système national des données de santé (SNDS), la création d'un groupement d'intérêt public–la plateforme des données de santé ou *Health Data* Hub (HDH), et la création de l'espace numérique de santé[215].

Au terme de mois de travail au cours de la session parlementaire 2022-2023, la commission du Sénat a entendu émettre une quinzaine de recommandations concernant la gouvernance des données de santé, leur utilisation à des fins de recherche, et le renforcement de l'usage des plateformes dédiées au traitement des données. En effet, malgré les objectifs portés par les réformes successives concernant l'encadrement et l'utilisation des données de santé se veulent ambitieux, le rapport pointe des retards dans la mise en œuvre de ces derniers. La loi de 2019, bien que saluée, ne semble pas encore dévoiler son plein potentiel.

[213] Rapport d'information de la commission des affaires sociales du Sénat sur les données de santé, 12 juillet 2023, 178 p. Ci-après « Rapport DEROCHE ».

[214] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), *JORF* n° 0172 du 26 juillet 2019.

[215] Rapport DEROCHE, *op. cit.*, p. 34-35.

Dans le contexte du projet d'espace européen des données de santé (ou *European Health Data Space, EHDS*), il est bon de rappeler que la France a depuis un certain nombre d'années développé son propre système de collecte des données de santé à des fins de recherche et de facilitation de la prise en charge des patients. Si le modèle français a pu servir sur certains points d'inspiration au projet de règlement voulu par la Commission européen, il ne reste pas moins perfectible – notamment concernant la mise à disposition des données de santé à des fins de recherche dont les délais constituent un véritable frein.

Affichée comme une priorité de la Commission européenne sous le mandat de Madame VON DER LEYEN, la place du numérique en santé sera sans doute croissante dans les années à venir[216]. C'est dans cette optique qu'un projet de règlement européen créant l'espace européen des données de santé est en cours d'élaboration[217].

Dès lors, bien que les données de santé aient fait l'objet de l'élaboration d'une véritable politique publique et d'un encadrement juridique (**I**), le système français des données de santé doit faire l'objet d'adaptation afin de garantir sa pleine efficience dans un contexte de priorisation de la question au niveau européen (**II**).

I. UN MODÈLE FRANÇAIS PRÉCURSEUR BIEN QUE PERFECTIBLE

Le rapport du Sénat rappelle la politique menée en matière de données de santé et souligne son caractère précurseur au niveau européen (**A**). Toutefois, si le modèle français dispose d'un fort potentiel, force est de constater que certains changements sont à apporter quant à son fonctionnement (**B**).

A. Un système français précurseur et faisant preuve de potentiel

La France a su entamer la constitution de bases de données à des fins administratives et épidémiologiques dès la fin des années 1970. Se limitant initialement au simple recensement des activités des professionnels de santé au niveau national, les bases de données de santé se sont améliorées au fil des années pour aboutir à une modernisation du système de santé par le numérique. Cette modernisation s'est accompagnée d'un encadrement juridique de l'accès aux données de santé premièrement établi à partir de 1999, et aménagé au gré des réformes successives.

La structuration des bases de données françaises s'est ainsi faite progressivement pour constituer aujourd'hui un ensemble riche qualifié de « trésor national » par le rapport du Sénat. C'est en 2016[218] que le législateur a voulu réunir les multiples bases de données en créant le Système National des Données de Santé (SNDS).

Ce dernier a réuni, entre autres :

- le système national d'information interrégimes de l'assurance maladie (Sniiram) créé en 1999 ;
- les systèmes d'informations hospitaliers constitués de données médico-administratives ;
- le système d'information alimenté par es maisons départementales des personnes handicapées ;
- les données sur les causes de décès.

Ces bases de données constituent alors ce qui est communément appelé le SNDS « historique ». Les fichiers contenus par le SNDS permettent de couvrir l'ensemble de

[216] DE GROVE VALDEYRON Nathalie, « De l'espace européen de la santé en ligne à l'espace européen des données de santé : le numérique au service de la construction d'une Union européenne de la santé », *RAE.*, 2021, n°2, p. 335-347.

[217] Proposition de règlement du Parlement européen et du Conseil du 3 mai 2022 relatif à l'espace européen des données de santé, *COM(2022)* 197 final.

[218] Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé (1), *JORF* n° 0022 du 7 janvier 2016.

la population et se révèle être une base précieuse, d'autant plus qu'elle a bénéficié d'un élargissement en 2019[219] incluant six nouvelles bases. Néanmoins, l'aspect pléthorique de ces données peut constituer une difficulté supplémentaire. La Dress[220] souligne que ces données doivent être rassemblées, qualifiées, et pseudonymisées, ce qui peut conduire à un délai de mise à disposition plus long.

Aujourd'hui ce délai est en moyenne de 18 mois, représentant un obstacle pour l'utilisation secondaire de ces données notamment à des fins de recherche. À ces longs délais de mise à disposition s'ajoute par ailleurs une actualisation des données du SNDS à la fréquence peu régulière et pouvant prendre plusieurs mois.

Les données rassemblées au sein du SNDS sont indéniablement une source extraordinaire pour la recherche et l'établissement de politiques de santé publiques. Cependant des obstacles demeurent, qu'il s'agisse de la nature des données au sein du SNDS, de leur gouvernance, ou bien du virage numérique abordé que partiellement. Par conséquent, le rapport DEROCHE souligne que le potentiel complet du système français n'a pas encore pu se déployer.

B. Des améliorations possibles du système national des données de santé

La nature médico-administrative des données présentes au sein du SNDS est pointée par le rapport comme une de ses limites. Le manque de données cliniques dans le SNDS se trouve toutefois atténué par l'existence des entrepôts de données de santé (EDS), apparaissant comme le « volet médical » du SNDS. La grande diversité des sources des données cliniques versées aux EDS rend leur exploitation difficile, conduisant la Haute Autorité de santé à recommander un socle commun de données afin de garantir leur qualité.

En outre, le rapport sénatorial souligne les déficiences du SNDS quant aux données issues des parcours de soins, encore trop faiblement appariées avec le SNDS. Parmi les bases de données qui seraient bénéfiques à la recherche, le rapport mentionne les bases épidémiologiques spécifiques, le dossier pharmaceutique ou encore le dossier médical en santé au travail.

Au faible appariement des données de santé, s'ajoute le faible investissement dans la recherche dénoncé par le Sénat (un soutien public à la recherche en baisse de 28% entre 2011 et 2018). En effet, le rapport DEROCHE soutient qu'un meilleur investissement dans la recherche permettrait de stimuler la création des données non existantes.

Toutefois, comme indiqué précédemment, la difficulté majeure quant à l'exploitation des données de santé réside avant tout dans l'existence de délais de mise à disposition loin d'être optimum. Le parcours d'accès présente des marges de fluidification que le rapport dessine. Tout d'abord en clarifiant la gouvernance opérationnelle de l'accès aux données de santé du SNDS. Celle-ci est partagée entre différents acteurs, ce qui a pour résultat de complexifier et allonger la procédure d'accès.

La CNIL[221] en charge de l'autorisation d'accès aux données, et le Cesrees[222] en charge de vérifier l'intérêt de l'accès aux données, respectent globalement les délais imposés. Toutefois, la mise à disposition par la Caisse nationale de l'assurance maladie (CNAM) des données peut prendre jusqu'à dix mois, allongeant considérablement le délai d'accès. De façon globale, les demandes d'accès aux données sont complexes et requièrent des porteurs de

[219] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *op. cit.*
[220] Direction de la recherche, des études, de l'évaluation et des statistiques.
[221] Commission nationale informatique et liberté.
[222] Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé.

projets une grande attention. Afin de réduire les délais, le Sénat esquisse plusieurs pistes de réflexion : revoir la procédure en envisageant que l'expert du SNDS de la Cnam puisse rendre son avis en amont ; la priorisation des projets en fonction de leur intérêt scientifique ; la tarification des données au moins pour les acteurs privés – ce qui pourrait à terme réduire le nombre de demandes ; et le renforcement des moyens des différents organes. Aussi, dans le cadre de l'espace européen des données de santé, ces délais devront faire l'objet d'une amélioration afin de respecter les échéances que dresse le projet de règlement européen.

La loi de 2019 a entendu restructurer le système des données de santé en substituant l'institut national des données de santé par la Plateforme des données de santé ou *Health Data Hub*. Ce dernier a pour rôle la gestion et la mise à disposition des données du SNDS. Néanmoins, l'absence de copie du SNDS hébergée par le *Health Data Hub* met à mal l'ambition de la loi de 2019. Voulu comme un « guichet unique » d'accès au SNDS, cette absence empêche de mener à bien sa mission, rajoutant de fait un acteur supplémentaire. Perçue comme la faille majeure du système des données de santé en France, le Sénat appelle à trouver une solution dans les plus brefs délais quant à l'hébergement d'une copie du SNDS, sans quoi un retard important sera pris par la recherche médicale.

Malgré des difficultés qui restent à surmonter, le système français des données de santé a pu bénéficier de certaines réformes bienvenues afin de préparer l'émergence d'un espace européen des données de santé.

II. LE SYSTÈME FRANÇAIS PREPARÉ À L'EMERGENCE D'UN ESPACE EUROPEEN DES DONNEES DE SANTE

La loi de 2019 a permis d'accélérer le virage numérique dans la santé permettant à la France de faire figure de proue dans le domaine des données de santé en Europe (**A**). Afin de préparer pleinement le système français à l'émerge de l'Espace européen des données de santé (EDHS, *European Health Data Space*), des adaptations resteront toutefois nécessaire (**B**).

A. Un virage numérique accéléré par la réforme de 2019

L'émergence du modèle français s'est faite progressivement, et s'est parfois confrontée à des échecs, notamment dans la volonté de créer un dossier médical personnel (DMP). Voulu par le législateur en 2004 afin de regrouper les données de prévention, de diagnostic ou de soins, sa conception n'a pas permis de le déployer à grande échelle. Jugées « irréalistes » par l'Inspection générale des affaires sociales, les ambitions du DMP se sont écrasées sur la réalité de sa réalisation. Reposant sur une demande de création expresse du patient, le déploiement du dispositif fut un échec. En 2012, seuls 156 000 DMP avaient été créés. Relancé en 2008 puis en 2016, le DMP ne sera généralisé sous une nouvelle forme qu'à la suite de la réforme portée en 2019 laquelle modifie les modalités de création du dossier en ne la faisant plus reposer sur la demande exprès du patient.

Prévu pour une entrée en vigueur au 1er janvier 2022 au plus tard, l'Espace numérique de santé (ENS) intègre le DMP. Grâce à cette nouvelle méthode, seulement 2% des assurés se sont opposés à la création de leur ENS. Ce sont donc 65,7 millions d'ENS qui ont pu être créés, regroupant environ 150 millions de documents en juillet 2023 – ce qui reste toutefois inférieur à l'objectif visé de 250 millions de documents. L'ouverture automatique de l'ENS a permis par la même occasion la création des DMP, accélérant finalement le virage numérique dans le suivi des patients.

Pour que ce virage s'accélère davantage, le Sénat recommande de renforcer les incitations conventionnelles à l'utilisation de *Mon espace santé* et de faciliter le déploiement du dispositif aux professions de santé qui en sont dépourvues. L'assurance maladie ayant

déjà eu recours à ces conventions pour inciter financièrement les professionnels de santé libéraux à l'usage des outils numériques, le Sénat envisage alors de favoriser ces incitations pour garantir l'atteinte des objectifs.

Ces incitations doivent toutefois s'accompagner d'une information claire sur l'usage de *Mon espace santé* et d'un effort de formation des professionnels de santé concernés, et des populations les plus fragiles dans l'utilisation des outils numériques.

En définitive, le système issu de la réforme de 2019 a permis un bon en avant en matière de numérique en santé. Toutefois, le manque de formation et d'usage des outils à la disposition des patients et des professionnels de santé persistent à constituer un obstacle dans le déploiement du plein potentiel de l'ENS. Le Sénat recommande en ce sens de faciliter l'accès des professionnels de santé à l'ENS, ce qui passe par un effort de formation initiale et continue. Par conséquent, dans un contexte d'européanisation des données de santé, le modèle français devra encore faire l'objet de certaines adaptations.

B. Des adaptations à prévoir en amont de la création de l'EDHS

La facilitation des échanges de données de santé avait été déjà engagée par le l'Union européenne à travers une directive européenne de 2011[223] voulant faciliter l'échange de données de santé dans le cadre des soins transfrontaliers. Cette directive a permis d'établir la plateforme en ligne « MaSanté@EU » donnant lieu à l'échange de données relatives au parcours de soins des patients (synthèses médicales et prescriptions électroniques notamment).

Lorsque la France a rejoint l'infrastructure commune centralisée MaSanté@UE (MyHealth@UE), le cadre juridique du DMP a subi certaines modifications afin d'autoriser l'accès des données par des professionnels de santé d'États membres dans des conditions strictes prévues par un décret de 2021[224], tout en respectant le consentement du patient.

Dans le cadre du projet de règlement européen établissant un espace européen des données de santé[225] – lequel a été finalisé au printemps 2024 – l'Union européenne entend faciliter l'utilisation primaire des données de santé. Ce règlement prévoit l'élaboration d'un format européen commun d'échange des dossiers de patients, des exigences renforcées en matière d'interopérabilité, et un respect accru des droits des patients. La facilitation de l'échange des données devrait aussi passer, selon le règlement, par une participation obligatoire à la plateforme sécurisée *MaSanté@EU*, mise à disposition par la Commission.

Par ailleurs, certaines fonctionnalités restent peu usitées par les professionnels et les patients en raison d'un retard accumulé par le système français. À titre d'exemple, seuls 2% des citoyens bénéficient de l'existence d'un « résumé patient » à leur endroit au niveau national,[226] lequel est pourtant nécessaire pour l'échange de données. C'est dans ce contexte-là que l'ENS devra faire l'objet de nouveaux ajustements. Le rapport DEROCHE dresse ainsi une liste de points précis sur lesquels le cadre français doit s'adapter. Plus particulièrement, en renforcement le déploiement de l'ENS afin de pouvoir mieux garantir le développement de la prescription électronique laquelle permettra aux patients de se voir délivrer leurs prescriptions dans un contexte

[223] Directive n° 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* n° L 88/45 du 4 avril 2011.

[224] Décret n° 2021-914 du 8 juillet 2021 relatif aux dispositions propres à la prise en charge du patient à l'occasion des soins de santé délivrés dans un autre État membre de l'Union européenne, *JORF* n° 0159 du 10 juillet 2021.

[225] Proposition de règlement relatif à l'espace européen des données de santé, *op. cit.*

[226] Réponse apportée par la Direction ministérielle du numérique en santé à la mission d'information du Sénat, voir rapport DEROCHE, *op. cit.*, p. 149.

transfrontalier. Le rapport conclut à l'accélération des efforts d'investissement dans les infrastructures et le développement des usages numériques afin de préparer l'émergence de l'EDHS.

MARCHAND-ARVIER Jérôme et *al.*, *Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé*, 5 décembre 2023

par Shana LEVI

Étudiante en Master 2 DIDE, Juriste européen, programme « Droit européen général »
Université Toulouse Capitole

La confiance, est le maitre mot de ce rapport : confiance en l'avenir des données de santé et leur réutilisation, « confiance sur la volonté et la capacité des acteurs à coopérer ensemble, sous l'impulsion politique nécessaire pour mettre en œuvre rapidement et efficacement les recommandations qui seraient endossées » (présent rapport, p. 3-4). En effet, Jérôme MARCHAND-ARVIER n'a eu de cesse dans ce rapport de rappeler l'importance de la collaboration, de la cohésion mais surtout de la volonté pour faire de l'utilisation secondaire des données de santé une des préoccupations premières. Parce qu'il est indéniable que nombre de progrès sont à réaliser afin d'avoir une réutilisation optimale.

« Par lettre en date du 31 mai 2023, le ministre de l'Économie, des finances et de la souveraineté industrielle et numérique, la ministre de l'enseignement supérieur et de la recherche et le ministre de la santé et de la prévention ont lancé une mission visant à poser les bases d'une feuille de route française en matière de réutilisation des données de santé » (p. 21).

La mission a mis en lumière les difficultés auxquelles était confrontée l'exploitation des données, que cela soit « des questions de délai, de mise à disposition sous-optimales, qui s'expliquent en partie par le fait que les extractions et appariements de données issues de la base principale du SNDS demeurent traitées par la CNAM, faute pour la Plateforme des données de santé (désignée Health Data Hub dans la suite du rapport) de pouvoir, à ce stade, héberger et exploiter une copie de cette base sur sa plateforme technologique (p. 22). Au terme de cette mission 37 recommandations ont été formulées.

« Le rapport assume une orientation résolument optimiste. Il ne s'agit pas d'un optimisme naïf : beaucoup de progrès ont été accomplis en quelques années en matière d'utilisation secondaire des données de santé. L'ensemble des acteurs ont conscience de l'importance des données de santé. Tous savent aussi qu'il est nécessaire de bien structurer, avec des infrastructures adaptées, ces données de santé pour pouvoir les réutiliser d'une manière optimale, et des investissements notables ont été réalisés en la matière. Tous savent enfin, et l'assument désormais, qu'une logique d'ouverture et de partage de ces données fait progresser la science, la recherche et la santé. Mais cette orientation relève également d'un optimisme de la volonté, car force est de reconnaître que ces progrès ne peuvent masquer le « verre à moitié vide », avec certes des processus d'accès aux données longs, complexes et coûteux, mais aussi une culture collective qui, trop souvent encore, conduit *in fine* à ne pas tout faire ensemble pour que concrètement, le partage des données de santé soit plus fluide et plus rapide. Il en va certes de la responsabilité du système – et donc de la nécessité de procéder à des évolutions de ce système -, mais il en va aussi de la responsabilité de chacun des acteurs, qui doivent, avec confiance, s'engager résolument dans une logique et une culture d'ouverture et de partage qui

n'est pas encore suffisamment présente » (p. 3).

Ces mots de Jérôme MARCHAND-ARVIER dans son préambule marquent l'importance de réformer le système des données de santé et de l'améliorer. Ce rapport est d'autant plus important qu'il aborde de manière détaillée les enjeux liés à la réutilisation des données de santé et propose des solutions concrètes pour surmonter les obstacles actuels. En effet, la réutilisation des données de santé représente une opportunité majeure pour améliorer la recherche médicale, l'innovation, la qualité des soins aux patients en France mais aussi la gestion des crises sanitaires.

Une utilisation optimale permettrait indéniablement de transformer le secteur médical. Le rapport MARCHAND-ARVIER met en lumière plusieurs aspects cruciaux de cette réutilisation.

Le rapport souligne que, « bien que la France dispose d'un patrimoine de données de santé très riche, elle reste en retrait par rapport à d'autres pays comme les États-Unis, Israël et le Royaume-Uni, qui exploitent mieux ces ressources » (p. 6). Ce retard peut s'expliquer par une série de freins structurels et culturels, qui limitent la pleine exploitation de ce potentiel.

Pour lever ces obstacles à la réutilisation des données de santé, le rapport ARVIER propose comme énoncé précédemment des recommandations clés. En premier lieu, il est crucial de réformer les procédures actuelles pour rendre les autorisations exceptionnelles plutôt que la norme. Le rapport recommande de renforcer la co-construction des méthodologies de référence avec les acteurs concernés et d'étendre le champ des procédures simplifiées. Cela permettrait de réduire les délais d'accès aux données et de faciliter leur réutilisation pour des projets de recherche et d'innovation.

Ensuite, il est nécessaire de promouvoir une meilleure interopérabilité entre les bases de données et de réduire les exigences de centralisation sur des plateformes uniques comme le *Health Data Hub*. Le rapport propose de lever l'obligation de centralisation auprès du *Health Data Hub* pour l'extension du catalogue du SNDS. Cela permettrait d'enrichir ce catalogue sans imposer des contraintes excessives aux producteurs de données, favorisant ainsi un partage plus large et plus efficace des données de santé. Le rapport insiste également sur l'importance de renforcer la coopération entre les différents acteurs. Pour améliorer cette coopération, il propose de développer des formations, des outils partagés et des standards communs. Par exemple, des formations spécifiques pourraient être mises en place pour les chercheurs et les professionnels de santé afin de les sensibiliser aux bonnes pratiques en matière de partage et de réutilisation des données. De plus, le développement d'outils partagés, tels que des "bacs à sable" pour tester la faisabilité des projets, pourrait faciliter l'accès aux données et encourager l'innovation.

Enfin, le rapport MARCHAND-ARVIER suggère de mettre en place des indicateurs de délai pour la mise à disposition des données. Ces mesures visent à accroître la transparence et à réduire les délais d'accès aux données, ce qui est essentiel pour encourager les chercheurs et les entreprises à poursuivre des projets ambitieux.

Le rapport insiste sur la nécessité d'une mise en œuvre rapide et pragmatique de ses recommandations. Pour cela, il est essentiel de renforcer le rôle du comité stratégique des données de santé dans la coordination interministérielle. Ce comité doit garantir la cohérence des initiatives et favoriser le partage des données. En outre, il est crucial d'assurer des financements stables pour les infrastructures de données de santé, incluant les entrepôts de données hospitaliers et les cohortes. Le rapport propose également de mettre en place une grille tarifaire harmonisée pour l'accès aux données, afin de simplifier les procédures de contractualisation et de rendre le système plus transparent et compétitif.

Améliorer la transparence vis-à-vis des citoyens sur l'utilisation de leurs données de santé et faciliter l'exercice de leurs droits sont des priorités. Le rapport recommande la création de plateformes centralisées pour l'exercice des droits des patients, ce qui permettrait de simplifier les démarches pour les citoyens et de renforcer leur confiance dans le système de réutilisation des données de santé. Ces plateformes pourraient également servir à informer les patients sur les bénéfices de la réutilisation des données pour la recherche et l'innovation médicale.

Enfin, le rapport propose de développer de nouvelles bases de données dans des domaines insuffisamment explorés, comme la santé mentale ou les pathologies chroniques. Il suggère également d'établir des croisements intersectoriels, notamment avec les champs environnementaux et sociaux, pour enrichir le patrimoine de données en santé et favoriser une approche plus holistique de la recherche médicale. Par exemple, l'intégration de données environnementales pourrait permettre d'étudier l'impact des facteurs environnementaux sur la santé et de développer des stratégies de prévention plus efficaces.

Ainsi, le rapport MARCHAND-ARVIER est une mine d'or et gage d'optimisme pour l'avenir. Si les recommandations proposées sont appliquées cela permettrait d'exploiter pleinement le potentiel des données de santé. La France peut espérer améliorer la qualité de ses soins, de sa recherche mais aussi renforcer sa position sur la scène internationale. Ces solutions représentent de ce fait une base solide pour libérer l'utilisation secondaire des données de santé et en maximiser les bénéfices pour la société.

Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel, JORF n°0113 du 16 mai 2024

L'arrêté du 26 avril 2024 modifiant l'arrêté publié le 29 juin 2019 s'adresse aux organismes publics ou privés qui hébergent, exploitent un système d'information contenant des données de santé à caractère personnel ou réalisent des sauvegardes pour le compte d'un établissement de santé ou d'un tiers de santé, et souhaitant obtenir la certification « Hébergeurs de données de santé » qui est opérationnelle depuis juillet 2018 (article L. 1111-8 du code de la santé publique).

Il décrit le processus d'accréditation des organismes de certification habilités à délivrer les certificats de conformité HDS (le COFRAC, en France ou son équivalent dans les autres États membres), exigeant, tout d'abord, le respect des exigences de la norme NF ISO 17021-1 (v. « 5.2. Exigences d'accréditation »). L'accréditation consiste à s'assurer que les organismes accrédités sont compétents et impartiaux, et qu'ils le demeurent dans le temps, quel que soit le contexte.

Cet arrêté fournit aussi des indications sur le processus de certification, qui nécessite du candidat hébergeur qu'il réponde aux exigences du référentiel de certification, et de l'organisme certificateur qu'il procède à l'audit de conformité (audit documentaire et audit sur site). L'hébergeur dispose alors de trois mois après la fin de l'audit pour corriger les éventuelles non-conformités et faire auditer ses corrections. Le certificat HDS est finalement délivré pour trois ans, et chaque année, un audit de surveillance est effectué.

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1), *JORF* n° 0117 du 22 mai 2024

La loi visant à sécurité et à réguler l'espace numérique, dite « Sren », a été publiée au Journal officiel le 22 mai 2024. Si le texte ne comportait initialement aucune disposition concernant directement les données de santé, il a été enrichi par les sénateurs puis les députés de deux articles additionnels permettant de renforcer les exigences de sécurité relatives à leur hébergement.

D'une part, **l'article 31** impose aux administrations de l'État, à ses opérateurs et aux groupes d'intérêt public (GPI) de s'assurer que les fournisseurs de services d'informatique en nuage (*cloud computing*) respectent des critères de sécurité et de protection contre l'accès aux données sensibles par des autorités publiques d'États tiers non autorisées par le droit de l'Union européenne ou d'un État membre, lorsqu'ils font appel à eux pour l'hébergement de ces données. Sont qualifiées de sensibles « les données qui relèvent de secrets protégés par la loi » et les « données nécessaires à l'accomplissement des missions essentielles de l'État notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes », ce qui intègre donc les données de santé. Un décret en Conseil d'État pris sous six mois devra détailler « les critères de sécurité et de protection, y compris en termes de détention du capital, des données [sensibles] ». Il sera également possible pour les ministres qui seront concernés par le projet nécessitant le recours à un service d'informatique en nuage, et après validation du premier ministre, d'accorder une « dérogation motivée et rendue publique », sans que celle-ci puisse excéder 18 mois à compter de la date à laquelle une offre de services d'informatique en nuage acceptable

est disponible en France. Ces dispositions s'appliquant expressément à l'Institut national des données de santé (INDS ou *Health Data Hub*), ce dernier devra alors recourir à une solution certifiée SecNumCloud par l'Agence nationale de la sécurité des systèmes d'information (Anssi).

D'autre part, **l'article 32** modifie l'article L. 1118-8 du code de la santé publique, en étendant la certification HDS, applicable aux hébergeurs de données de santé, aux fournisseurs de service d'archivage numérique de ces données à l'issue de leur durée de conservation au sens du RGPD, jusqu'à présent soumis à une procédure d'agrément spécifique du ministère de la culture. Ces nouvelles dispositions s'appliqueraient à une date fixée par décret, au plus tard le 1er juillet 2025, de manière à laisser aux acteurs concernés le temps de s'adapter.

Arrêté du 23 octobre 2023 modifiant l'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,

***JORF* n° 0253 du 31 octobre 2023**

L'espace numérique de santé (« Mon espace santé ») est un espace personnel proposé par l'État et l'Assurance maladie. Il a été créé par la loi n°2019-774 relative à l'organisation et la transformation du système de santé (loi OTSS)[227]. Il permet à chaque utilisateur de stocker et partager des documents et données de santé en toute sécurité. L'outil met ainsi en place un dossier médical partagé sur lequel chaque patient peut retrouver toutes ses informations de santé (traitements, résultats d'examens, ordonnances, etc.). Il permet également à l'utilisateur de renseigner son profil médical et d'avoir accès à une messagerie sécurisée avec les professionnels de santé. Enfin, cet espace propose un catalogue d'outils et de services numériques dont l'objectif est de permettre aux utilisateurs de trouver des services de qualité et de confiance en lien avec la santé[228]. Pris en application des articles L.1470-5, R.1111-37 et R.1111-39 du code de la santé publique, l'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[229], que le présent arrêté modifie, prévoit alors les critères applicables au référencement des services et outils numérique au catalogue de service de « Mon espace santé ».

Afin d'être référencés, l'arrêté de 2022 prévoit que les outils et services numériques doivent répondre à certaines exigences permettant de garantir leur qualité et leur sécurité. Le référencement assure donc aux utilisateurs que les outils et services numériques proposés satisfont à des exigences de sécurité et qu'ils peuvent ainsi les utiliser en toute confiance. L'arrêté de 2022 précise ainsi la procédure et les critères de référencement et indique les pièces justificatives et complémentaires obligatoires pour présenter une demande de référencement.

En ce qui concerne les nouveautés apportées par l'arrêté du 23 octobre 2023, celui-ci approuve une nouvelle version du référentiel relatif aux critères de référencement d'un outil ou service numérique dans « Mon espace santé »[230]. Ce référentiel est basé sur cinq thématiques : « urbanisation », « interopérabilité », « maturité sécurité », « éthique », et « sécurité pour le référencement avec échange de données ». Outre la simplification de certains critères dans cette nouvelle version, celle-ci apporte une nouveauté avec la partie sur la « sécurité pour le référencement avec échange de données » qui ne figurait pas dans sa version initiale de 2022. Cette nouvelle partie ajoute des critères relatifs à la sécurisation des outils et services numériques dans le cadre d'échanges de données avec « Mon espace santé » et impose la transmission de pièces justificatives pour attester de leur respect (Politique de sécurité des systèmes

[227] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n°0172 du 26 juillet 2019.

[228] Mon espace santé : ce qu'il faut savoir | ameli.fr | Assuré

[229] 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, *JORF* n° 0154 du 5 juillet 2022.

[230] Référentiel V2 relatif aux critères de référencement d'un outil ou service numérique dans « Mon espace santé », annexé à l'arrêté du 23 octobre 2023 modifiant l'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, *JORF* n° 0253 du 31 octobre 2023.

d'information, analyse de risques, rapport d'audit, description des protocoles et algorithmes de protection d'intégrité et confidentialité des données au repos et lors du transport, etc.).

Ces nouveaux critères, qui consistent en diverses obligations à l'endroit de l'industriel (en ce sens le verbe « devoir » est utilisé à l'impératif et s'écrit en majuscule : « L'industriel DOIT »), ont pour objet de se conformer aux exigences de sécurité prévues par le RGPD[231] et d'éviter l'exposition à des cyber-attaques, étant donné le caractère sensible des données de santé. Cet ajout fait référence à la suppression du deuxième alinéa de l'article 1er de l'arrêté dans sa version de 2022 qui indiquait que « *Les services conformes à ces seuls critères ne peuvent pas encore proposer à leurs utilisateurs d'échanger des données avec Mon espace santé.* »

Par conséquent, l'objet principal de l'arrêté est de prévoir les garanties nécessaires afin que les outils et services numériques référencés au catalogue de service de l'espace numérique de santé soient en mesure d'échanger des données avec l'espace numérique de santé des assurés lorsque l'ouverture des échanges de données avec celui-ci sera effective. Dans ce cadre, conformément à l'article L.1111-13-1 du code de la santé publique, l'accès aux données des utilisateurs sera conditionné à l'accord exprès de ces derniers, qui doivent être informés des finalités et des modalités de cet accès lorsqu'ils installent ces outils et services.

Par ailleurs, l'accès ne sera autorisé qu'à des fins de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour une durée de conservation qui doit être strictement proportionnée à ces finalités[232].

[231] Règlement n° 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données – RGPD), *JOUE* n° L 119 du 4 mai 2016.

[232] Article L.1111-13-1, paragraphe III, alinéa 2, code de la santé publique.

Loi de financement de la sécurité sociale pour 2024 Focus sur certaines dispositions

Loi n° 2023-1250 du 26 décembre 2023 de financement de la sécurité sociale pour 2024,
JORF n° 0299 du 27 décembre 2023

par Sarah BISTER

Avocate au Barreau de Paris,
Docteure en droit public

En France, la loi de financement de la sécurité sociale (« LFSS ») est une loi spécifique votée chaque année par le Parlement. Il s'agit d'une loi qui détermine les conditions générales de l'équilibre financier de la sécurité sociale, et compte tenu des prévisions des recettes, fixe ses objectifs de dépenses, dans les conditions et sous les réserves prévues par une loi organique[233]. Le projet de loi est présenté par le Gouvernement au Parlement au plus tard le 15 octobre de chaque année pour une adoption avant la fin de l'année.

La LFSS pour 2024 a été adoptée le 26 décembre 2023[234]. Composée de 115 articles, cette loi aborde de nombreux sujets. Le présent article n'a pas pour objet de revenir sur l'ensemble de la LFSS, mais de mettre l'accent sur certains articles intéressant notamment la téléconsultation.

I. MISE SOUS ACCORD PRÉALABLE OU SOUS OBJECTIF APPLICABLE DES SOCIÉTÉS DE TÉLÉCONSULTATIONS

Le premier article sur lequel va porter notre attention est l'article 63 de la LFSS. Cette disposition s'inscrit dans un chapitre consacré à la garantie de la soutenabilité du modèle social français. Cette disposition a pour ambition de diminuer les arrêts de travail non justifiés en améliorant et facilitant les contrôles tant sur les prescripteurs que sur les assurés. En France, sous certaines conditions, un arrêt de travail peut donner lieu pour celui qui en bénéficie à des indemnités journalières compensant la perte de revenus liée à la cessation temporaire de l'activité professionnelle. Le montant de ces indemnités journalières se chiffre en milliards d'euros chaque année et ne cesse d'augmenter. Face à cette hausse, le législateur a estimé nécessaire de renforcer les mesures de responsabilisation collective des prescripteurs et des assurés afin d'assurer la soutenabilité du système de santé français.

Le contrôle des assurés sociaux par l'assurance maladie ne sera pas abordé ici. Ce qui nous intéresse davantage est le contrôle des prescripteurs par le service du contrôle médical de l'assurance maladie. Celui-ci est amené à constater les abus en matière de prescription d'arrêt de travail. Pour ce faire, le médecin-conseil, - un agent des services de l'assurance maladie -, peut pratiquer des contrôles de prescriptions d'arrêt de travail d'un professionnel de santé, lorsque son activité de prescription sur ce sujet apparaît anormalement élevée comparativement à la pratique observée chez les professionnels de santé appartenant à la même profession et sur la base de profil de patients comparable. Le prescripteur peut alors être mis sous accord préalable (« MSAP ») ou mis sous objectif (« MSO »).

Certes, en droit français, le Code de la santé pose le principe de la liberté des prescriptions des médecins. Cela ne va pas sans un rappel déontologique du fait que les prescriptions et actes des médecins doivent être limités à ce qui est nécessaire à la qualité, sécurité et efficacité des soins[235]. La

[233] Article 34 de la Constitution française.
[234] Loi n°2023-1250 du 26 décembre 2023 de financement de la sécurité sociale pour 2024, JORF du 27 décembre 2023.
[235] Article R. 4127-8 du Code de la santé publique.

prescription des arrêts de travail n'échappe pas à ce principe.

La MSAP permet de subordonner à l'accord préalable du service du contrôle médical de l'assurance maladie, les prescriptions du médecin concerné s'il s'avère que ce dernier prescrit un nombre plus important d'arrêts de travail que ses confrères situés dans la même région et dans des domaines d'activité comparables. Cette MSAP peut être prononcée pour une durée maximale de six mois. Des sanctions financières peuvent, le cas échéant, être imposées au médecin prescripteur.

Dans un souci de transparence envers l'assuré à qui un arrêt de travail a été prescrit, celui-ci est informé, par courrier, que le prescripteur fait l'objet d'une MSAP et que sa prescription est sujette à des conditions particulières de prise en charge.
En alternative à la procédure de MSAP, la Caisse primaire d'assurance maladie (« CPAM ») peut proposer au prescripteur, conjointement avec le service du contrôle médical, d'opter pour la mise sous objectif. La MSO équivaut à un engagement du prescripteur à atteindre un objectif de réduction des prescriptions sous un délai déterminé[236]. Si le prescripteur refuse cette procédure, la CPAM engage la procédure de MSAP.

L'article 63 de la LFSS pour 2023 étend les procédures de MSAP et MSO aux centres de santé et aux sociétés de téléconsultation. Les sociétés de téléconsultation disposent d'un statut juridique ad hoc en droit français depuis la LFSS de 2023[237] et la publication du décret n°2024-164 du 29 février 2024[238]. Sans entrer plus avant sur le statut de ces sociétés, il s'agit de sociétés commerciales ayant pour objet de proposer une offre médicale de téléconsultations via des médecins qu'elles salarient[239].

Désormais, par modification de l'article L. 162-1-15 du Code de la sécurité sociale, les sociétés de téléconsultation peuvent également se voir appliquer les procédures de MSO ou MSAP.

II. LIMITATION DE LA PRESCRIPTION ET DE LA PRISE EN CHARGE DES PRODUITS ET DES ACTES EN TÉLÉCONSULTATION

L'article 65 de la LFSS pour 2024 se concentre sur la téléconsultation et notamment sur les arrêts de travail d'une durée supérieure à trois jours et la prescription de produits pris en charge par l'assurance maladie obligatoire.

S'agissant des arrêts de travail, le législateur a justifié l'instauration des nouvelles dispositions par la vigilance à accorder à la qualité des pratiques et la prise en compte des besoins des patients lorsque ceux-ci ont eu recours à une téléconsultation[240]. Il semblerait que le développement de la télémédecine et, plus spécifiquement des téléconsultations, se soit accompagné d'une augmentation des prescriptions d'arrêts de travail et de leur durée[241]. L'objectif est d'éviter la

[236] L'objectif de réduction ne peut être inférieur à la moyenne servant de base de référence. Le délai laissé au prescripteur pour atteindre l'objectif fixé est de quatre à six mois à compter de la date de réception de la proposition de MSO. Dans le cas où le prescripteur accepte la MSO, si, au terme de délai imparti, l'objectif n'est pas atteint, la Caisse primaire d'assurance maladie est susceptible d'engager la procédure de pénalité financière prévue à l'article L. 114-17-1 du Code de la sécurité sociale.

[237] LOI n° 2022-1616 du 23 décembre 2022 de financement de la sécurité sociale pour 2023, *JORF* du 24 décembre 2022.

[238] Décret n° 2024-164 du 29 février 2024 relatif aux sociétés de téléconsultation, JORF du 1er mars 2024.

[239] Voir notamment article L. 4081-2 du Code de la santé publique.

[240] Exposé des motifs du projet de loi, article 28, p. 80.

[241] Selon une étude de la Caisse nationale d'assurance maladie, des augmentations de plus de 100% ont été constatées en 2021 comparativement à l'année précédente, augmentation qui s'est également vérifiée en 2022 avec une hausse de nouveau équivalente à 100% sur le premier trimestre 2022 par rapport à 2021. Sur ce point cf. Fiches d'évaluation préalable des articles du projet de loi, article 28 – Limitation de la durée des arrêts de travail prescrits en téléconsultation et limitation de la prise en charge des prescriptions aux

surconsommation de soins non justifiée qui pourrait être facilitée par le développement des plateformes de téléconsultations.

L'article L. 6316-1 du Code de la santé publique définissant la télémédecine est désormais complété par un alinéa disposant que *« lors d'un acte de télémédecine, la prescription ou le renouvellement d'un arrêt de travail ne peut porter sur plus de trois jours ni avoir pour effet de porter à plus de trois jours la durée d'un arrêt de travail déjà en cours »*. L'article se poursuit en introduisant toutefois deux atténuations.

La première concerne le cas où la prescription ou le renouvellement de l'arrêt de travail est accordé par le médecin traitant du patient ou sa sage-femme référente. Cette dérogation au principe d'interdiction s'explique par la connaissance préalable du patient par le professionnel médical. Un professionnel médical qui suit régulièrement le patient a connaissance de ses antécédents, de son état de santé et de l'environnement au sein duquel il évolue, ce qui lui permet, quand bien même il n'y aurait (pas) d'examen physique, d'apprécier plus justement la situation par téléconsultation que ne pourrait le faire un médecin ou une sage-femme qui ne connaît pas le patient.

La seconde atténuation couvre les cas dans lesquels le patient peut justifier d'une impossibilité d'obtenir une consultation en présentiel pour le renouvellement de son arrêt de travail. Ces cas peuvent se présenter notamment lorsque le patient réside en zone de faible densité médicale, lorsque son médecin traitant est absent ou indisponible et qu'il n'a pas de remplaçant. L'ensemble des difficultés d'accès aux soins est couvert.

Ce nouvel alinéa de l'article L. 6316-1 du Code de la santé publique a fait l'objet de contestation auprès du Conseil constitutionnel dans le cadre du contrôle a priori du projet de loi. Les députés à l'origine de la saisine soutenaient que les deux exceptions prévues étaient rédigées de manière trop restrictive ayant pour effet d'empêcher certains patients d'obtenir un arrêt de travail d'une durée de plus de trois jours, alors même que leur état de santé l'exigerait. Selon eux, une telle disposition était contraire au Préambule de la Constitution française aux termes duquel la Nation garantit à tous la protection de la santé[242] et un droit à ouverture aux prestations sociales.

Les Sages ont rejeté cette position pour trois motifs.

Premièrement, le Conseil constitutionnel considère que l'objectif annoncé du législateur consistant à favoriser la qualité des soins et éviter les risques d'abus liés à la prescription d'arrêt de travail dans le cadre d'une téléconsultation est rempli. Selon lui, cet objectif poursuit une finalité d'intérêt général et vise à lutter contre la fraude en matière de protection sociale qui est reconnu comme un objectif de valeur constitutionnelle.

Deuxièmement, le Conseil constitutionnel évoque, sans s'y attarder, les exceptions au principe de non-renouvellement d'un arrêt de travail. La lecture de la décision du Conseil constitutionnel n'est pas vraiment éclairante sur ce point.

Enfin, pour le Conseil constitutionnel, il existe une obligation d'information du patient nécessitant un arrêt de travail d'une durée supérieure à trois jours sur les conditions dans lesquelles il peut obtenir la prolongation de cet arrêt. Là encore, le Conseil constitutionnel n'est pas plus éloquent que cela. Ce motif est intéressant dans la mesure où cette obligation découle « seulement » d'un devoir d'information des médecins et sages-femmes. Rien dans la nouvelle rédaction de l'article 6316-1 du Code de la santé publique ne fait référence à cette obligation.

Par conséquent, ce nouvel article est désormais entré dans le droit commun.

téléconsultations avec vidéotransmission ou échange téléphonique, p. 290.

[242] Alinéa 11 du Préambule de la Constitution de 1946.

L'article 65 de la LFSS pour 2024 fait état d'une seconde nouveauté. Désormais, une prise en charge par l'assurance maladie de traitements, d'examens ou des soins prescrits lors d'une téléconsultation ou d'un télésoin ne sera possible que si la téléconsultation a été réalisée via vidéotransmission ou contact téléphonique avec le patient. Jusqu'à présent si la consultation, en elle-même, pour être remboursée au patient supposait d'avoir été réalisée en visio ou par téléphone, rien n'était prévu pour les actes et produits prescrits. Autrement dit, la téléconsultation pouvait ne pas être prise en charge par l'assurance maladie contrairement aux actes et prescriptions. Cette nouvelle disposition découle de la constatation de pratiques réalisées par certaines plateformes en ligne délivrant des ordonnances à des patients sur la base de réponses apportées à un questionnaire ou via un outil de conversation en ligne (chat ou sms). La qualité de la prise en charge du patient pose réellement question dans ces cas précis. C'est pourquoi dorénavant, un échange oral avec le patient sera nécessaire si celui-ci entend bénéficier d'une prise en charge des actes et produits prescrits.

III. REJET DE CERTAINES DISPOSITIONS VISANT À GARANTIR ET SÉCURISER L'ACCÈS DES FRANÇAIS AUX MÉDICAMENTS DU QUOTIDIEN ET AUX PRODUITS DE SANTÉ INNOVANTS

Deux dispositions seront abordées dans cette partie.

La première porte sur l'article 72 de la LFSS pour 2024. Cet article renforce les leviers d'épargne de médicaments en cas de rupture d'approvisionnement. Autrement dit, parmi les dispositions proposées, le législateur souhaitait interdire la prescription d'antibiotiques en téléconsultation, lors de situations de pénuries identifiées, au motif qu'une telle prescription suppose un examen clinique du patient. Toutefois, cette interdiction aurait pu être levée en cas de situations épidémiques ayant donné lieu à des consignes de réduction de déplacements, de cas de prophylaxie antibiotique ne nécessitant pas d'examen clinique comme par exemple les antibiotiques prescrits avant une intervention de chirurgie dentaire ou dans le cas de la maladie de Lyme et, enfin, pour les antibiotiques pour les lesquels un test rapide d'orientation diagnostique (TROD) peut être utilisé en pharmacie d'officine pour confirmer la délivrance d'antibiotiques.

Cette disposition de l'article 72 de la LFSS a été déférée au Conseil constitutionnel au motif qu'elle pourrait engendrer une impossibilité pour certains patients ne pouvant consulter physiquement un médecin de se voir prescrire un médicament essentiel eu égard à leur état de santé. Pour les parlementaires auteurs de la saisine, outre la violation du principe constitutionnel de la garantie offerte à tous à la protection de santé, c'est également le principe d'égalité devant la loi qui est bafoué.

Le Conseil constitutionnel a jugé que la disposition en cause n'était pas conforme à la Constitution car elle pourrait avoir pour effet de priver un patient de se voir prescrire un traitement nécessaire pour lui en raison d'une téléconsultation et non d'une consultation en présentiel. Les quelques explications des Sages laissent penser que si le législateur avait assorti cette disposition de quelques exceptions supplémentaires, telles que le recours au médecin traitant pour la téléconsultation ou l'impossibilité d'obtenir une consultation en présentiel avec un médecin dans un délai compatible avec son état de santé, elle aurait pu être jugée conforme à la Constitution.

La position retenue par le Conseil constitutionnel est tout à fait louable, à notre sens, dans la mesure où le législateur s'efforce depuis des années à faire reconnaître la télémédecine, non comme une forme de médecine différente de la

médecine en présentiel, mais seulement comme une activité médicale à part entière garantissant la sécurité de la prise en charge.

La seconde disposition, ayant été rejetée par le Conseil constitutionnel, sur laquelle nous nous attarderons dans les prochaines lignes, concerne l'article 75 du projet de loi. Cet article découlait d'un amendement du Gouvernement dont l'objet était de modifier l'article L. 162-16-6 du Code de la sécurité sociale en ajoutant le point suivant :
« Les prescripteurs recueillent les données de suivi des patients traités, selon des modalités définies par décret. Ces données sont transmises, dans des conditions assurant le respect du secret médical, au Comité économique des produits de santé ainsi qu'à l'entreprise titulaire des droits d'exploitation, à l'entreprise assurant l'importation parallèle ou à l'entreprise assurant la distribution parallèle du médicament. L'entreprise titulaire des droits d'exploitation, l'entreprise assurant l'importation parallèle ou l'entreprise assurant la distribution parallèle du médicament participe en tout ou partie au financement du recueil des données »[243].

La justification de cet amendement repose sur la volonté de faciliter la transmission des données d'efficacité portant sur la performance des médicaments de thérapie innovante[244] au comité économique des produits de santé (« CEPS »). Depuis la LFSS pour 2023[245], les médicaments de thérapie innovante font l'objet d'un paiement à la performance. Cela signifie que l'étude des données en vie réelle de ces médicaments peut amener à la réévaluation du prix ou au versement de remises.

L'article 75 du projet de loi prévoyait que les prescripteurs recueillent les données de suivi des patients traités selon des modalités définies par décret. Ces données devaient ensuite être transmises au CEPS ainsi qu'à l'entreprise titulaire des droits d'exploitation, assurant l'importation parallèle ou celle chargée de la distribution parallèle du médicament. Aussi, il était mentionné explicitement que les industriels participaient financièrement, et ce de manière obligatoire, au recueil des données via un outil spécifique.

Cet article a été supprimé de la version du texte de loi après que le Conseil constitutionnel, saisi de sa conformité, a estimé qu'il s'agissait d'un cavalier législatif. En d'autres termes, la disposition envisagée n'avait *« pas d'effet ou un effet trop indirect sur les dépenses ou les recettes des régimes obligatoires de base ou des organismes concourant à leur financement »*[246]. Cela ne présume pas pour autant de la conformité ou non de cette disposition à la Constitution puisque la question même de la conformité n'a pas été abordée. Cette disposition sera peut-être donc prochainement proposée dans un autre projet ou proposition de loi de santé.

[243] Amendement n°3086 déposé le vendredi 20 octobre 2023 par le Gouvernement.
[244] Les médicaments de thérapie innovante recouvrent les médicaments de thérapie génique, les médicaments de thérapie cellulaire somatique, les produits issus de l'ingénierie tissulaire et les médicaments combinés de thérapie innovante.
[245] Article 54 de la loi de financement de la sécurité sociale pour 2023.
[246] Point 88 de la décision n°2023-860 DC du 21 décembre 2023.

La reconnaissance des sociétés de téléconsultation en droit français comme véritables opérateurs de santé ?

Décret n°2024-164 du 29 février 2024 relatif aux sociétés de téléconsultation, *JORF* n° 0051 du 1er mars 2024

par Sarah BISTER

Avocate au Barreau de Paris,
Docteure en droit public

Si la crise sanitaire du Covid-19 a eu d'innombrables impacts négatifs, on lui doit toutefois le développement, en France, de la télémédecine, plus particulièrement des téléconsultations. La télémédecine n'en était encore qu'à ses balbutiements plus de dix ans après l'instauration d'un cadre légal[247]. Avec l'essor de la télémédecine, se sont multipliées les sociétés commerciales proposant des téléconsultations réalisées par des médecins salariés. Jusqu'à la loi de financement de la sécurité sociale (LFSS) pour 2023[248], l'activité de ces sociétés n'était pas réglementée. Leur structuration juridique, alors considérée comme non suffisamment pérenne par les pouvoirs publics, ne permettait pas la facturation des prestations à l'assurance maladie[249] : ainsi, les téléconsultations réalisées via de telles sociétés n'étaient pas prises en charge par l'assurance maladie[250].

Pour autant, ces sociétés permettent de pallier un besoin de soins de la population : soit ponctuellement pour les patients résidant dans des zones sous denses en offre médicale, soit pour des patients ne disposant pas d'un médecin traitant.

Du côté de la structuration juridique, le problème résidait dans le fait que les professionnels de santé autorisés à facturer des soins pris en charge par l'assurance maladie étaient strictement listés par la Code de la sécurité sociale[251] : professionnels de santé en exercice libéral, professionnels de santé salariés d'un autre professionnel de santé libéral, professionnels de santé d'une maison de santé, professionnels de santé salariés d'un centre de santé, professionnels de santé salariés d'un établissement de santé ou encore d'un établissement social et médico-social. Les sociétés de téléconsultation n'y trouvaient pas leur compte : aucun de ces statuts juridiques n'était adapté à ce qu'elles proposaient. Si des montages juridiques ont bien été envisagés et mis en œuvre, ils se sont rapidement vu retoqués par les autorités[252].

C'est dans ce contexte que la LFSS pour 2023 a proposé la création d'un statut *ad hoc* pour ces sociétés afin de clarifier les exigences liées aux modalités d'exercice. L'article 53 de la LFSS pour 2023 prévoyait que ses dispositions entreraient en vigueur dans des conditions et à une date fixées par décret et, au plus tard, le 31 décembre 2023. Finalement, il a fallu attendre le 1er mars 2024, pour que le décret n°2024-164 du 29 février 2024 relatif aux sociétés de

[247] C'est à la loi n°2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (dite loi « HPST ») que l'on doit la réglementation de la télémédecine en France. Les actes de télémédecine ont été définis par le décret n°2010-1229 du 19 octobre 2010.

[248] Loi n°2022-1616 du 23 décembre 2022 de financement de la sécurité sociale pour 2023, *JORF* du 24 décembre 2022.

[249] Hormis pour les sociétés disposant d'un numéro FINESS dans le cadre dérogatoire des expérimentations de l'article 51 de la LFSS pour 2018.

[250] La prise en charge de téléconsultations a cependant pu être accordée sous certaines conditions pendant la période Covid-19, notamment pendant les confinements.

[251] Article 162-1-7 du Code de la sécurité sociale.

[252] Nous faisons ici référence aux sociétés de téléconsultation qui ont créé des associations pour gérer des centres de santé virtuels, ce que le législateur ne permettait pas.

téléconsultation[253] soit publié au Journal officiel.

Ce décret précise les conditions de délivrance de l'agrément pour les sociétés éligibles, l'agrément est un gage de la qualité de leurs pratiques des téléconsultations (**I**). Du côté des médecins salariés, le législateur a également entendu garantir les conditions de leur intervention, notamment via un contrôle de la gouvernance médicale (**II**).

I. L'AGRÉMENT OU L'ASSURANCE DE LA QUALITÉ DES PRATIQUES DE TÉLÉCONSULTATIONS PAR LES SOCIÉTÉS DE TÉLÉCONSULTATION

Aux termes de l'article L. 4081-2 du Code de la santé publique, les sociétés de téléconsultation sont des sociétés commerciales, dont l'objet – à titre exclusif ou non – est de proposer une offre médicale de téléconsultations. Afin d'éviter tout conflit d'intérêt, les sociétés de téléconsultation ne peuvent pas être détenues par des personnes physiques ou morales exerçant une activité de fournisseur, de distributeur ou de fabricant de médicaments, de dispositifs médicaux ou de dispositifs médicaux de diagnostic in vitro. Enfin, ces sociétés doivent se conformer aux dispositions relatives à la protection des données à caractère personnel.

Jusqu'au décret n°2024-164, les sociétés de téléconsultation devaient être adossées à un centre de santé pour pouvoir employer des médecins et établir des factures auprès de l'assurance maladie. Ces sociétés pourront dorénavant salarier des médecins pour autant qu'elles soient agréées. L'agrément concerne uniquement les sociétés de téléconsultation salariant des médecins et proposant des téléconsultations aux patients. Cela signifie que ne pourront pas être agréées les sociétés proposant seulement des outils de mise en relation entre patients et médecins pour la réalisation de téléconsultation mais qui ne salarient pas ces médecins. Les accompagnements à la téléconsultation par des professionnels de santé ou les téléconsultations réalisées par les sages-femmes ne sont pas concernés par l'agrément.

L'agrément est délivré par les ministres chargés de la santé et de la sécurité sociale. La demande d'agrément, adressée par voie dématérialisée, comporte, outre les informations d'identification de la société, la description prévisionnelle de l'organisation mise en place pour garantir le respect des exigences relatives à la réunion régulière d'un comité médical, l'élaboration d'un programme d'actions et la transmission chaque année au Conseil national de l'ordre des médecins et aux ministres compétents d'un rapport sur ses activités.

La demande est également accompagnée d'une attestation par laquelle le représentant légal de la société certifie s'engager à respecter les règles de prise en charge des téléconsultations fixées par la convention nationale, la présentation sur le site internet de toutes les mentions d'informations sur les frais auxquels la personne pourrait être exposée à l'occasion de la téléconsultation et le référentiel de bonnes pratiques professionnelles relatives à la qualité et à l'accessibilité de la téléconsultation, qui a été publié par la Haute Autorité de santé le 21 décembre 2023[254]. Afin d'aider les sociétés à déposer leur demande, le ministère du travail, de la santé et des solidarités met à disposition un document type[255].

Enfin, le demandeur doit joindre le certificat de conformité au référentiel applicable aux systèmes d'informations de téléconsultation défini par un arrêté du 9

[253] Décret n° 2024-164 du 29 février 2024 relatif aux sociétés de téléconsultation, *JORF* du 1er mars 2024.
[254] Haute Autorité de santé, Référentiel de bonnes pratiques et méthodes d'évaluation applicables aux sociétés de téléconsultation, Validé par le Collège le 21 décembre 2023.
[255] Attestation de conformité relatif à la demande d'agrément pour les sociétés de téléconsultation.

février 2024[256], certificat délivré par l'Agence du numérique en santé.

Les ministres compétents peuvent demander à la société de téléconsultation de leur communiquer tout document permettant d'assurer l'exactitude du contenu de la demande d'agrément et du respect de tous les engagements qui s'imposent à elle.

Dès lors que le dossier est complet, la société reçoit un récépissé. L'agrément est délivré dans un délai de quatre mois. A défaut de demande de complément ou de réponse dans ce délai, la demande est réputée acceptée. Si une demande de complément est adressée à la société, celle-ci dispose de minimum dix jours pour apporter une réponse. Pendant ce laps de temps, le délai des quatre mois est suspendu. Si la société ne respecte pas le délai imparti pour communiquer les éléments complémentaires, la demande est réputée rejetée. Tout refus de demande d'agrément devra être motivé.

L'agrément est délivré pour une durée de deux ans. Tout changement substantiel affectant les éléments ayant permis la délivrance de l'agrément devra être déclaré dans le délai d'un mois auprès des ministres compétents.

Au moins quatre mois avant l'échéance de l'agrément, la demande de renouvellement doit être présentée dans les mêmes conditions que la demande initiale. Le renouvellement de l'agrément est alors valable pour une durée de trois ans.

L'agrément pourra être suspendu ou retiré si l'ensemble des exigences à respecter ne le sont plus. Notamment les manquements portant atteinte à la sécurité des patients pourront conduire à une suspension de l'agrément et à une mise en conformité dans un délai imparti. En revanche, en cas de fraude à l'égard de l'assurance maladie dans le cadre des activités de téléconsultation, le retrait définitif de l'agrément sera prononcé.

II. LE CONTROLE DE LA GOUVERNANCE MEDICALE OU LA GARANTIE D'INTERVENTION DES MEDECINS SALARIES

Dès lors qu'une société de téléconsultation agréée salarie plusieurs médecins, elle est tenue de les réunir régulièrement en un comité médical. Le décret a précisé que ces réunions devaient avoir lieu, dès lors que la société l'estime nécessaire pour mettre en œuvre ses missions et a minima trois fois par an. La société de téléconsultation doit s'assurer que le comité médical dispose des moyens logistiques pour lui permettre de réaliser ses réunions.

Le comité a une triple finalité :

- donner son avis sur la politique médicale de la société et sur le programme d'actions visant à garantir le respect de ses obligations. Le programme d'actions est assorti d'indicateurs de suivi. L'article D. 4081-5 du Code de la santé publique mentionne que des critères communs aux indicateurs de suivi du programme d'actions sont définis par arrêté ministériel ;
- contribuer à la définition de sa politique médicale et l'élaboration de la politique d'amélioration continue de la qualité et de la sécurité des soins ;
- s'assurer de la cohérence de la formation médicale continue des médecins salariés.

S'agissant de la composition de ce comité, lorsque la société salarie jusqu'à deux médecins, le comité est composé de tous les médecins salariés et d'un représentant des usagers. Si l'effectif de la société comprend trois médecins ou plus, le

[256] Arrêté du 9 février 2024 approuvant le référentiel d'interopérabilité, de sécurité et d'éthique des systèmes d'informations de téléconsultation et définissant la procédure de délivrance du certificat de conformité des systèmes d'information des sociétés de téléconsultation en application du 3° de l'article L. 4081-2 du code de la santé publique, *JORF* du 11 février 2024, NOR : TSSD2400438A.

comité est alors composé des médecins salariés élus par leurs pairs au scrutin secret uninominal majoritaire, éventuellement à deux tours, et d'un minimum de deux représentants des usagers, ceux-ci étant désignés parmi les membres d'associations agréées ou proposées par elles.

Au plus, le comité comporte douze membres. Il ne délibère sur première convocation que si la moitié au moins des membres sont présents. Si ce n'est pas le cas, le comité se réunit alors sur nouvelle convocation huit jours plus tard et délibère valablement quel que soit le nombre de membres présents. C'est au comité lui-même de définir son organisation, son fonctionnement, ses modalités de représentations des médecins salariés et ses modalités de désignation de sa présidence. Le décret précise que le représentant légal de la société peut être entendu à la demande des membres du comité, de même que toute personne extérieure dont l'expertise pourrait être utile au bon déroulement de ses missions, sur un point inscrit à l'ordre du jour. Ces personnes n'ont pas de voix délibérative et assistent uniquement à la partie des débats qui justifie leur présence.

A minima, le représentant légal sera entendu au moins une fois par an par les membres du comité médical.

Le secret professionnel s'impose aussi bien aux membres du comité médical qu'aux personnes qu'il est amené à entendre.

Afin que l'indépendance du comité soit assurée, les médecins qui en sont membres ne peuvent ni avoir de part ou d'actions, ni de titres, ni exercer de fonctions dirigeantes au sein de la société qui les salarie.

Outre la gouvernance médicale, les médecins exerçant dans des sociétés de téléconsultations seront assurés de pouvoir exercer dans le respect des règles déontologiques qui leur sont applicables. A titre d'exemple, l'indépendance des médecins prévue à l'article R. 4127-5 du Code de la santé publique[257] devra être respectée en toute circonstance. Les sociétés de téléconsultation devront également porter une attention des plus vigilantes lorsqu'elles réaliseront des actes de communication sur leurs activités afin de ne pas mettre à mal les principes déontologiques des médecins en termes de communication et de publicité.

Les sociétés de téléconsultations devront aussi garantir que les médecins salariés respectent les règles de prise en charge de l'assurance maladie et le volume d'activité à distance. En effet, tant la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie que l'accord national destiné à organiser les rapports entre les centres de santé et les caisses d'assurance maladie fixent à 20% maximum le volume d'activité pouvant être réalisé à distance sur une année civile[258]. Ce plafond de 20% s'entend des activités de téléconsultation et de téléexpertise. Il n'est effectivement aujourd'hui pas possible pour un médecin conventionné de réaliser un exercice exclusivement en distanciel. Aussi, même si les sociétés de téléconsultation n'étaient pas adossées à un centre de santé, ce plafond de 20% reste tout de même applicable aux médecins salariés en raison du respect de leur propre convention nationale qui s'impose à eux.

Du côté des patients, précisons que ceux-ci ne pourront être redevables pour une téléconsultation que des tarifs fixés conventionnellement. Autrement, la tarification des consultations ne sera plus libre pour les sociétés agréées, les autres restant libres de déterminer les prix qu'elles souhaitent. Des prestations complémentaires optionnelles payantes pourront être proposées aux patients, sous

[257] Aux termes de cet article, *« le médecin ne peut aliéner son indépendance professionnelle sous quelque forme que ce soit »*.

[258] Arrêté du 22 septembre 2021 portant approbation de l'avenant n°9 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, *JORF* du 25 septembre 2021, NOR : SSAS2128599A.

réserve que ceux-ci en aient reçu une information préalable. Ce dernier point entrera en vigueur le 1er septembre 2024, soit six mois après la publication du décret. Ce délai doit permettre aux sociétés de se mettre en conformité et d'adapter leur modèle économique, qui jusque-là, prévoyait pour nombre d'entre elles des frais de service aux patients.

Les autres dispositions sont, quant à elles, applicables depuis le 2 mars 2024. Il ne fait pas de doute que l'avènement de ce statut juridique *ad hoc* pour les sociétés de téléconsultation est un pas important vers la reconnaissance de leur rôle dans l'offre de soins aux patients résidant en France. Avec le développement (tant attendu) de la télémédecine, face aux déserts médicaux de plus en plus nombreux et aux difficultés pour les patients de trouver un médecin traitant, le législateur se devait de considérer plus attentivement l'activité de ces nouveaux acteurs. Mais alors est-ce que la reconnaissance des sociétés de téléconsultations comme nouveaux offreurs de soins est au rendez-vous ? Une réponse mitigée est de mise à plusieurs égards. On ne peut que remarquer la place particulière qui a été donnée à ces sociétés dans le Code de la santé publique. On aurait pu légitimement s'attendre à ce que les dispositions légales afférentes soient intégrées à la sixième partie du Code de la santé publique consacrée aux « autres services de santé » : attribuer une place aux sociétés de téléconsultation à côté de celle dédiée aux maisons et centres de santé n'aurait pas été surprenante. Ce qu'il l'est davantage, et qui traduit la position du législateur, c'est d'avoir lié les dispositions relatives aux sociétés de téléconsultation à celles consacrées aux professionnels de santé prévues par la quatrième partie du Code de la santé publique. Cette position est toutefois pleinement assumée puisque le législateur n'a pas hésité à préciser, dans l'analyse d'impact du projet de loi, que les sociétés de téléconsultation seront positionnées « en subsidiarité de l'offre de soins existante » (Fiches d'évaluation préalable des articles du projet de loi, article 28 – Régulation des sociétés de téléconsultation facturant à l'assurance maladie obligatoire, p. 175). C'est donc une place subsidiaire qui est laissée à ces sociétés et non, pour le moment, une reconnaissance en tant qu'offreur de soins « classique ». Il est peut-être encore trop tôt pour savoir si les règles fixées par la LFSS pour 2023 et le décret n°2024-164 sont adaptées au développement de ces sociétés ou si, au contraire, elles sont trop contraignantes pour pérenniser leur structuration dans l'environnement des offreurs de soins conventionnés

L'organisation et le fonctionnement du Service d'accès aux soins (SAS) davantage précisés

Le Service d'accès aux soins (SAS), pour « évaluer le besoin en santé de toute personne qui le sollicite, (…) délivrer à celle-ci les conseils adaptés et (…) faire assurer les soins appropriés à son état » (article L. 6311-2, code de la santé publique) procède en deux étapes. D'abord, un assistant de régulation médicale (ARM) qualifie chaque appel. Ensuite, en fonction de cette qualification et du degré d'urgence réel, la personne qui appelle le SAS est prise en charge soit par le service d'aide médicale urgente, soit par la régulation de médecine ambulatoire. Cette dernière est portée à la fois par des médecins régulateurs généralistes (professionnels médicaux, docteurs juniors, médecins remplaçants) et des opérateurs de soins non programmés (ONSP) qui assistent les premiers dans leur mission d'orientation des patients (prise de rendez-vous pour une consultation en cabinet ou à domicile, accès à une téléconsultation ou à des télésoins, orientation vers un établissement de santé). Les acteurs de la chaîne de régulation peuvent notamment s'appuyer sur la « plateforme numérique du Service d'accès aux soins », leur permettant, d'une part, de visualiser les créneaux ou plages disponibles des effecteurs de soins participant au SAS et, d'autre part, de réserver pour le patient un rendez-vous dans un délai de 48 heures.

Décret n° 2024-541 du 14 juin 2024 relatif à l'organisation et au fonctionnement du service d'accès aux soins,
***JORF* n° 0139 du 15 juin 2024**

EN SAVOIR PLUS

Décret n° 2023-1222 du 20 décembre 2023 relatif à la mise en œuvre de la prescription électronique,

***JORF* n° 0295 du 21 décembre 2023**

Prise en application de la loi n°2019-774 relative à l'organisation et à la transformation du système de santé (loi OTSS)[259], l'ordonnance n°2020-1408 portant mise en œuvre de la prescription électronique[260] pose le principe de la dématérialisation des prescriptions de soins, de produits de santé et de prestations établies ou exécutées par les professionnels de santé. L'ordonnance établit alors que les professionnels de santé autorisés à prescrire utilisent la prescription électronique et établissent ainsi leurs prescriptions de manière dématérialisée et les transmettent pas l'intermédiaire des téléservices mis à disposition par la Caisse nationale de l'assurance maladie (CNAM)[261]. De même, les professionnels de santé exécutant les prescriptions transmettent les données qui y sont relatives par l'intermédiaires des téléservices mentionnés[262]. La prescription électronique s'entend ainsi comme « *la dématérialisation des prescriptions de soins, de produits de santé et de prestations établies ou exécutées par les professionnels de santé et leur transmission à l'assurance maladie par voie électronique.* »[263]. Le déploiement de la prescription dématérialisée s'inscrit dans le cadre du programme du Ségur du numérique en santé qui a pour but de soutenir le développement du numérique en santé en France.

Ainsi, conformément à l'article L.4071-6 du code de la santé publique, le présent décret définit les conditions de mise en œuvre et d'entrée en vigueur de la prescription électronique. Il prévoit également les droits des patients dans le cadre de ces prescriptions dématérialisées et de leurs conditions d'exécution. Enfin, le décret précise les situations dans lesquelles, par dérogation, la dématérialisation pourra ne pas être mise en œuvre. Les professionnels de santé devront se conformer à l'obligation de dématérialisation des prescriptions au plus tard le 31 décembre 2024 (article 5, présent décret).

Les professionnels de santé devront se conformer à l'obligation de dématérialisation des prescriptions au plus tard le 31 décembre 2024

Premièrement, le décret prévoit que la CNAM assure la conception et la mise en œuvre des traitements de données dans le cadre de la dématérialisation des prescriptions. A ce titre, c'est elle qui développe et met à disposition des professionnels les téléservices permettant la transmission des prescriptions et des informations sur leur exécution et la centralisation de ces données (article R.4071-1, code de la santé publique).

Les logiciels utilisés par les professionnels de santé pour prescrire et informer sur l'exécution des prescriptions (au moyen desquels les professionnels de santé utilisent les téléservices de la CNAM) doivent avoir obtenu un agrément délivré par la CNAM et qui assure, au regard du respect de spécifications techniques, leur capacité de fonctionner avec les téléservices de la CNAM (article R.4071-2, code de la santé

[259] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, *JORF* n°0172 du 26 juillet 2019.
[260] Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique, *JORF* n°0280 du 19 novembre 2020.
[261] Articles L.4071-1 et L.4071-3, code de la santé publique.
[262] Article L4071-2, code de la santé publique.
[263] Voir notice du décret.

publique). Par ailleurs, le décret précise que les données renseignées dans le cadre de la dématérialisation des prescriptions sont conservées pendant une durée de cinq ans à compter de la rédaction de la prescription.

Deuxièmement, concernant les droits des patients, le décret prévoit que ceux-ci peuvent s'opposer à ce que le professionnel de santé prescripteur consulte les données d'exécution de la prescription électronique, au moment de l'établissement de celle-ci ou ultérieurement (article R.4072-1, code de la santé publique).

Dans les cas où cela est nécessaire pour la coordination et au suivi du parcours de soin du patient, les différents professionnels de santé qui suivent un patient peuvent avoir accès aux informations relatives aux prescriptions de ce patient et à leur exécution (article R.4072-2, code de la santé publique).

Le décret organise également l'accès à ces données dans le cadre des personnes mineures non émancipées et des personnes prises en charge pour une interruption volontaire de grossesse (articles R.4072-4 et R.4072-5, code de la santé publique).

Enfin, lorsqu'un professionnel de santé établit une prescription électronique, il en remet une copie papier à son patient, à moins que ce dernier indique qu'il préfère la recevoir dans la messagerie sécurisée proposée par l'espace numérique de santé (« Mon espace santé »). Dans ce cadre, l'ordonnance papier ou numérique contient un dispositif d'identification permettant aux professionnels exécutant la prescription d'avoir accès à la prescription électronique (article R.4072-3, code de la santé publique).

Troisièmement, le décret prévoit des exceptions à l'obligation de dématérialisation dans différents cas de figure, tels que l'indisponibilité des téléservices gérés par la CNAM, une connexion internet insuffisante, l'absence d'une prescription dématérialisée pour le professionnel qui exécute la prescription, etc. (article R.4073-2, 1°, 2°, 3° et suivants, code de la santé publique).

Lorsque, pour une de ces raisons, la prescription ne peut être dématérialisée pour des médicaments ou produits destinés à la médecine humaine et classés comme stupéfiants ou soumis à la réglementation des stupéfiants, le décret prévoit que le prescripteur doit établir une prescription papier qui répond à des spécifications techniques, fixées par arrêté (article R.5132-5, code de la santé publique).

En conclusion, en pratique, le processus de prescription dématérialisée se déroule comme suit : le prescripteur renseigne les données de prescription dans son logiciel agréé par la CNAM. Ces données sont alors transmises et stockées dans la base e-prescription (téléservice géré par la CNAM). Un numéro unique d'identification est associé à chaque ordonnance et est accessible sur l'ordonnance papier ou numérique via un QR code. Par le biais de ce QR code, le professionnel de santé qui exécute la prescription peut consulter les données de prescription en accédant à la base e-prescription par l'intermédiaire de son logiciel, également agréé par la CNAM[264]. Par ailleurs, le décret indique que les données relatives aux prescriptions électroniques sont également transmises à l'assurance maladie par le biais des téléservices qu'elle a mis en place (article R.161-48, code de la sécurité sociale).

La mise en place de ce processus de prescription dématérialisée devrait permettre, d'une part, de renforcer la sécurité des prescriptions afin d'éviter les fraudes et, d'autre part, de permettre la transmission des ordonnances électronique dans un cadre transfrontière au sein de l'Union, notamment dans le cadre de la mise en œuvre de l'Espace européen des données de santé

[264] Ordonnance numérique | G_NIUS (esante.gouv.fr) et Ordonnance numérique | ameli.fr | Pharmacien.

Arrêté royal fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux praticiens de l'art dentaire pour l'utilisation de la télématique et pour la gestion des dossiers médicaux en 2023,

M.B. du 27 décembre 2023

Pour obtenir une intervention de l'Institut national d'assurance maladie-invalidité (INAMI) dans le coût afférent à l'utilisation de la télématique et à la gestion électronique des dossiers médicaux pour l'année 2023, le praticien dentaire doit atteindre durant l'année de la prime des seuils d'utilisation des services de la plateforme « MyCareNet ». Qu'il s'agisse de consulter l'assurabilité du patient (articles 4, §1, 1° et §2, 1°), les tarifs des prestations dispensées (article 4, §1, 2° et §2, 2°), le DMG du patient (article 4, §1, 4° et §2, 4°) ou de facturer en tiers payant via la facturation électronique (article 4, §1, 3° et §2, 3°).

EFPIA, Improving access to digital therapeutics in Europe, June 2023

par Dorianne CATTOEN

Étudiante en Master de droit européen
Université Toulouse Capitole

Le rapport de la Fédération européenne des associations et industries pharmaceutiques, EFPIA, de juin 2023, présente des recommandations pour améliorer l'accès aux thérapies numériques (DTx). Les thérapies numériques sont des innovations fondées sur des données probantes, destinées aux patients[265]. Ces thérapies se basent sur un programme de logiciel afin de prévenir, gérer, alléger ou traiter la pathologie médicale. Actuellement, les DTx sont soumises au règlement 2017/745[266]. L'article 2, définissant un dispositif médical (DM), ~~comprend définition~~ inclut les DTx comprenant l'intervention d'un composant matériel associé avec le logiciel comme composant moteur de l'effet thérapeutique. Elles peuvent prendre la forme d'une application connectée par exemple.

Ces innovations représentent un enjeu important pour l'Union européenne (UE), car elles profitent à toute la société. Tout d'abord, les patients voient la qualité de leurs soins de santé améliorée, notamment pour ceux nécessitant un suivi pour une maladie chronique telle que le diabète. Ces thérapies innovantes offrent la possibilité d'une approche plus adaptée aux besoins du patient. Ils deviennent de réels acteurs de leur santé en renseignant eux-mêmes la progression de leur maladie. Pour les professionnels de santé, ces thérapies facilitent le suivi du traitement et améliorent sa qualité avec une meilleure accessibilité des informations médicales des patients. Enfin, concernant les systèmes de santé, les DTx pourraient être utilisées pour cibler des besoins non satisfaits ou des domaines mal pourvus par les systèmes de santé. La gestion des pathologies à distance permet de réduire la pression sur les systèmes de santé.

En dépit de cela, des défis rendent la démocratisation des thérapies numériques compliquée. Au travers de ce rapport, l'EFPIA met en avant des recommandations afin d'y remédier.

I. LES DTX EN EUROPE, UNE MISE EN PLACE LENTE ET RETARDÉE PAR DE NOMBREUX OBSTACLES

La crise de la covid-19 a conforté l'intérêt pour les thérapies numériques. En 2019, le nombre d'utilisateurs s'élevait à 11 millions, en 2021 à 44 millions et une estimation de 1,4 milliards pour 2025.[267] En 2019, le marché était estimé à une valeur de 2 milliards de dollars. Pour l'année 2024, l'estimation est à 32 milliards de dollars, soit 28 milliards d'euros[268]. En outre, il existe trois types de DTX. Tout d'abord, la thérapie numérique autonome est utilisée indépendamment de tout autre produit médical, par exemple un produit

[265] European Federation of Pharmaceutical Industries and Associations – EFPIA, *Improving access to digital therapeutics in Europe*, juin 2023, p. 4.

[266] Règlement n° 2017/745/UE du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive n° 2001/83/CE, le règlement n° 178/2002/CE et le règlement n° 1223/2009/CE et abrogeant les directives du Conseil n°s 90/385/CEE et 93/42/CEE, *JOUE* n° L 117 du 5 mai 2017, p. 1-175.

[267] MSD, *Thérapies numériques : aperçu des soins du futur* [en ligne] (consulté le 23/04/24).

[268] *Ibid*.

pharmaceutique. Ensuite, il existe également la thérapie numérique de « compagnie utilisée pour les maladies ». Elle est utilisée avec des médicaments, un dispositif médical ou d'autres thérapies pour améliorer le soin prodigué du patient et ses résultats médicaux. Enfin, il est possible de citer la thérapie numérique de combinaison utilisant un logiciel et d'autres composants comme un logiciel pour médicament ou un logiciel de dispositif médical. Ces logiciels doivent être nécessairement utilisés ensemble.

Néanmoins, le domaine de la santé est peu numérisé à l'heure actuelle, malgré l'intérêt grandissant des systèmes de santé et leurs efforts pour incorporer la santé numérique, notamment pendant la pandémie. Le rapport présente les situations de différents États.

L'Allemagne apparaissait comme le pays le plus avancé en 2019. La loi sur les soins de santé numériques de 2019 (Digitale Versorgung Gesetz, DVG) a mis en place un processus rapide pour les applications admissibles afin de les inclure dans un répertoire central d'applications de santé numérique. Pour ces applications, il est possible d'avoir un remboursement uniquement si la thérapie innovante fait partie de la catégorie des thérapies autonomes présentant des risques faibles ou moyens. En janvier 2023, 161 applications avaient été envoyées dans le but d'être évaluées, 125 étaient dans une liste provisoire et 36 dans une liste finale. En définitive, 40 décisions ont été prononcées pour que des applications passent dans la liste provisoire ou finale[269].

En Belgique, une voie d'accès distincte a été mise en place pour les thérapies numériques. Une plateforme a été créée et collecte toutes les applications qui ont reçu le marquage CE en tant que dispositif médical et les évalue à l'aide d'une pyramide de validation à trois niveaux. Seules les applications qui possèdent des preuves de bénéfices économiques et sociaux peuvent atteindre le niveau 3 et être remboursées. Cette pyramide a été créée en 2018 et le rapport précise qu'une seule application a pu atteindre le niveau 3[270]. De plus, le remboursement offert par le niveau 3 n'est que temporaire.

Le Royaume-Uni, quant à lui, a progressé dans l'établissement d'un cadre d'évaluation pour les DTx. Néanmoins, les voies d'accès restent moins accessibles qu'en Belgique ou en Allemagne. Le National Institute for Health and Care Excellence est l'organisme responsable de classifier les DTx selon leurs fonctions et les risques potentiels pour l'utilisateur[271]. Il n'y a pas d'obligation de financement de ces DTx malgré le fait qu'elles soient recommandées par l'organisme. En comparaison, le rapport précise qu'une telle obligation existe dans le domaine pharmaceutique.

Le rapport explique que les autres États européens ne possèdent pas de voie spécifique nationale pour l'accès aux DTx. Cela signifie qu'au sein d'un même État, il n'y a pas nécessairement une réglementation uniforme nationale pour la promotion et l'utilisation des DTx. Dans certains États, des cadres existent tout de même, notamment au travers des DM. En France, la réglementation pour les DM est utile pour l'évaluation et la fixation d'un prix pour les DTx, en s'appuyant également sur des lignes directrices spécifiques et des critères publiés[272]. En 2022, un accès rapide a été introduit pour un remboursement temporaire des activités de télésurveillance et des appareils médicaux numériques avec

[269] Federal Institute for Drugs and Medical Devices, *DiGA Digital Health Applications* [en ligne] (consulté le 08/05/24).
[270] MHealth Belgium, *All applications* [en ligne] (consulté le 08/05/24).
[271] NICE, *Evidence standards framework for digital health technologies* [en ligne] (consulté le 08/05/24).
[272] MedTech Europe, *Recognising the value of digital health apps: An assessment of five European healthcare systems* [en ligne], 15 novembre 2021, 20 p (consulté le 08/05/24).

un but thérapeutique, ce qui inclut les DTx[273].

L'EFPIA explique que l'utilisation des DTx reste faible et concerne peu de pays. Elle retient quatre défis qui freinent la mise en place des DTx.

En premier lieu, même si les DTx sont couvertes par le règlement sur les DM, il y a un manque d'harmonisation dans les exigences réglementaires à cause des différences d'interprétation. En effet, le marquage CE permet une certaine harmonisation, mais les critères du dossier ne sont pas interprétés de la même façon entre les États membres de par la nature innovante des DTx[274]. Selon la définition citée auparavant, les DTx seront considérées comme des DM au sens du règlement 2017/745. Selon le groupe de coordination des DM, logiciels qui répondent à la définition de DM (MDSW) peuvent être catégorisés en quatre classes : classe I pour des risques faibles, classe IIA pour des risques moyens, classe IIB pour des risques moyens ou hauts et classe III pour des risques élevés.[275] Les DTx doivent passer un test de conformité afin d'être évaluées et remboursées. Au terme de cette évaluation, la thérapie pourra obtenir le marquage CE. Le rapport souligne le caractère inadapté du cadre réglementaire pour les DM dû à l'évolution rapide des logiciels. Il est préconisé d'avoir une approche flexible basée sur le risque permettant l'innovation tout en minimisant les risques pour les patients et en maintenant une sécurité haute, efficace et des standards de qualité. Les DTx relevant du cadre des DM, elles doivent respecter les dispositions du règlement général sur la protection des données (RGPD). Les États peuvent adopter des règles nationales dans ce domaine et celui de la vie privée. Le rapport souligne, encore une fois, le manque d'harmonisation compliquant la mise en place des DTx.

Le rapport mentionne les difficultés relevant des critères de preuve et de l'absence de mécanismes d'estimation de la valeur.[276] En l'absence d'un cadre unique, il existe une incertitude sur les preuves nécessaires à présenter afin d'avoir une évaluation positive. Les exigences de preuves sont susceptibles de varier entre chaque État. Les données probantes issues d'essais contrôlés randomisés sont les preuves principales.[277] L'EFPIA explique que cela n'est pas l'approche optimale et, par ailleurs, cette approche renforce le manque d'harmonisation des preuves et les difficultés pour les entreprises de développer des plans cliniques. Le rapport explique qu'il est pertinent d'avoir différents éléments pour prouver la valeur ajoutée. Pour l'EFPIA, les données de vie réelle joueront un rôle majeur dans le futur.[278] Il est précisé que les essais randomisés ne permettent pas d'évaluer de manière continue l'effectivité des DTx dans le monde réel. Il est nécessaire d'avoir une approche globale basée sur le patient. En outre, l'évaluation est importante puisqu'elle permet d'avoir le remboursement des DTx. En effet, lorsqu'une thérapie a été évaluée comme fiable avec des bénéfices avérés, cela encouragerait les États à les instaurer et les prendre en charge. Cette évaluation possède

[273] *All applications* [en ligne], *op. cit*.
[274] EFPIA, *Improving access to digital therapeutics in Europe, op. cit*., p.9.
[275] Article 51 du règlement n°2017/745/UE, *op. cit*.
[276] EFPIA, *Improving access to digital therapeutics in Europe, op. cit.*, p.10.
[277] Les essais contrôlés randomisés (ECR) peuvent être définis comme visant à mesurer l'impact d'une intervention donnée en comparant les résultats d'un groupe expérimental (recevant l'intervention) et d'un groupe de contrôle (ne la recevant pas), auxquels les individus sont assignés de manière aléatoire.
[278] Les données de vie réelle ont été définies par Dominique POLTON comme des données qui ne sont pas collectées dans un cadre expérimental, mais qui sont générées dans la pratique courante, notamment à l'occasion des soins réalisés en routine, v. Dominique POLTON, « Données de vie réelle : un enjeu majeur, une dynamique qui s'accélère », *in* Colloque HAS, « Construction et Dialogue des savoirs vers de meilleures décisions individuelles et collectives en santé, 21 novembre 2019, Paris.

différents critères selon les pays. Le rapport souligne la problématique des capacités des États à pouvoir évaluer correctement les DTx.

L'importance du remboursement a également été citée, notamment à cause de l'absence d'une approche standardisée ou spécifique pour l'obtenir[279]. Dans la majorité des États, les DTx ne sont pas remboursées ou les délais de remboursement sont longs ou les fournisseurs individuels s'en chargent. Tout cela introduit une incertitude sur les critères de remboursement. Le rapport soutient le remboursement lorsque les bénéfices pour la santé ont été prouvés. Le temps de décision sur la possibilité de l'obtenir étant long dans la majorité des États, il semble donc très peu probable que le remboursement soit obtenu selon le rapport. Dans les États dans lesquels il est possible d'en bénéficier, comme aux Pays-Bas, des incertitudes sur les critères de la procédure subsistent à cause de la procédure décentralisée. Néanmoins, des améliorations sont à noter puisque certains États, comme la Belgique ou l'Allemagne, ont mis en place des mécanismes de remboursement et de fixation des prix.

Enfin, le rapport indique que malgré la garantie d'un remboursement, le manque de financement est un frein à l'utilisation des DTx.[280] Il a été relevé qu'un financement n'était disponible que dans certains États. Il permet de promouvoir l'accessibilité de ces thérapies aux patients. Les conditions de financement et d'utilisation des DTx dépendent des critères fixés au niveau national, de la structure du système de santé de l'État et du budget national alloué au système de santé. Toutes ces différences amènent l'EFPIA à suggérer l'existence d'un cadre commun afin d'assurer un financement correct des DTx. Toutefois, l'éducation des patients et des professionnels de santé seront essentielles afin qu'ils comprennent ces nouvelles thérapies et qu'ils aient confiance dans leur valeur et leur qualité. Pour ce faire, il est suggéré que les responsables politiques, les organisations professionnelles ainsi que les développeurs de DTx collaborent pour éduquer les professionnels de santé. Par ailleurs, de nombreux pays devront améliorer la numérisation de leur système de santé puisque certains n'ont pas la structure nécessaire pour, par exemple, mettre en place un dossier médical en ligne. La mise en place de dossiers médicaux en ligne fait partie de la construction de l'espace européen de données de santé (EHDS)[281]. Cet espace est basé sur le partage des données européennes de santé. Les innovations numériques dans le domaine de santé, tel que le dossier médical numérique, facilitent la promotion d'un véritable marché unique des systèmes de dossiers médicaux électroniques. Comme les DTx, l'EHDS vise à donner aux citoyens la possibilité de prendre le contrôle de leurs données de santé. Les difficultés de numérisation auxquelles les États font face constituent un frein à la mise en place des DTx et, plus largement, de l'EHDS.

EFPIA est satisfaite des initiatives qui ont été prises pour mettre en avant les DTx. Le rapport avance neuf recommandations destinées aux États afin de favoriser le développement des DTx.

II. LES DTX EN EUROPE, UNE NECESSITÉ D'HARMONISATION ET DE DÉFINITION DES NORMES DES ÉTATS

Le rapport recommande d'avoir des critères réglementaires harmonisés associés à des indications claires pour assurer un accès simplifié aux DTx.[282] L'EFPIA souhaite des standards élevés de sécurité, d'efficacité et de qualité pour les DTx tout en garantissant un accès pour les patients

[279] EFPIA, *Improving access to digital therapeutics in Europe, op. cit.*, p.12.
[280] *Ibid.*, p.13.
[281] Commission Européenne, « Espace européen des données de santé » (consulté le 18/06/2024).
[282] EFPIA, *Improving access to digital therapeutics in Europe, op. cit.*, p.14.

dans un temps raisonnable. L'approche sera basée sur le risque mais restera flexible et garantira l'innovation. Elle sera composée de critères harmonisés qui assureront un développement et une commercialisation plus simples et, par conséquent, un accès plus rapide aux DTx. Il devra être soumis au règlement 2017/745, au RGPD et aux règles nationales supplémentaires. De plus, le rapport préconise une clarification des preuves cliniques nécessaires lors de la demande du marquage CE. Les États et leurs responsables politiques devraient développer leur capacité d'assurer les autorisations de mise sur le marché en temps opportun, permettant un accès dans un temps raisonnable pour les patients, en maintenant des standards élevés.

Ensuite, il est suggéré d'avoir des critères d'estimation de la valeur qui soient sur-mesure et adaptés à l'objectif de la thérapie numérique. Ces critères doivent être également plus prévisibles et cohérents et comporter un portefeuille de preuves pouvant comprendre des données de vie réelle. Le large portefeuille de preuves garantira la prédictibilité, la clarté et la cohérence des besoins de preuve pour les États. Il inclura des données cliniques, des données des consommateurs, des données de vie réelle. Les données de vie réelle devraient avoir un rôle important dans l'estimation de la valeur, car elles auront été générées par les DTx grâce à l'action des patients. Les critères seront définis de manière claire et transparente. L'approche devra être globale plutôt que basée sur des indications spécifiques. Une approche globale est nécessaire, selon le rapport, pour traiter les patients avec un mélange unique de paramètres qui leur sera propre.

Par ailleurs, les États et la Commission européenne devraient envisager de soutenir les collaborations entre États pour harmoniser les critères au sujet des preuves cliniques.[283] La Commission devrait faciliter la reconnaissance mutuelle des preuves et la collaboration entre États pour avoir une approche constante et rapide de l'estimation des DTx. Les États devraient établir un ensemble minimal d'exigences en commun pour faciliter la reconnaissance commune. Le rôle de la Commission consisterait aussi à faciliter le partage de connaissances entre États, soutenir l'échange de bonnes pratiques et de preuves cliniques reconnues au niveau national ou infranational par certains organismes d'évaluation des technologies de santé et des acheteurs dans les États. L'EFPIA salue la mise en place du groupe de travail européen pour l'évaluation harmonisée des dispositifs médicaux numériques.

Dans sa quatrième recommandation, l'EFPIA souligne que la collaboration entre les États et la Commission sera nécessaire pour soutenir le partage des données et construire une infrastructure pour exploiter le potentiel des DTx. L'espace européen des données de santé facilitera les échanges de données de santé dans la vie des patients et améliorera la collaboration entre États. L'interopérabilité des systèmes de santé sera mise en avant par cet espace européen. Le suivi médical des patients deviendra continu avec leurs données de santé accessibles quel que soit le système de santé.

De surcroît, il est préconisé aux États de créer des mécanismes clairs et transparents au niveau national pour la tarification et le remboursement. Des voies de remboursement devraient être mises en place au niveau national pour les DTx autonomes ou DTx compagnons. Pour les thérapies numériques combinées, il est nécessaire qu'elles soient remboursées avec le produit pharmaceutique associé. Le système de remboursement doit prendre en compte l'existence des différents types de DTx.

Deux recommandations sont explicitement adressées aux payeurs.[284] D'une part, ils devraient offrir une approche souple pour autoriser un accès provisoire à la DTx pendant la génération de données

[283] *Ibid*., p.15.

[284] *Ibid*., p.16.

supplémentaires. Les preuves de vie réelle générées pourraient être utilisées pour soutenir l'évaluation clinique ainsi qu'économique et médicale de la thérapie numérique. Cela accélérerait l'accès pour le patient aux technologies innovantes tout en permettant aux acheteurs d'incorporer les données de vie réelle dans leur décision finale de remboursement. L'accès provisoire dans un futur proche serait bénéfique pour les domaines dans lesquels les ressources nécessaires manquent ou lorsque les besoins ne sont pas remplis.

D'autre part, les payeurs devraient envisager d'introduire de nouveaux modèles de paiement pour gérer les incertitudes de preuve. Les DTx, par leur nature innovante, font qu'il n'y a pas de comparateur, rendant l'estimation de leur valeur compliquée. Cette évaluation devrait être adaptative et efficace pour incorporer les données de vie réelle collectées avant et après l'estimation de valeur. Les nouveaux modèles de paiement, comme les accords axés sur les résultats qui tirent parti des résultats déclarés par les patients, pourraient être attrayants lorsque les payeurs ne sont pas convaincus que les données cliniques représentent des soins concrets pour les patients.

Concernant la nécessité de financement adéquat, il est impératif que les besoins en financement soient explicités et budgétisés. Cependant, les patients ne devraient pas supporter un fardeau financier. Il ne faut pas, qu'avec les professionnels de santé, ils soient freinés dans leur utilisation par la peur de répercussions financières. Le rôle des États est d'assurer un financement suffisant en utilisant des modèles de financement qui soutiennent les approches fondées sur la valeur. Le rapport recommande que les États se dotent d'un budget dédié à la santé numérique.

Enfin, l'utilisation croissante des DTx nécessitera des efforts groupés des décideurs politiques, des professionnels de santé et des entreprises pour développer la confiance dans ces thérapies. Les parties prenantes doivent travailler ensemble pour améliorer l'éducation, les expériences et la sensibilisation des professionnels de santé et des patients. Les politiques nationales doivent promouvoir les connaissances dans la santé numérique et les DTx. Les actions nécessaires comprennent, entre autres, des investissements dans les infrastructures numériques et le soutien aux formations numériques. Une confiance généralisée dans les thérapies numériques est cruciale.

La reconnaissance pour les patients d'un accès gratuit à la première copie de leur dossier médical

CJUE, 26 octobre 2023, *FT c. DW*, aff. C-307/22, ECLI:EU:C:2023:811

par Sarah BISTER

Avocat au Barreau de Paris,
Docteure en droit public

Dans un arrêt rendu le 26 octobre 2023[285], la Cour de justice de l'Union européenne (« CJUE ») revient sur les conditions entourant le droit d'accéder, gratuitement, pour les patients à leur dossier médical.

C'est en Allemagne que l'affaire débute. Un patient, mécontent des soins dentaires qu'il recevait et soupçonnant une mauvaise prise en charge par son dentiste, a demandé à celui-ci la remise, à titre gratuit, d'une copie intégrale de son dossier médical. Le professionnel de santé a estimé qu'il ne ferait droit à cette demande que contre remboursement de ses frais par le demandeur.

Le patient a alors introduit un recours contre le professionnel de santé devant le tribunal de district allemand qui a fait droit à sa demande. Le dentiste a interjeté appel devant le tribunal régional : il a vu sa demande déboutée sur la base de l'article 15 du Règlement général sur la protection des données (« RGPD »)[286]. Le tribunal régional estimait que la demande d'exercice du droit d'accès à ses données, prévue par cet article du RGPD, n'est pas nécessairement liée à la protection des données.

Le dentiste s'est pourvu devant le Bundesgerichtshof, Cour fédérale allemande de justice, pour demander l'annulation de l'arrêt du tribunal régional et le rejet du recours du patient. Le Bundesgerichtshof confirme qu'en vertu du droit allemand, le professionnel de santé n'est pas tenu de communiquer gratuitement au patient des copies de son dossier médical. Pour autant, la Cour fédérale considère qu'une lecture du RGPD pourrait conduire à une interprétation différente. C'est dans ce contexte que le Bundesgerichtshof a sursis à statuer et posé à la CJUE trois questions préjudicielles

- Une portant sur l'accès aux données dans un but autre que la protection des données à caractère personnel (**I**) ;
- Une deuxième sur l'accès gratuit aux copies de documents (**II**) ;
- Une dernière sur la notion même de copie des données (**III**).

I. LE CONDITIONNEMENT DE L'ACCÈS AUX DONNÉES À LA PROTECTION DES DONNÉES : LE REFUS D'UNE INTERPRÉTATION RESTRICTIVE

L'article 12 du RGPD, sur la *« transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée »*, précise en substance, au paragraphe 5, qu'aucun paiement n'est exigé pour fournir les informations que tout responsable de traitement doit communiquer aux personnes lorsqu'il collecte directement ou indirectement leurs données et pour procéder à la communication de ces

[285] Arrêt de la Cour, 26 octobre 2023, *FT*, aff. C-307/22, ECLI:EU:C:2023:811.

[286] 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, JOUE L. 119 du 4 mai 2016.

données. Deux atténuations sont toutefois prévues. D'une part, le paiement de frais raisonnables peut être exigé ou le refus de donner suite à la demande, invoqué, lorsque les demandes de la personne concernée sont manifestement infondées ou excessives[287]. D'autre part, en cas de doutes raisonnables quant à l'identité de la personne à l'origine de la demande, le responsable de traitement peut demander des informations complémentaires[288].

L'article 15 du RGPD concerne plus précisément le droit d'accès de la personne concernée. Il dispose que cette dernière peut obtenir confirmation par le responsable de traitement du traitement ou non de ses données personnelles et, le cas échéant, des informations détaillées à ce sujet[289], ainsi que la communication d'une copie des données objet du traitement[290].

L'article 15 n'apporte aucune exception ou condition à l'exercice du droit d'accès. Si tel avait été le cas, le législateur l'aurait clairement précisé comme nous pouvons le constater pour d'autres droits. A titre d'illustration, le droit à l'effacement[291], le droit à la portabilité[292] ou encore le droit d'opposition[293] sont conditionnés à la base légale sur laquelle repose le traitement : il n'est ainsi pas possible pour une personne concernée de faire jouer son droit d'opposition lorsque le traitement des données est fondé sur le respect d'une obligation légale.

La Cour fédérale allemande de justice s'interrogeait notamment sur la lecture combinée des articles 12 et 15 du RGPD avec le considérant 63 du règlement aux termes duquel *« une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité […] »*. Faut-il en déduire que la demande d'accès a donc nécessairement un lien avec la manière dont le responsable de traitement respecte la réglementation sur la protection des données ? Nous rejoignons l'Avocat général, suivi par la CJUE, qui ne le pense pas[294]. En effet, dans la mesure où les articles mêmes du règlement n'encadrent pas la finalité du droit d'accès, il serait étonnant qu'une position différente soit retenue sur la base d'un considérant. La disposition de ce considérant n'entraine pas une approche limitative du droit d'accès mais souligne l'importance de ce droit.

Par conséquent, le droit d'accès aux données dont dispose le responsable de traitement à l'égard d'une personne concernée ne serait pas uniquement limité au cadre de la protection des données. C'est d'ailleurs la position retenue par le Comité européen de la protection des données (« CEPD ») dans les lignes directrices sur les droits des personnes concernées[295]. Le CEPD rappelle qu'il n'appartient pas au responsable de traitement d'apprécier les raisons pour lesquelles une demande d'accès est exercée mais seulement les informations demandées. Le CEPD illustre ces propos en prenant l'exemple qu'un responsable de traitement ne devrait pas refuser le droit d'accès *« au motif qu'il soupçonne que les données demandées pourraient être utilisées par la personne concernée pour se défendre en justice en cas de licenciement ou de conflit commercial avec le responsable de traitement »*.

---

[287] Article 12, paragraphe 5, RGPD.
[288] Article 12, paragraphe 6, RGPD.
[289] Article 15, paragraphe 1, RGPD.
[290] Article 15, paragraphe 3, RGPD.
[291] Article 17 RGPD. Le droit à l'effacement ou droit à l'oubli des données ne s'applique pas dans différentes hypothèses prévues aux paragraphes 2 et 3 de l'article.
[292] Article 20 RGPD. Le paragraphe 3 précise explicitement que le l'exercice de ce doit « ne s'applique pas au traitement 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.
[293] Article 21 RGPD.
[294] Conclusions de l'Avocat général Monsieur Nicholas Emiliou, présentée le 20 avril 2023, *FT c. DW*, aff. C-307/22, ECLI:EU:C:2023:315.
[295] CEPD, *Lignes directrices 01/2022 sur les droits des personnes concernées*, 28 janvier 2022.

Cet exemple est tout à fait transposable au cas d'espèce. Le patient souhaitait avoir accès à ses données pour, potentiellement, intenter une action en responsabilité médicale contre le praticien. Celui-ci ne pouvait donc pas refuser de faire droit à la demande au prétexte qu'il pourrait être judiciairement inquiété par les futures actions du patient.

Au vu de l'ensemble de ces éléments, la Cour de justice conclut, à la première question, qu'un responsable de traitement est obligé de fournir à la personne concernée, à titre gratuit, une première copie de ses données à caractère personnel, objet du traitement, quand bien même la demande serait motivée dans un but autre que la prise de connaissance du traitement et la vérification de sa licéité.

II. L'ACCÈS GRATUIT A LA PREMIÈRE COPIE DES DONNÉES CONFIRMÉ PAR LA COUR

La deuxième question posée à la Cour portait sur le fait de savoir si l'article 23 du RGPD, prévoyant des limitations pour l'exercice des droits des personnes, permet qu'une législation nationale, adoptée avant l'entrée en vigueur du RGPD, restreigne le droit des personnes concernées à obtenir, à titre gratuit, une copie de leurs données, en leur imposant le remboursement des frais exposés par le responsable de traitement dans ce cadre.

Le juge de l'Union indique que l'article 23, paragraphe 1, du RGDP se borne à préciser que la limitation de la portée des obligations et des droits prévues par le règlement par une législation nationale est possible dès lors qu'une telle limitation *« respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée pour garantir […] la protection de le personne concernée ou des droits et libertés d'autrui »*. Il en déduit que le fait que la législation nationale en cause soit antérieure à l'adoption du RGPD n'a aucune incidence pour autant qu'elle respecte les exigences de nécessité et de proportionnalité.

En l'espèce, la législation allemande met à la charge des patients les coûts liés à la fourniture d'une copie de leur dossier médical sollicitée par eux, que ce soit la première copie ou non, dans le but de protéger l'intérêt économique des praticiens. L'objectif visé est de dissuader les demandes de copies futiles et permettre aux praticiens de ne pas perdre inutilement du temps et des moyens à faire droit à de telles demandes. Le temps médical étant précieux, il serait ainsi davantage préservé grâce à l'instauration d'une mesure telle que celle en cause, et éviterait que les praticiens gaspillent leur énergie à des tâches administratives évitables.

La CJUE considère que l'intérêt économique des praticiens est déjà prévu par le RGPD puisque l'article 15 du règlement leur permet de faire face aux abus dans les demandes d'exercice d'accès, en requérant le paiement de frais raisonnables en cas de demande manifestement infondée ou excessive. En outre, l'article 12 précise explicitement qu' *« aucun paiement n'est exigé pour fournir les informations […] et pour procéder à toute communication »* et l'article 15 que *« le responsable de traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée »*. Cette dernière disposition suppose donc que la première copie est gratuite et seules les copies supplémentaires sont facturables.

A la question de savoir si une législation nationale telle que celle en cause permet de protéger *« les droit et libertés d'autrui »*, la Cour se prononce négativement. Sans revenir sur la notion d' « autrui », elle conclut que les éléments communiqués par la juridiction de renvoi semblent attester que la législation nationale vise uniquement la protection d'intérêts *« d'ordre purement administratif et économique »* (considérant n°66). La protection des droits et libertés d'autrui ne relève donc pas de l'objectif visé

par la mesure allemande. De plus, en admettre sa conformité reviendrait à méconnaître le principe de gratuité de la première copie et remettre en cause l'effet utile du droit d'accès.

La position de l'Avocat général, dans ses conclusions, est intéressante en ce qu'elle diverge de celle retenue par la Cour. Ses explications détaillées conduisent à une solution différente. Selon lui, la notion de *« droits et libertés d'autrui »* pourrait inclure les droits et libertés du responsable de traitement. La notion de *« autrui »* choisie par le législateur ne serait pas anodine et emporterait acception différente de celle de *« tiers »*. Le tiers est une personne autre que la personne concernée et le responsable de traitement. Pour l'Avocat général, les droits économiques du responsable de traitement que la législation allemande cherche à protéger recouvrent la liberté d'entreprise, la liberté professionnelle et le droit de travailler ainsi que le droit de propriété, tous ces droits étant reconnus par la Charte des droits fondamentaux de l'Union européenne. Il en déduit que la position du législateur allemand découle d'une mise en balance entre les différents intérêts en jeu. Le résultat aboutissant au paiement de la première copie du dossier médical demandé par le patient ne serait pas contraire au droit de l'Union. Il suggère toutefois à la juridiction de renvoi de s'assurer que la restriction au droit d'accès soit réellement pertinente, nécessaire et proportionnée aux objectifs de protection de la santé publique et de la libre prestation des activités des professionnels de santé.

Pour sa part, après avoir effectué la mise en balance de la protection des intérêts économiques des praticiens et le droit d'accès gratuit du patient à son dossier médical, pour une première copie, la Cour en conclut que les droits du responsable de traitement ne sauraient prévaloir sur ceux de la personne concernée.

Ce faisant, la législation allemande devrait être revue afin de permettre aux patients de pouvoir obtenir gratuitement la copie de leur dossier médical dans le cadre d'une première demande et ce, quoi qu'il en coûte au praticien.

III. LES PRÉCISIONS SUR LA NOTION DE COPIE DES DONNÉES

La dernière question soulevée par la Cour fédérale allemande portait sur l'expression même de *« copie des données à caractère personnel faisant l'objet d'un traitement »*. La juridiction de renvoi s'interrogeait sur la manière d'interpréter cette disposition de l'article 15 du RGPD au regard des informations susceptibles d'être contenu dans le dossier médical. Plus précisément, le patient doit-il se voir remettre une copie intégrale des documents contenant ses données personnelles figurant dans son dossier médical ou uniquement une copie de ses données personnelles ?

Cette problématique a déjà été abordée par la CJUE dans un arrêt du 4 mai 2023[296], ce que la Cour rappelle. Dans cette affaire, la CJUE était interrogée sur la portée du droit d'accès accordé aux personnes concernées en vertu de l'article 15 du RGPD. Dans ce cadre, la notion de « copie » avait été étudiée. Dans la présente affaire, la Cour rappelle que *« le terme « copie » se rapporte non pas à un document en tant que tel, mais aux données à caractère personnel qu'il contient et qui doivent être complètes. La copie doit donc contenir toutes les données à caractère personnel faisant l'objet d'un traitement »* (considérant n°72). Aussi, la copie des données doit permettre au demandeur d'exercer effectivement son droit ce qui suppose que les données soient reproduites intégralement et fidèlement. Par conséquent, la reproduction d'extraits de documents, voire de documents dans leur entièreté, contenant, entre autres, des

[296] Arrêt de la Cour, 4 mai 2023, Österreichische Datenschutzbehörde, aff. C-487/21, ECLI:EU:C:2023:369.

données personnelles peut s'avérer indispensable si la remise de ces données dans leur contexte est indispensable pour en assurer l'intelligibilité.

Cette jurisprudence est confortée par le principe de transparence posé à l'article 5 du RGPD. De plus, sur le point de savoir si, en l'espèce, la communication d'une copie du dossier médical n'irait pas à l'encontre de l'article 12, paragraphe 1, du RGPD aux termes duquel les données fournies à la personne concernée doivent l'être *« d'une façon concise, transparente, compréhensible et aisément accessible »*, Avocat général et Cour de justice s'accordent. Permettre aux professionnels de santé de résumer ou compiler les données, afin de les communiquer sous une forme synthétique pourrait contrevenir à l'objectif fixé par la réglementation en ce sens que cela risquerait d'aboutir à l'omission de certaines données pertinentes ou reprises de manière incorrecte ou, de manière plus générale, rendre plus compliqué pour les patients d'en vérifier l'exactitude et l'exhaustivité. Certes, le patient – profane en la matière – pourrait se retrouver avec un flot d'informations qu'il ne serait pas en mesure de comprendre, mais finalement ne pas lui donner accès à ces informations sous ce prétexte reviendrait à l'empêcher d'avoir accès à des informations qui pourraient se révéler importante. Il n'appartient donc pas au professionnel de santé – responsable de traitement – de porter un jugement sur l'appréhension technique possible ou non des informations qu'il va communiquer.

En outre, le considérant 63 du RGPD est particulièrement éclairant sur le type de données pouvant être communiqué aux personnes concernées s'agissant de leur santé. Il y est précisé que le droit d'accès inclut l'accès, par exemple, aux données de leur dossier médicaux *« contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention administrés »*.

La réponse à la question soumise est donc claire : le patient a le droit d'obtenir une copie des données personnelles faisant l'objet du traitement ce qui implique la remise d'une reproduction fidèle et intelligible de l'ensemble de ces données.

Invoqué de plus en plus régulièrement, le droit d'accès des personnes concernées est ici grandement renforcé et confirme qu'il n'est pas circonscrit au domaine de la protection des données personnelles. La finalité même de la demande est étrangère à son exercice.

On ne saurait conclure sans faire un parallèle entre la législation allemande et le droit français. En effet, l'article L. 1111-7 du Code de la santé publique prévoit que toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels de santé ou tout autre établissement de soins et que la *« consultation sur place des informations est gratuite »*. Cette dernière disposition pourrait supposer que dans des situations autres que la consultation sur place, un paiement pourrait être exigé. C'était d'ailleurs ce que précisait, jusqu'à récemment, l'article R. 1111-2 du Code de la santé publique : *« Les frais de délivrance* [des copies de documents] *sont laissés à la charge du demandeur dans les conditions fixées par l'article L. 1111-7 »*. Mais la présente décision de la CJUE n'est pas restée sans échos et, très vite, le gouvernement s'est retrouvé face à sa non-conformité au droit de l'Union. Modifier l'article L. 1111-7 du Code de la santé publique n'est pas évident en pratique car cela suppose un véhicule législatif. En revanche, modifier la partie réglementaire du Code de la santé publique est plus facile. On ne peut ici que souligner l'habilité du gouvernement qui a profité de l'adoption d'un décret relatif à l'examen des caractéristiques génétiques d'une

personne[297] pour supprimer la disposition litigieuse de l'article R. 1111-2 du Code de la santé publique concernant les frais de délivrance des copies. Le lien avec les dispositions relatives à l'examen des caractéristiques génétiques est éloigné. Subrepticement glissée dans le décret entre différentes modifications relatives aux dispositions générales relatives à l'examen des caractéristiques génétiques d'une personne, la modification de l'article R. 1111-2 du Code passe presque inaperçue. Si nous doutons de la place de cette modification dans ce décret précis, nous ne pouvons qu'en louer le résultat. Désormais, les patients pourront obtenir une première copie gratuite de leur dossier médical

[297] Décret n° 2023-1426 du 30 décembre 2023 relatif à l'examen des caractéristiques génétiques d'une personne, *JORF* du 31 décembre 2023.

Vente en ligne de médicaments via la plateforme Doctipharma : la Cour de justice précise les interdictions que peut prononcer un État membre

CJUE, 29 février 2024, *Doctipharma*, aff. C-606/21, ECLI:EU:C:2023:585

par Claire BORIES

Docteure en droit public,
Université Toulouse Capitole

Dans le sillage de l'arrêt de la Cour de cassation du 19 juin 2019[298], qui déclarait l'activité du site Doctipharma (www.doctipharma.fr) illicite car participant en tant qu'intermédiaire entre les officines de pharmacie référencées sur son site et le public « au commerce électronique de vente de médicaments [sans ordonnance] bien que n'étant pas pharmacien » et violant ainsi les règles les plus élémentaires du monopole pharmaceutique (articles L. 5125-25 et L. 5125-26 du code de la santé publique), la Cour de justice de l'Union étudie les possibilités de limitation de ce type de vente par le droit national conformément à l'article 85 quater de la directive n° 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain[299]. Ainsi qu'il découle de cette disposition, les États membres peuvent établir des conditions spécifiques pour la vente à distance de médicaments au public pour autant qu'elles soient justifiées par la protection de la santé publique.

Alors, de deux choses l'une :

- soit il peut être conclu, au regard des particularités du service d'intermédiation fourni par la société Doctipharma, qui est, en toute hypothèse, comme l'indique la Cour en réponse à la première question préjudicielle, un « service de la société de l'information » au sens de l'article 1er, point 2, de la directive n° 98/34/CEE[300] et de l'article 1er, paragraphe 1, sous b), de la directive n° 2015/1535/UE[301] (point 32), que celle-ci doit être considérée comme étant elle-même prestataire de la vente, et, dans ce cas, l'article 85 quater de la directive n° 2001/83/CE ne s'oppose pas à l'interdiction de ce service par l'État membre sur le territoire duquel elle est établie (point 50) ;

- soit ce service consiste uniquement à mettre en relation des vendeurs avec des clients, de sorte que Doctipharma fournit un service propre et distinct de la vente. Dans cette deuxième hypothèse, ajoute la Cour, « ce service ne pourrait être interdit sur le fondement de l'article 85 quater, paragraphe 1, sous a), de la directive 2001/83 au [seul] motif qu[e la société en cause] participait au commerce électronique de vente de médicaments sans avoir la qualité de pharmacien » (point 52).

[298] N° 18-12292. V. à ce sujet, DANIS-FATOME Anne, « La plateforme Doctipharma a une activité illicite en participant, en tant qu'intermédiaire, au commerce électronique de médicaments en ligne. Note sous Cass. Com. 19 juin 2019, n° 18-12292 », *Revue des contrats*, n°4, Décembre 2019, p. 28-31.

[299] *JOUE* n° L 311/67 du 29 novembre 2001.

[300] Directive n° 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, *JOCE* n° L 204 du 21 juillet 1998.

[301] Directive n° 2015/1535/UE du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *JOUE* n° 241 du 17 septembre 2015.

LISTE DES CONTRIBUTEURS

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

Sarah BISTER
Avocate au Barreau de Paris et
Docteure en droit public

Claire BORIES
Docteure en droit public,
Université Toulouse Capitole

Dorianne CATTOEN
Étudiante en Master de droit européen
Université Toulouse Capitole

Noémie DUBRUEL
Doctorante en droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier,
UMR 1295 Inserm équipe BIOETHICS

Nino ESCUDIER
Étudiant en Master de droit européen
Université Toulouse Capitole

Lisa FERIOL
Doctorante CIFRE, Ekitia et Equipe BIOETHICS, CERPOP UMR1295 Inserm et Université Toulouse Paul Sabatier

Valentine DURAND
Doctorante en Droit public, IRDEIC Université Toulouse Capitole

Shana LEVI
Étudiante en Master 2 DIDE, Juriste européen, programme « Droit européen général »
Université Toulouse Capitole

Bulletin de
l'EDiHL
European Digital Health Law

Bulletin de l'EDiHL

European Digital Health Law

N° 1

1ère année – Bulletin annuel
Juin 2023-Juin 2024

Nathalie DE GROVE-VALDEYRON
Claire BORIES
Directrices scientifiques
Claire BORIES
Coordinatrice

Bulletin de l'EDiHL

European Digital Health Law

ACTUALITÉ DU DROIT EUROPÉEN DU NUMÉRIQUE EN SANTÉ
Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

À LA UNE

ESPACE EUROPÉEN DES DONNÉES DE SANTÉ

Vers une opérationnalisation de l'espace européen des données de santé (EEDS). Première analyse des projets de lignes directrices de l'action conjointe tehdas2 sur l'accès, l'utilisation et la sécurisation des données
par Winnie DONGBOU WAMBA

Consultation publique nationale « Construisons ensemble un patrimoine national des données de santé » et autres consultations publiques en matière d'utilisation secondaire des données de santé
Stratégie interministérielle pour construire notre patrimoine national des données de santé, Septembre 2024
par Lisa FERIOL

UTILISATION DE L'IA EN SANTÉ

Mettre l'intelligence artificielle au service de la santé : l'état des lieux du Ministère de la Santé et de l'Accès aux soins
Rapport du Ministère en charge de la santé, *Mettre l'intelligence artificielle au service de la santé – État des lieux de l'intelligence artificielle (IA) en santé*, Février 2025
par Joud GHARZEDDINE

RÈGLEMENTATION DES DISPOSITIFS MÉDICAUX

Le Règlement (UE) 2024/1860 du 13 juin 2024 : vers une mise en œuvre efficace d'EUDAMED ou une complexité accrue ?
par Kévin MINGOT

N° 2

2ère année – Bulletin annuel
Juin 2024 – Juin 2025

Cofinancé par l'Union européenne

Financé par l'Union européenne.

Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables

Funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them



ÉDITORIAL

Nathalie DE GROVE-VALDEYRON
Professeure de droit public
Chaire Jean Monnet (2017-2023) et (2023 - 2026)
Université Toulouse Capitole – IRDEIC

L'objet de ce bulletin qui porte sur le droit européen du numérique en santé est de suivre, au cours des trois années de la chaire Jean Monnet « EDIHL » (*European Digital Health Law*) dont je suis titulaire (2023-2026), l'activité législative, mais le cas échéant aussi contentieuse, de la construction de ce droit. Ce deuxième bulletin, coordonné par Claire BORIES, docteure en droit, spécialisée en droit de l'Union européenne, couvre la période de juin 2024 à juin 2025. Il témoigne de la place importante qu'occupe désormais ce droit naissant, l'année couverte étant particulièrement riche. L'adoption du règlement sur l'Espace européen des données de santé (EEDS), le 11 février 2025, représente à elle seule une évolution majeure tant ses implications sont et seront importantes à l'avenir, à la fois pour les patients mais aussi pour les professionnels de santé, les chercheurs et les détenteurs de données de santé. Certes des règlements d'exécution de la Commission sont encore attendus et une marge de manœuvre est laissée aux États, sur certains points jugés particulièrement sensibles, mais la locomotive est désormais en marche. Les États membres, certains plus rapidement que d'autres, compte tenu de leur degré d'intégration du numérique dans leurs systèmes de soins, pourront dès demain profiter des nouvelles perspectives offertes par le numérique en santé.

C'est aussi en juillet 2024 qu'a été publié le règlement sur l'IA (AI ACT) aujourd'hui largement commenté et dont les implications en santé seront également importantes, de nombreux produits de santé (et notamment les dispositifs médicaux à haut risque, faisant l'objet d'une évaluation de leur conformité par un « organisme notifié ») étant soumis à l'application du règlement. Il s'agira, ici aussi, d'intégrer dans les droits nationaux les nouvelles exigences mises en place par le droit de l'Union et d'articuler entre eux les deux récents règlements (en plus du RGPD qui trouve toujours à s'appliquer). Nul doute que les juristes spécialisés dans ce domaine seront sollicités dans les années à venir !

Ce bulletin entend surtout témoigner du rôle majeur de l'Union européenne dans le développement du numérique et notamment dans la création d'espaces de données spécifiques (aujourd'hui dans le domaine de la santé, demain dans d'autres domaines sectoriels comme l'agriculture). L'EEDS constitue ainsi une première manifestation opérationnelle de l'émergence de ce nouveau droit. Les enjeux sont immenses et les défis non moins importants comme l'a montré le colloque international organisé à Toulouse en juin 2024. Les communications présentées à l'occasion de ce colloque « Espace européen des données de santé et IA : enjeux juridiques et défis de mise en œuvre » peuvent être visionnées sur la chaine Youtube de l'Université Toulouse Capitole et les contributions, qui ont donné lieu à une publication aux Presses de Toulouse, sont accessibles en Open edition depuis le 6 mai 2025. Une publication portant sur « Le droit européen de la santé numérique, un droit en construction » (dir. N. DE GROVE -VALDEYRON) est sous presse chez Bruylant (publication juin 2025). Si la dimension du bulletin est principalement européenne, il ne néglige pas non plus les approches nationales, celles-ci étant essentielles pour comprendre l'intégration du numérique au sein des États membres. Le lecteur trouvera ainsi, dans ce deuxième bulletin, des incursions en droit français, belge et espagnol.

Bulletin de l'EDiHL
European Digital Health Law

Ce bulletin EDIHL n'existerait pas sans le soutien de chercheurs, de doctorants et docteurs en droit qui participent aussi activement aux activités de ma chaire, au-delà du bulletin. Qu'ils soient ici chaleureusement remerciés. Merci aussi aux étudiants du Master 2 droit de la santé et Master 2 juriste européen de l'Ecole de droit Toulouse (Université Toulouse Capitole) et du Master droit du numérique (Paris Sorbonne) qui ont participé avec enthousiasme à cette aventure. Un immense merci enfin à Claire BORIES pour son investissement remarquable dans la réalisation de ce bulletin et dans tant d'autres activités, qu'elles relèvent de la chaire – y compris dans ses enseignements au sein du DU EDIHL – ou en dehors du cadre de celle-ci, depuis de nombreuses années.

SOMMAIRE

N°2 /
2ème année – Bulletin annuel
Juin 2024-Juin 2025

VEILLE LÉGISLATIVE

Droit de l'Union européenne

LÉGISLATION EUROPÉENNE SUR L'INTELLIGENCE ARTIFICIELLE – AI ACT 9

Veille législative : le règlement européen sur l'intelligence artificielle appliqué au domaine de la santé
Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements n°s 300/2008/CE, 167/2013/UE, 168/2013/UE, 2018/858/UE, 2018/1139/UE et 2019/2144/UE et les directives n°s 2014/90/UE, 2016/797/UE et 2020/1828/UE, *JOUE* n° L 2024/1689 du 12 juillet 2024
par Luis HALEGUA 9

Lignes directrices de la Commission européenne sur les pratiques interdites en matière d'intelligence artificielle
Communication de la Commission du 4 février 2025 – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), *C(2025)* 884 final
Annexe de la communication de la Commission du 4 février 2025 – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), *C(2025)* 884 final
par Sarah BISTER 12

Plan d'action pour le continent de l'intelligence artificielle
Communication de la Commission du 9 avril 2025 – AI Continent Action Plan, *COM(2025)* 165 final
par Sarah BISTER 24

UTILISATION DE L'IA EN SANTÉ – EMA 28

EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, 9 September 2024
par Noémie DUBRUEL 28

EMA, Concept paper on the development of a Guideline on assessment and reporting of mechanistic models used in the context of model informed drug development, 20 January 2025
par Noémie DUBRUEL 29

EMA, Guiding principles on the use of large language models in regulatory science and for medicines regulatory activities, 29 August 2024 30

GROUPE DE PILOTAGE HMA – EMA 32

Note conjointe sous HMA-EMA, *Big Data Steering Group (BDSG), 2024 report*, EMA/471579/2024, 13 December 2024 ; HMA-EMA, *Joint HMA-EMA Network Data Steering Group*, EMA/419729/2024, 3 October 2024 et ; HMA-EMA, *Seizing opportunities in a changing medicines landscape - The European medicines agencies network strategy 2028*, 18 March 2025
par Valentine DURAND 32

Note conjointe sous HMA-EMA, *Joint HMA-EMA Network Data Steering Group*, EMA/419729/2024, 3 October 2024 et ; HMA-EMA, *Seizing opportunities in a changing medicines landscape - The European medicines agencies network strategy 2028*, 18 March 2025
par Winnie DONGBOU WAMBA 39

ESPACE EUROPÉEN DES DONNÉES DE SANTÉ – EEDS 41

Commission européenne, DG Santé, *Frequently Asked Questions on the European Data Health Space*, 5 March 2025
par Winnie DONGBOU WAMBA 41

Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement n° 2024/2847/UE, *JOUE* n° L 2025/327 du 5 mars 2025 42

Vers une opérationnalisation de l'espace européen des données de santé (EEDS). Première analyse des projets de lignes directrices de l'action conjointe TEHDAS2 sur l'accès, l'utilisation et la sécurisation des données
par Winnie DONGBOU WAMBA 42

RÈGLEMENTATION DES DISPOSITIFS MÉDICAUX 47

Le Règlement n° 2024/1860/UE du 13 juin 2024 : vers une mise en œuvre efficace d'EUDAMED ou une complexité accrue ?
Règlement n° 2024/1860/UE du Parlement européen et du Conseil du 13 juin 2024 modifiant les règlements n°s 2017/745/UE et 2017/746/UE en ce qui concerne un déploiement progressif d'EUDAMD, l'obligation d'informer en cas d'interruption ou de cessation d'approvisionnement et les dispositions transitoires applicables à certains dispositifs médicaux de diagnostic in vitro, *JOUE* n° L 2024/1860 du 9 juillet 2024
par Kévin MINGOT 47

RESPONSABILITÉ DU FAIT DES PRODUITS DÉFECTUEUX 52

Directive n° 2024/2853/UE relative à la responsabilité du fait des produits défectueux
Directive n° 2024/2853/UE du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive n° 85/374/CEE du Conseil, *JOUE* n° L 2024/2853 du 18 novembre 2024.
par Noémie DUBRUEL 52

CYBERSECURITÉ DE LA SANTÉ 55

Communication de la Commission du 15 janvier 2025 relative au « Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé », *COM(2025)* 10 final 55

Cybersolidarity Act – Règlement n° 2025/38/UE du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement n° 2021/694/UE, *JOUE* n° L 2025/38 du 24 janvier 2025 57

Droit français

UTILISATION DE L'IA EN SANTÉ 58

Mettre l'intelligence artificielle au service de la santé : l'état des lieux du Ministère de la Santé et de l'Accès aux soins
Rapport du Ministère en charge de la santé, *Mettre l'intelligence artificielle au service de la santé – État des lieux de l'intelligence artificielle (IA) en santé*, Février 2025
par Joud GHARZEDDINE 58

UTILISATION DE L'IA DANS LA RECHERCHE MÉDICALE – INSERM 61

Comité éthique de l'Inserm, *Guide de bonnes pratiques de l'Intelligence artificielle à l'Inserm*, Février 2025
par Noémie DUBRUEL 61

Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence artificielle dans la recherche à l'Inserm : la nécessité d'un arbitrage consciencieux entre soutien au progrès scientifique et prise en compte des risques délétères sous-jacents
Henry ATLAN et *al.*, *Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence Artificielle dans la recherche à l'Inserm. Guide de bonnes pratiques de l'Intelligence Artificielle à l'Inserm*, Février 2025
par Romane MASSIMI et Pierre-Emmanuel PARENT DE CURZON 63

UTILISATION SECONDAIRE DES DONNÉES DE SANTÉ 66

Consultation publique nationale « Construisons ensemble un patrimoine national des données de santé » et autres consultations publiques en matière d'utilisation secondaire des données de santé
Ministère du Travail, de la Santé et des Solidarité, *Stratégie interministérielle pour construire notre patrimoine national des données de santé*, Septembre 2024
par Lisa FERIOL 66

TRAITEMENT DES DONNÉES DE SANTÉ – RÉFÉRENTIELS SANTÉ 73

CNIL, *RÉFÉRENTIELS SANTÉ. Retour sur les contributions reçues dans le cadre de la consultation publique,* 10 décembre 2024 73

VEILLE CONTENTIEUSE 73

Conseil d'État, 10ème chambre, 12 juillet 2024, n° 488687, ECLI:FR:CECHS:2024:488687.20240712

CONSULTATION PUBLIQUE 73

IDENTITOVIGILANCE – RÉFÉRENTIEL INS 74

Arrêté du 12 décembre 2024 modifiant l'arrêté du 24 décembre 2019 portant approbation du référentiel relatif à l'identifiant national de santé, *JORF* n° 0294 du 13 décembre 2024 74

SÉGUR DU NUMÉRIQUE EN SANTÉ 75

Aperçu général sur le Ségur du numérique en santé 75

LE SÉGUR DU NUMÉRIQUE DANS LE SOCIAL & MÉDICO-SOCIAL : clôture de la Vague 1 76

Arrêté du 20 février 2025 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements, médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale – Fonction « partage d'images médicales » (= DRIMbox), *JORF* n° 0049 du 27 février 2025

Arrêté du 20 février 2025 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements, médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale – Fonction « système d'information de radiologie » – Vague 2 (= RIS), *JORF* n° 0049 du 27 février 2025

LE SÉGUR DU NUMÉRIQUE POUR LES SPÉCIALISTES DE L'IMAGERIE : lancement de la vague 2 77

Arrêté du 12 décembre 2024 modifiant l'arrêté du 7 septembre 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour le domaine protection de l'enfance » – Vague 1, *JORF* n° 0298 du 18 décembre 2024

Arrêté du 12 décembre 2024 modifiant l'arrêté du 2 février 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour les domaines personnes âgées, personnes en situation de handicap et acteurs de l'aide et du soin à domicile » – Vague 1, JORF n° 0298 du 18 décembre 2024

Arrêté du 12 décembre 2024 modifiant l'arrêté du 16 août 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour le domaine personnes en difficultés spécifiques » – Vague 1, *JORF* n° 0298 du 18 décembre 2024

ACTIVITÉS DE TÉLÉSURVEILLANCE MÉDICALE 78

Aperçu général sur activités de télésurveillance médicale 78

Inscription au remboursement du DMN de télésurveillance MyDiabby Healthcare pour le diabète gestationnel 79

Arrêté du 19 août 2024 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0199 du 22 août 2024

Arrêté du 19 août 2024 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0199 du 22 août 2024

Inscription au remboursement du DMN de télésurveillance Glooko XT pour le diabète gestationnel 79

Arrêté du 26 décembre 2024 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0309 du 31 décembre 2024

Arrêté du 26 décembre 2024 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0309 du 31 décembre 2024

Inscription au remboursement du DNM de télésurveillance Techcare pour le cancer 79

Arrêté du 31 mars 2025 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0081 du 4 avril 2025

Arrêté du 31 mars 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0081 du 4 avril 2025

Inscription au remboursement du DNM de télésurveillance Satelio Cardio pour l'insuffisance cardiaque 80

Arrêté du 28 mars 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0087 du 1er avril 2025

Arrêté du 28 mars 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0087 du 1er avril 2025

Fin de la prise en charge du DNM de télésurveillance Moovcare poumon pour le cancer 80

Arrêté du 14 février 2025 portant radiation d'un dispositif médical de la liste des produits et prestations

remboursables prévue à l'article L. 165-1 du code de la sécurité sociale, *JORF* n° 0040 du 16 février 2025

Arrêté du 31 mai 2024 modifiant l'arrêté du 24 juin 2021 relatif à l'expérimentation de télésurveillance médicale des patients transplantés, *JORF* n° 0132 du 8 juin 2024 **80**

CYBERSECURITÉ DE LA SANTÉ – CaRE 81

La cybersécurité des établissements de santé financée grâce au programme CaRE 81

Cour des comptes, *Observations définitives. La sécurité informatique des établissements de santé : un renforcement récent et à poursuivre, face à la multiplication des cyberattaques*, Octobre 2024 **82**

Instruction n° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaire, p. 57-61 **84**

Ministère de l'action publique et de la Fonction publique et de la simplification, *Plan de résilience des services publics face aux crises. Dossier de presse*, Avril 2025 **85**

LFSS POUR 2025 : TOUTES LES MESURES RELATIVES AU NUMÉRIQUE DE LA SANTÉ EN DÉTAIL 86

Loi n° 2025-199 du 28 février 2025 de financement de la sécurité sociale pour 2025 (1), *JORF* n° 0051 du 28 février 2025 **86**

Les mesures du numérique en santé censurées par le Conseil Constitutionnel
Conseil Constitutionnel, Décision du 28 février 2025 n° 2025-875 DC **88**

Droit belge

ACCÈS AUX DONNÉES DE SANTÉ 91

Arrêté royal du 15 décembre 2024 sur l'accès aux données de santé, M.B du 19 décembre 2024 **91**

Décret du 21 novembre 2024 relatif à la simplification administrative et aux communications par voie électronique entre les usagers et les autorités publiques wallonnes (1), M.B du 19 décembre 2024 **92**

Décret du 21 novembre 2024 relatif, pour les matières réglées en vertu de l'article 138 de la Constitution, à la simplification administrative et aux communications par voie électronique entre les usagers et les autorités publiques wallonnes (1), M. B. du 19 décembre 2024 94

Droit espagnol

DÉMATÉRIALISATION DE LA CARTE INDIVIDUELLE DE SANTÉ 95

Real Decreto 922/2024, de 17 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual, *BOE* núm. 226 de 18 de septiembre de 2024 **95**

VEILLE CONTENTIEUSE

Droit de l'Union européenne

VENTE EN LIGNE DE MÉDICAMENTS 96

Reconnaissance de la qualité à agir des concurrents de l'auteur présumé d'une violation du RGPD : la Cour de justice fait le choix d'un régime renforcé de protection

CJUE, 4 octobre, 2024, *Lindenapotheke*, aff. C-21/23, ECLI:EU:C:2024:846

par Joud GHARZEDDINE 96

Droit français

HÉBERGEMENT DES DONNÉES DE SANTÉ 100

Conseil d'État, 10ème chambre, 13 novembre 2024, *Association INTERHOP et autres*, n° 475297, ECLI:FR:CECHS:2024:475297.20241113 et Conseil d'État, 10ème chambre, 13 novembre 2024, n° 492895, ECLI:FR:CECHS:2024:492895.20241113

par Maximilien MAUGEAIS 100

Le Conseil d'État valide l'hébergement des données de santé par Microsoft dans le projet DARWIN.EU

Conseil d'État, Juge des référés, 25 avril 2025, n° 503163, ECLI:FR:CEORD:2025:503163.20250425 **107**

ACCÈS AU DOSSIER MÉDICAL PARTAGÉ

Modalités d'accès au dossier médical partagé d'un patient par des professionnels « hors santé » participant à sa prise en charge : une affirmation non équivoque de constitutionnalité

Conseil Constitutionnel, 12 septembre 2024, Décision n° 2024-1101 QPC, *JORF* n° 0218 du 13 septembre 2024

Conseil d'État, 10ème et 9ème chambres réunies, 10 juin 2024, n° 490409, ECLI:FR:CECHR:2024:490409.20240610

par Joud GHARZEDDINE 108

Droit de l'Union européenne

Veille législative : le règlement européen sur l'intelligence artificielle appliqué au domaine de la santé

par Luis HALEGA

Étudiant en Master 2 Droit de la santé et de la protection sociale, Université Toulouse Capitole

Introduction

« L'intelligence artificielle est un outil puissant, mais elle ne doit jamais supplanter la sagesse humaine dans les décisions qui engagent la vie et la dignité des individus ». Par cette phrase, la juriste française Mireille Delmas-Marty soulève une question qui fait couler beaucoup d'encre dans l'opinion publique : l'intelligence artificielle (IA) médicale est-elle une bénédiction pour la science ou une menace pour les droits fondamentaux de tout un chacun ? Depuis le 13 juin 2024, une loi[1] 1 encadre son utilisation afin d'éviter les abus, les discriminations et les erreurs qui "pourraient" coûter bien plus qu'un simple bug dans un logiciel.

Avant d'entrer dans le vif du sujet, il est essentiel de comprendre comment ce règlement a vu le jour. Contrairement aux législations nationales, le droit de l'Union européenne (UE) repose sur un équilibre complexe entre les institutions. Le règlement sur l'intelligence artificielle (RIA) n'a pas émergé du néant, il s'inscrit à ce titre dans une dynamique de régulation numérique amorcée dès la fin des années 2010, avec des textes comme le règlement général sur la protection des données (RGPD)[2] ou encore le Digital Services Act (DSA)[3].

Le processus législatif a débuté par une proposition de la Commission européenne en avril 2021, dans le cadre de sa stratégie numérique. Après un long processus de négociation, impliquant le Parlement européen et le Conseil de l'UE, le texte a été amendé, précisé, parfois controversé. Les États membres ont débattu de la place à accorder aux innovations médicales, entre protection des citoyens et compétitivité économique. Finalement, la version définitive dudit règlement a été adoptée en 2024, marquant une étape majeure dans la régulation des technologies d'IA appliquées à la santé.

Avec l'essor du deep learning et des réseaux neuronaux convolutifs, l'intelligence artificielle a investi le domaine médical comme un chirurgien en salle d'opération. Diagnostic assisté, dispositifs médicaux intelligents, médecine personnalisée : la machine est partout, plus rapide que l'œil humain, plus précise qu'une

[1] Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* n° L 2024/1689 du 12 juillet 2024.

[2] Règlement n° 2016/679/UE 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, *JOUE* n° L 119/1 du 4 mai 20216.

[3] Règlement n° 2022/2065/UE du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive n° 2000/31/C, *JOUE* n° L 277/1 du 27 octobre 2022.

main experte. Mais que se passe-t-il lorsque la machine se trompe ? Qui en est responsable ? Et surtout, *quid* des algorithmes mal créés qui produisent des biais injustes ? Autant de questions cruciales auxquelles le RIA tente d'apporter des réponses.

Afin de garantir la sécurité juridique et de suivre le rythme des avancées technologiques, le règlement encadre strictement la notion de « système d'IA ». Cette définition s'aligne sur les standards internationaux et repose sur un élément clé, en l'occurrence la capacité d'inférence qui peut se définir comme le processus par lequel un système d'IA génère des prédictions, des recommandations ou des décisions influençant l'environnement physique ou numérique. Loin d'être un simple outil de traitement de données, l'IA intègre ainsi des mécanismes d'apprentissage et de raisonnement. Son autonomie relative lui permet d'opérer avec une intervention humaine minimale, soulevant des enjeux majeurs en matière de contrôle et de responsabilité juridique.

Au demeurant, le texte définit également un cadre strict, avec des niveaux de risque allant du « risque inacceptable » où l'IA se voit tout bonnement interdite au « risque élevé », exigeant des garanties solides en matière de transparence et de protection des données. Mais au fond, il semble opportun d'admettre qu'il y a, depuis peu, une tension entre deux mondes, celui de la promesse technologique, et celui du droit qui tente d'encadrer cette révolution sans en étouffer l'élan.

C'est précisément dans cette dualité que s'inscrit la veille juridique soumise à l'étude. D'un côté, l'IA révolutionne l'acte médical, du diagnostic à la prise en charge thérapeutique, remettant en question le rôle traditionnel du médecin (**I**). De l'autre, cette avancée soulève des problématiques majeures à l'instar de la responsabilité juridique, transparence algorithmique, discrimination involontaire (**II**) que le RIA cherche à remédier.

I. LE SERMENT D'HIPPOCRATE A L'EPREUVE DES ALGORITHMES

Longtemps, l'acte médical s'est fondé sur l'expertise humaine, sur cette capacité intuitive du médecin à décrypter les signes cliniques, à interpréter ce que les examens ne révèlent pas toujours explicitement. *Ars medica*[4], science autant qu'art, reposait sur l'empirisme et le discernement. Mais avec l'essor des algorithmes, la médecine connaît une transformation radicale puisqu'en effet, les systèmes d'intelligence artificielle, analysant des volumes massifs de données, surpassent parfois l'œil humain en matière de précision diagnostique. La détection des tumeurs via l'imagerie médicale en est l'exemple le plus frappant. Cette évolution, bien qu'indéniablement bénéfique, ne se réduit pas à un simple progrès technique. Elle ouvre un débat fondamental, non plus entre tradition et modernité, mais entre la puissance des algorithmes et les impératifs éthiques et juridiques.

Le RIA du 13 juin 2024 consacre cette tension en posant un principe structurant : *fiat justitia, ruat caelum*, la justice doit être rendue, quoi qu'il en coûte. En d'autres termes, si l'IA est un levier d'innovation, son utilisation dans la prise de décision médicale doit impérativement s'inscrire dans le respect des droits fondamentaux. Toujours est-il, là où il y a un droit, il doit y avoir un recours. Que se passe-t-il lorsqu'une décision médicale automatisée se révèle biaisée ou injuste ?

L'exemple des algorithmes de tri des patients en attente de transplantation est une parfaite illustration. Dans une logique purement statistique, ces systèmes attribuent les greffons en fonction de critères quantifiables, à savoir l'état de santé, la compatibilité biologique,

[4] Palmieri Nicoletta, *L'art medica de Galien: lectures antiques et médiévales*, Publication de l'Université Saint-Étienne, 2018, 219 p.

l'espérance de vie post-opératoire. Mais un biais algorithmique, qu'il soit dû à une base de données déséquilibrée ou à un défaut de paramétrage, peut engendrer des décisions dramatiques. Un patient se voit refuser une greffe, non en raison d'un arbitrage médical éclairé, mais parce que son profil statistique le classe comme « non prioritaire ». Dès lors, l'application aveugle d'une règle, sans prise en compte des réalités humaines, peut aboutir à l'injustice la plus absolue.

Ce faisant, face à ces dérives potentielles, le RIA pose des garde-fous. L'article 14 impose une obligation de transparence et de traçabilité des décisions algorithmiques dans le domaine médical. Toute décision prise par un système d'IA ayant une incidence sur les droits d'un patient doit être explicable, vérifiable et justifiable et en ce sens, il ne saurait exister de vide juridique dans le contrôle de ces outils. La loi du 12 juin 2024, dans cette lignée, rappelle que la responsabilité ne peut être diluée dans l'opacité des algorithmes. Médecins, concepteurs de logiciels et établissements de santé demeurent comptables des choix effectués. Ainsi, loin d'être un simple outil technique, l'IA médicale s'inscrit dans un cadre normatif strict, visant à concilier innovation et protection des patients. Si son potentiel est immense, sa régulation l'est tout autant, afin d'éviter que la rationalité algorithmique ne prenne le pas sur la justice et l'équité du soin.

II. LE RIA FACE AUX DERIVES ALGORITHMIQUES

Les histoires récentes qu'il y a eues ont prouvé que l'intelligence artificielle peut être aussi discriminante qu'un assureur en quête de bons profils. Loin d'être un risque hypothétique, ces biais algorithmiques sont une réalité documentée. En 2019, une étude parue dans *Science* révélait qu'un algorithme utilisé aux États-Unis sous-évaluait systématiquement les besoins des patients noirs, non par intention malveillante, mais en raison d'une base de données insuffisamment représentatives[5]. A cet égard, si un biais s'immisce dans l'entraînement du modèle, c'est toute l'équité du système de soins qui s'effondre. Ce type de dérive est précisément ce que le RIA entend empêcher.

Par ailleurs, le fondement juridique de cette lutte contre les discriminations algorithmiques est limpide. L'article 21 de la Charte des droits fondamentaux de l'UE interdit toute discrimination fondée sur la race, le sexe ou toute autre caractéristique protégée. En vertu du principe *ubi lex, ibi poena*[6], si un modèle d'IA produit des décisions biaisées en raison de données défectueuses, alors son utilisation devient illégale, c'est ce qu'il appert de l'article 10 du RIA, qui impose aux concepteurs d'IA d'assurer une qualité suffisante des jeux de données utilisés pour l'entraînement des modèles. Loin d'être un simple garde-fou éthique, cette disposition pose une obligation positive de vigilance à l'égard des biais implicites.

Cependant, le risque ne s'arrête pas là. L'IA n'est pas seulement un outil de diagnostic, elle est aussi un instrument d'individualisation des traitements. Avec l'essor de la médecine personnalisée, elle analyse le génome des patients pour ajuster les prescriptions thérapeutiques. Or, qui bénéficiera réellement des traitements ultraciblés ? S'agira-t-il de l'ensemble des patients ou uniquement de ceux en mesure de financer ces avancées ? La question n'est pas purement théorique. En l'absence d'encadrement strict, l'IA médicale pourrait accentuer les fractures socio-économiques plutôt que les résorber.

Le législateur européen a anticipé ces dérives potentielles. L'article 9 du RIA impose une évaluation préalable rigoureuse des systèmes d'IA médicale avant leur mise sur le marché. Cet encadrement repose sur le principe *ex ante*, selon lequel une

[5] Ziad Obermeyer et *al.*, « Dissecting racial bias in an algorithm used to manage the health of populations », Science, vol. 366, n° 6464, p. 447-453.

[6] « Là où il y a une norme, il y a une sanction ».

technologie ne peut être déployée que si elle respecte des exigences strictes en matière de transparence et d'équité. Cette logique de précaution s'accompagne d'une obligation de traçabilité des décisions algorithmiques, afin que chaque patient puisse comprendre les critères ayant influencé son accès aux soins.

Conclusion

Ainsi, le règlement du 13 juin 2024 ne saurait être réduit à une simple réglementation technique. Cette réglementation traduit une prise de conscience profonde : celle que les algorithmes, loin d'être des entités neutres, sont le reflet des choix de conception et des biais inhérents aux données qui les nourrissent. Si le droit n'intervient pas pour en fixer les limites, le risque est grand de voir émerger une médecine à deux vitesses, où l'accès aux traitements et aux décisions médicales serait conditionné par des critères opaques et parfois discriminants. C'est tout l'enjeu du principe de responsabilité algorithmique, qui repose sur l'idée que la performance ne peut jamais être poursuivie au détriment de la justice sociale et du respect des droits fondamentaux. *Lex praecedit machinam* : cette fois, c'est peut-être la loi qui devance la machine.

Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements n°s 300/2008/CE, 167/2013/UE, 168/2013/UE, 2018/858/UE, 2018/1139/UE et 2019/2144/UE et les directives n°s 2014/90/UE, 2016/797/UE et 2020/1828/UE, *JOUE* n° L 2024/1689 du 12 juillet 2024.

Lignes directrices de la Commission européenne sur les pratiques interdites en matière d'intelligence artificielle

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en droit public

Le 4 février 2025, la Commission européenne approuvait le projet de lignes directrices sur les pratiques interdites en matière d'intelligence artificielle[7] (ci-après « IA ») afin de clarifier l'application des dispositions de l'article 5 du règlement (UE) 2024/1689 sur l'intelligence artificielle[8] (ci-après « AI Act »).

L'AI Act a été élaboré pour harmoniser l'utilisation de l'IA dans l'ensemble de l'Union européenne (« UE ») dans l'objectif de protéger les droits de l'homme et les libertés fondamentales.

L'AI Act est entré en vigueur le 1er août 2024. Mais son entrée en application est prévue de manière échelonnée afin de permettre aux acteurs concernés de se mettre en conformité. L'AI Act adopte une approche fondée sur les risques, classant les systèmes d'IA en quatre catégories selon *« l'intensité et […] la portée des risques [qu'ils] peuvent générer »*[9], allant des systèmes à risque minimal aux systèmes à risque inacceptable, pour lesquels l'utilisation est strictement interdite.

L'article 5 de l'AI Act, énumérant les pratiques interdites jugées incompatibles

[7] *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* C(2025) 884 final et *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 884 final.

[8] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE du 12 juillet 2024.

[9] Considérant 26 de l'AI Act.

avec les principes fondamentaux de l'Union, est entré en application le 2 février 2025[10]. Depuis cette date, tous les systèmes d'IA, y compris ceux déjà utilisés, sont censés être conformes. C'est donc seulement deux jours après l'entrée en application de cet article 5 que les présentes lignes directrices, très attendues, ont été publiées. Bien que non-contraignantes, elles n'en sont pas moins cruciales pour toutes les parties prenantes impliquées dans les systèmes d'IA. Première étape de mise en œuvre de l'AI Act, elles visent à soutenir l'innovation tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux[11].

I. PRECISIONS SUR LE CHAMP D'APPLICATION DE L'AI ACT

Avant d'entrer plus en détail dans chacune des interdictions prévues par la réglementation, la Commission a pris le soin de revenir sur le champ d'application et les exclusions mentionnés dans l'AI Act.

L'AI Act distingue différentes catégories d'opérateurs en lien avec les systèmes d'IA : les fournisseurs, les déployeurs, les importateurs, les distributeurs et les fabricants de produits.

Les fournisseurs sont définis comme les personnes physiques ou morales, les autorités publiques, agences ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, que ce soit à titre onéreux ou gratuit[12].

Les déployeurs sont entendus comme les personnes physiques ou morales, les autorités publiques, les agences ou tout autre organisme utilisant sous leur propre autorité un système d'IA, à moins que ce système ne soit utilisé de manière non professionnelle[13].

Personnes physiques ou morales établies dans l'Union européenne, les importateurs et les distributeurs mettent sur le marché de l'Union ou à disposition dans l'Union un système d'IA[14].

Quant aux fabricants de produits, il s'agit des personnes physiques ou morales qui mettent sur le marché ou mettent en service un système d'IA sous leur propre nom ou propre marque[15].

Les lignes directrices s'adressent aux fournisseurs et aux déployeurs de système d'IA. Après avoir rappelé les définitions de ces deux catégories d'opérateurs, une précision importante est apportée : les opérateurs peuvent cumuler simultanément plusieurs rôles. Ainsi, un opérateur, qui développe son propre système d'IA qu'il utilise par la suite, sera considéré à la fois comme un fournisseur et comme un déployeur de ce système, quand bien même ce système serait aussi utilisé par d'autres déployeurs à qui il aurait été fourni à titre onéreux ou gratuit[16].

Cela pouvait effectivement sembler logique, pour autant, une précision en ce sens est toujours bienvenue pour lever tout doute quant au cumul des obligations applicables.

Les pratiques interdites par l'AI Act s'appliquent lors de la mise sur le marché[17], la mise en service[18] ou l'utilisation d'un système d'IA. Les lignes directrices reviennent sur chacune de ces notions par des exemples concrets, mais surtout, comblent l'absence de définition de la notion d'« utilisation » qui n'est pas explicitement abordée dans l'AI Act.

[10] Article 113 de l'AI Act.
[11] Article 1er de l'AI Act.
[12] Article 3 (3) de l'AI Act.
[13] Article 3 (4) de l'AI Act.
[14] Articles 3 (6) et 3 (7) de l'AI Act.
[15] Article 2, point 1 e) de l'AI Act.
[16] Paragraphe 19, p.6, des lignes directrices.
[17] La mise sur le marché se définit comme *« la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'Union »*, article 3 (9) de l'AI Act.
[18] La mise en service s'entend de *« la fourniture d'un système d'IA en vue d'une première utilisation directement au déployeur ou pour usage propre dans l'Union, conformément à la destination du système d'IA »*, article 3 (11) de l'AI Act.

L'utilisation doit être entendue au sens large, couvrant l'utilisation ou le déploiement du système à tout moment de son cycle de vie après avoir été mis sur le marché ou mis en service. Cela inclut également toute utilisation néfaste et abusive du système d'IA susceptible d'être assimilée à une pratique interdite[19]. Les lignes directrices illustrent ceci avec l'exemple de l'interdiction par l'employeur d'utiliser un système d'IA pour déduire les émotions sur le lieu de travail, hormis le cas où le système serait utilisé à des fins médicales ou de sécurité. Cette interdiction s'applique donc aux déployeurs que le fournisseur du système ait ou non exclu une telle utilisation dans les conditions d'utilisation.

L'article 2 de l'AI Act prévoit un certain nombre d'exclusions générales du champ d'application, sur lesquelles reviennent les lignes directrices afin de mieux appréhender l'application pratique des interdictions des systèmes d'IA. Sont ainsi concernés :

- les systèmes utilisés exclusivement à des fins militaires, de défense ou de sécurité nationale ;
- les systèmes utilisés dans le cadre de la coopération judiciaire et répressive avec les États membres pour autant que des garanties appropriées soient en place ;
- les activités de recherche et développement scientifiques tant que le système d'IA n'est pas mis sur le marché. Cela signifie, selon les lignes directrices, qu'au cours de la phase de recherche et développement, les développeurs d'IA ont la liberté d'expérimenter et de tester de nouvelles fonctionnalités pouvant faire appel à des techniques pouvant être considérées comme manipulatrices et couvertes par l'interdiction de l'article 5 de l'AI Act, si elles étaient utilisées dans des applications destinées aux consommateurs[20]. Mais une fois mis sur le marché ou mis en service, le règlement sera applicable ;
- les activités personnelles à caractère non-professionnel ;
- les systèmes d'IA publiés dans le cadre de licences libres et ouvertes, sauf s'ils sont mis sur le marché ou mis en service en tant que système d'IA à haut risque ou système interdit par l'article 5.

En revanche, les lignes directrices indiquent clairement que les interdictions de l'article 5 concernent à la fois les systèmes d'IA à usage général et les systèmes d'IA ayant une destination. Il y est précisé que si le préjudice découle souvent de la manière dont les systèmes d'IA sont utilisés dans la pratique, les fournisseurs ont également la responsabilité de ne pas mettre sur le marché ou en service des systèmes d'IA, y compris des systèmes d'IA à usage général, qui sont raisonnablement susceptibles de se comporter ou d'être directement utilisés d'une manière interdite par l'article 5 de l'AI Act[21]. En conséquence, les fournisseurs sont également censés prendre des mesures efficaces et vérifiables pour mettre en place des mesures de protection pour prévenir les abus. Ils doivent également, dans leurs relations contractuelles, exclure l'utilisation du système d'IA pour des pratiques interdites et fournir aux déployeurs des informations appropriées dans les instructions d'utilisation concernant la surveillance humaine.

II. PRATIQUES INTERDITES EN VERTU DE L'ARTICLE 5 DE L'AI ACT

Pour chacune des pratiques interdites décrites à l'article 5 de l'AI Act, le projet de lignes directrices apporte un aperçu des principaux éléments de la disposition de l'article, des exemples pratiques, des éclaircissements sur les pratiques qui ne sont pas visées par les interdictions et sur les mesures qui peuvent être prises pour éviter

[19] Paragraphe 14, p. 5, des lignes directrices et considérant 28 de l'AI Act.

[20] Lignes directrices, paragraphe 30, p. 9.

[21] Lignes directrices, paragraphe 40, p. 13.

de fournir ou d'utiliser des systèmes d'IA d'une manière susceptible d'être interdite.

Afin de simplifier la lecture des apports des lignes directrices, une présentation sous forme de tableau est proposée. **Page suivante**

Pratiques interdites	Points clés de l'AI Act	Points clés des lignes directrices	Exemples de systèmes d'IA interdits (non exhaustifs)	Exemples de systèmes d'IA légaux
Techniques subliminales, délibérément manipulatrices ou trompeuses	Système d'IA qui • a recours à des techniques subliminales ou à des techniques délibérément manipulatrices ou trompeuses • avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne ou d'un groupe de personnes • en portant considérablement atteinte à leur capacité à prendre une décision éclairée, amenant ainsi la personne à prendre une décision qu'elle n'aurait pas prise autrement • d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne, à une autre personne ou à un groupe de personnes	• Systèmes d'IA manipulant des individus sans qu'aucun humain ne le veuille couverts par l'interdiction des techniques de manipulation intentionnelle. Pas de nécessité d'avoir l'intention de tromper • Réduction du risque de tromperie et d'effets de distorsion nuisibles sur la formation des opinions, des croyances et du comportement de l'individu par l'étiquetage visible des « deep fakes » et des chatbots	• Messages subliminaux visuels (images clignotantes), auditifs (sous masqués ou à faible volume), tactiles (sensations physiques) • Chatbot se faisant passer pour un ami d'une personne avec une voix synthétique et tentant de faire croire qu'il s'agit de la personne, ce qui entraîne des escroqueries et des préjudices importants	• Systèmes proposant des recommandations publicitaires personnalisées sur la base du consentement de l'utilisateur • Systèmes analysant les émotions des clients pour améliorer le service, sous réserve qu'ils fonctionnent de manière transparente
Techniques exploitant des vulnérabilités	Système d'IA qui • exploite les vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne physique ou d'un groupe de personnes donné • avec pour objectif ou effet d'altérer substantiellement le comportement de cette	• Définition large de la notion de « vulnérabilités » incluant les formes de vulnérabilité cognitive, émotionnelle, physique et autres • Limitation aux personnes concernées par l'interdiction en raison de	• Jeu alimenté par l'IA encourageant les enfants à relever des défis de plus en plus risqués • Jeu alimenté par l'IA analysant le comportement individuel et les préférences des enfants et créant des récompenses	• Systèmes d'IA susceptibles de ne causer aucun dommage significatif comme un chatbot thérapeutique utilisant des techniques subliminales pour orienter les utilisateurs vers un mode de vie plus sain et

	personne ou d'un membre de ce groupe • d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à un tiers	leur âge, handicap ou situation socio-économique	personnalisées renforçant leur addiction au jeu • Robot destiné à aider les personnes âgées exploitant leur situation pour les forcer à effectuer certaines activités contre leur gré, pouvant aggraver considérablement leur santé mentale et leur causer de graves préjudices psychologiques • Chatbot thérapeutique destiné aux personnes handicapées mentales exploitant leurs capacités intellectuelles limitées pour les inciter à acheter des produits médicaux coûteux • Algorithme prédictif d'IA ciblant des personnes à faible revenu avec des publicités pour produits financiers prédateurs	stopper les mauvaises habitudes
Classification/notation sociale	Système d'IA • pour l'évaluation ou la classification de personnes physiques ou de groupes de personnes au cours d'une période donnée	• Inclusion des systèmes d'IA effectuant le profilage de personnes physiques en vertu de la législation de l'UE sur la protection des données à caractère personnel	• Système d'IA utilisé par une administration fiscale pour détecter les fraudes aux allocations familiales en établissant des profils et classant les bénéficiaires soupçonnés sur la base de	• Pratiques légitimes de notation conformes au droit de l'UE ou droit national comme les systèmes dévaluation du crédit financier

	• en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, conduisant au traitement préjudiciable ou défavorable
	  ○ dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine
	  ○ injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci
		• Inclusion des pratiques de notation fondées sur l'IA pouvant combiner une évaluation humaine
		
		• Possibilité de traitement préjudiciable ou défavorable même si la notation est produite par une organisation différente de celle utilisant le score
			critères tels que le faible revenu, la double nationalité, le comportement social. De la notation découlent des inspections
			
			• Collecte d'information auprès d'une banque par une compagnie d'assurance sur les dépenses et autres informations financières non déterminante pour l'éligibilité à un contrat mais utilisées pour déterminer le prix de la prime à payer
			
			• Mise en œuvre d'un système de surveillance partiellement automatisé dans les camps de réfugiés par une autorité chargé de l'immigration et de l'asile basé sur une série d'infrastructures de surveillance (caméras et détecteurs de mouvement notamment)
				• Système d'IA utilisant des données collectées dans les camps de réfugiés pour prendre des décisions en matière de réinstallation ou d'emploi
				
				• Plateforme de profilage des utilisateurs pour des raisons de sécurité sur leurs services

Évaluations des risques et prédiction des infractions pénales	Système d'IA • pour mener des évaluations des risques des personnes physiques visant à évaluer ou à prédire le risque qu'une	• Application aux acteurs privés si ○ agissement dans le cadre de pouvoir confier par la loi	• Système d'IA utilisée par une autorité pour prédire le comportement criminel tels que le terrorisme, uniquement sur la base de l'âge, de la nationalité, de	• Système d'IA utilisé par les services de police pour prédire la probabilité de criminalité des différentes zones d'une ville sur la base des taux de

	personne physique commette une infraction pénale • uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques	○ si évaluation ou prédiction nécessaire pour se conformer à une obligation légale • Exclusion des systèmes de prévision de la criminalité de personnes morales (entreprises ou organisations non gouvernementales)	l'adresse, du type de voiture et de l'état civil des individus • Système d'IA utilisé par les services de police pour évaluer le risque que les jeunes enfants et adolescents soient impliqués dans de futurs délits violents et contre les biens	criminalité antérieurs par zone et d'autres informations complémentaires • Système d'IA utilisé par les services de police pour détecter et localiser les coups de feu en temps réel grâce à des capteurs acoustiques • Système d'IA soutenant l'évaluation humaine et permettant de profiler et catégoriser un comportement dangereux raisonnablement suspect dans une foule
Reconnaissance faciale par moissonnage non ciblé	Système d'IA • créant ou développant des bases de données de reconnaissance faciale • par le moissonnage non ciblé d'images faciales • provenant de l'internet ou de la vidéosurveillance	• Capacité pour les bases de reconnaissance faciale de faire correspondre un visage humain provenant d'une image numérique ou d'une séquence vidéo à une base de données de visages. Il peut ne pas s'agir de leur seul but • Notion de non ciblée signifiant que l'on ne se concentre pas spécifiquement sur un individu ou groupe d'individus donné	• Entreprises collectant via un système d'IA des photos sur les réseaux sociaux sans le consentement de l'utilisateur pour former des modèles de reconnaissance faciale	• Système d'IA récoltant de grandes quantités d'images faciales sur Internet pour former des modèles d'IA qui génèrent de nouvelles images de personnes fictives

		• Si collecte d'images ou de vidéos de visages humains uniquement de personnes spécifiques ou groupe de personnes prédéfini, alors moissonnage ciblé • Interdiction non applicable au moissonnage non ciblé de données biométriques autre que les images faciales comme des échantillons de voix		
Reconnaissance des émotions sur les lieux de travail et dans les établissements d'enseignement	Systèmes d'IA • pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement • sauf utilisation du système d'IA mise en place ou mise sur le marché pour des raisons médicales ou de sécurité	• Inclusion à la fois des systèmes d'IA identifiant ou déduisant des émotions ou intentions • Interprétation large de la notion d'émotions ou d'intentions • Interprétation large de la notion de lieu de travail, applicable également aux candidats pendant une procédure de sélection et d'embauche	• Système d'IA déduisant des émotions à partir de la frappe sur un clavier, des expressions faciales, des postures ou des mouvements du corps basé sur des données biométriques • Utilisation par un centre d'appel de vidéosurveillance et de systèmes de reconnaissance vocale pour suivre les émotions des employés telle que la colère • Utilisation d'un système d'IA de reconnaissance des émotions par un établissement d'enseignement lors de	• Système d'IA déduisant des émotions sur le lieu de travail et dans les établissements d'enseignement pour des raisons médicales ou de sécurité • Système d'IA déduisant des émotions à partir d'un texte écrit et non basé sur des données biométriques • Système d'IA détectant des états physiques tels que la douleur ou la fatigue pour prévenir des accidents • Système d'IA pour détecter des émotions en dehors des lieux de travail

			tests d'amissibilité pour les nouveaux étudiants	et d'enseignement par exemple pour suivre les émotions des clients
Catégorisation biométrique	Système d'IA • catégorisant individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle • sauf étiquetage ou filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif	• Catégorisation par un système biométrique n'est pas une identification d'une personne ou vérification de son identité mais une classification d'une personne dans une catégorie • Application de l'interdiction en cas de catégorisation individuelle de personnes physiques	• Système d'IA classant les personnes actives sur une plateforme de médias sociaux en fonction de leur orientation politique supposée en analysant les données biométriques des photos téléchargées par elles sur la plateforme afin de leur envoyer des messages politiques ciblés • Système d'IA catégorisant les personnes actives sur une plateforme de médias sociaux en fonction de leur orientation sexuelle supposée en analysant des photos partagées sur cette plateforme afin de leur proposer des publicités • Système de catégorisation biométrique capable de déduire la race d'une personne à partir de sa voix • Système de catégorisation biométrique capable de déduire l'orientation religieuse d'une personne à	• Système d'IA de catégorisation biométrique accessoire à un service commercial et strictement nécessaire pour des raisons techniques objectives • Etiquetage ou filtrage d'ensembles de données biométriques légalement acquis

			partir de ses tatouages ou de son visage	
Identification biométrique à distance en temps réel à des fins répressives	Systèmes d'IA • d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives • sauf si strictement nécessaire pour un ensemble d'objectifs strictement définis tels que la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ou de personnes disparues, la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes, la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale	• Interdiction applicable à l'utilisation uniquement et non à la mise sur le marché • Exclusion de la notion « à distance » des systèmes biométriques pour confirmer l'identité d'une personne dans le seul but d'avoir accès à un service, de déverrouiller un appareil ou d'avoir un accès sécurisé à des locaux	• Système de reconnaissance en temps réel dans la rue pour des raisons de sécurité générale, de prévention de la criminalité ou surpeuplement	• Système d'identification biométrique à distance en temps réel utilisé par les services de police pour identifier un voleur à l'étalage et compare les images faciales à des bases données criminelles

III. IMPLICATIONS OPERATIONNELLES ET SANCTIONS

Au vu de la longueur et de la richesse des lignes directrices émises par la Commission, il est évident que le cadre réglementaire entourant les systèmes interdits visés à l'article 5 de l'AI Act est complexe. Les fournisseurs de systèmes d'IA et les déployeurs devront procéder à une évaluation préliminaire approfondie des interdictions énoncées.

Des analyses d'impact devront être réalisées incluant non seulement les aspects liés à la protection des données personnelles conformément au règlement général sur la protection des données, tout en prenant en considération les dimensions de risque supplémentaires identifiées par l'AI Act.

Ces lignes directrices restent, à l'heure de rédaction de cet article, à l'état de projet. Même, si à terme, elles ne revêtiront pas un caractère contraignant, elles apportent déjà de précieuses précisions sur la portée des interdictions. Pour autant, certaines questions restent en suspens notamment s'agissant de la coordination pratique entre les autorités compétentes en matière d'IA et les autorités de protection des données, les critères d'évaluation du seuil d'importance du préjudice nécessaires à l'établissement de pratiques interdites ou encore l'identification des frontières entre les pratiques permises au regard des exemptions prévues dans l'AI Act et les pratiques interdites.

Les opérateurs ne pourront faire l'économie de la mise en œuvre de mesures techniques et organisationnelles pour intégrer l'ensemble des exigences réglementaires dès la phase de conception des systèmes d'IA. L'accompagnement de personnels formés dans le développement et l'utilisation des systèmes d'IA sera incontournable.

En termes de sanctions, la violation des interdictions prévues à l'article 5 de l'AI Act est la plus sévèrement punie par le régime fixé par le règlement. Ainsi, toute violation de pratiques interdites sera susceptible d'entraîner une amende administrative pouvant aller jusqu'à 35 millions d'euros ou, pour les entreprises, jusqu'à 7% de leur chiffre d'affaires mondial total de l'exercice précédent, le montant le plus élevé étant retenu. En outre, en cas d'infractions répétées, l'amende maximale pourra être majorée jusqu'à 2%, accentuant encore davantage l'effet dissuasif.

Le régime des sanctions est applicable à compter du 2 août 2025. Néanmoins, les interdictions posées à l'article 5 de l'AI Act ont un effet direct, dès leur entrée en application, pour les fournisseurs et les déployeurs de systèmes d'IA. Cela signifie que toute partie concernée peut les faire appliquer devant les tribunaux nationaux et demander des injonctions provisoires à l'encontre de pratiques interdites[22].

Communication de la Commission du 9 avril 2025 – AI Continent Action Plan, *COM(2025)* 165 final

[22] Paragraphe 432, p. 135, des lignes directrices.

Plan d'action pour le continent de l'intelligence artificielle

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en droit public

Leader mondial de l'intelligence artificielle. Voilà l'objectif clairement affiché de l'Union européenne. Le législateur européen ne compte pas s'arrêter à l'adoption du règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle[23] (« AI Act »). Afin de devenir un acteur monial de premier plan dans le domaine de l'intelligence artificielle (« IA »), cela n'est pas suffisant. C'est ainsi que la Commission européenne a présenté, le 9 avril 2025, un ensemble de mesures ambitieuses traduit dans un plan d'action pour un continent de l'IA[24]. Cette initiative répond au rapport sur la compétitivité de l'ancien président de la Banque centrale européenne, Mario DRAGHI, qui avertissait que l'Union européenne se devait d'intensifier les investissements, de simplifier la réglementation et de mener une politique industrielle coordonnée si elle voulait combler le fossé d'innovation avec les États-Unis et la Chine[25].

S'appuyant sur les recommandations de ce rapport, la Commission avait déjà publié « la boussole pour la compétitivité »[26], en janvier 2025, destinée à orienter les travaux de la Commission pour les cinq prochaines années. Cette feuille de route s'articule autour de trois objectifs : réduire le déficit d'innovation, décarboner l'économie et réduire les dépendances stratégiques.

Le plan d'action pour un continent de l'IA transforme ces objectifs en actions à travers cinq piliers clés : la puissance de calcul et l'infrastructure, les données pour l'IA, l'innovation stratégique et l'adoption de l'IA, les compétences et les talents de l'IA et la simplification réglementaire.

I. INFRASTRUCTURE INFORMATIQUE DE CALCUL À GRANDE ECHELLE

Une infrastructure de pointe et la puissance de calcul sont essentielles pour les innovations en matière d'IA. Le plan d'action prévoit donc la création de fabriques d'IA et de giga-fabriques d'IA qui permettront de fournir la puissance de calcul et les ressources nécessaires pour développer, affiner, tester et renforcer la capacité d'inférence des modèles d'IA. Ces installations intégreront des supercalculateurs, des ressources de données et des installations de programmation et d'entraînement dans le but de créer un écosystème dynamique pour l'innovation en matière d'IA.

Ce sont ainsi treize fabriques d'IA qui seront établies dans douze États membres et pleinement opérationnelles pour fin 2025. Neuf supercalculateurs seront également déployés dans l'ensemble de l'Union en 2025/2026.

[23] Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* du 12 juillet 2024.

[24] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Plan d'action pour un continent de l'IA, *COM(2025)* 165 final.

[25] *The Draghi report: a competitiveness strategy for Europe*, September 2024.

[26] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Une boussole pour la compétitivité de l'UE, *COM(2025)* 30 final.

La Commission prévoit d'établir jusqu'à cinq giga-fabriques d'IA. Il s'agit d'installations à grande échelle qui développent et entraînent des modèles d'IA complexes à une échelle sans précédent, avec des billions de paramètres. La mise en place de ces giga-fabriques supposent des investissements importants, c'est pourquoi elles seront mises en œuvre au moyen de partenariats public-privé et de « mécanismes de financement innovants ». Vingt milliards d'euros d'investissements sont envisagés.

Dans ce premier pilier, la Commission évoque également le renforcement des capacités de l'Union en matière d'informatique en nuage et de centres de données. Elle entend faire passer l'infrastructure cloud de l'Union au niveau supérieur et la rendre plus puissante et indépendante. La Commission reconnaît son retard par rapport aux États-Unis et à la Chine en ce qui concerne les capacités des centres de données. L'Union s'est fortement appuyée sur des infrastructures installées et contrôlées par d'autres régions du monde. Or, « une dépendance excessive à l'égard d'infrastructures de pays tiers peut entraîner des risques pour la sécurité économique et constitue une préoccupation pour l'industrie européenne »[27]. La Commission souhaite pousser le secteur privé des entreprises de l'Union à développer leurs propres capacités informatiques puissantes et indépendantes au sein de l'Union. Cela sera encouragé par un nouveau règlement sur le développement de l'informatique en nuage et de l'IA dont la proposition est attendue pour fin 2025, début 2026.

II. DONNÉES POUR RENFORCER LES CAPACITES DE L'IA

Parallèlement à l'amélioration et au renforcement prévus de l'infrastructure numérique physique dans l'Union européenne, la Commission européenne souhaite améliorer la disponibilité des données et leur interopérabilité dans tous les secteurs. Dans ce contexte, des laboratoires de données seront créés dans le cadre de l'initiative sur les fabriques d'IA. Ils organiseront et géreront des données provenant de différentes sources, garantissant aux développeurs d'IA l'accès à des ensembles de données fiables et diversifiés dans les secteurs de la santé, de l'énergie ou autres. L'un des éléments clés de l'initiative est l'introduction d'un logiciel de cloud partagé appelé *Simpl* visant à simplifier la gestion et la connexion des espaces de données.

III. PROMOTION DE L'IA DANS LES SECTEURS STRATEGIQUES

La Commission européenne rappelle que l'adoption de l'IA favorise l'innovation, ce qui, par conséquent, est essentiel si l'Union entend renforcer sa compétitivité et sa croissance économique. Pour parvenir à cela, la stratégie pour l'application de l'IA se concentre sur certains secteurs industriels dans lesquels l'Union joue un rôle de premier plan. Outre un certain nombre de secteurs comme l'aérospatial, la sécurité et la défense, ou l'agroalimentaire, cela comprend, dans le domaine de la santé, les produits pharmaceutiques et les biotechnologies. Au-delà, le secteur public apparaît aussi, pour la Commission, comme un moteur stratégique pour l'application de l'IA dans des domaines tels que les soins de santé.

Dans le but de promouvoir les activités de transformation numérique, la Commission soutient l'idée de mettre en place des pôles européens d'innovation numérique dans tous les États membres et dans dix autres pays européens, couvrant ainsi 85% des régions européennes.

Le réseau de pôles européens d'innovation numérique fonctionnera en synergie avec l'écosystème des fabriques d'IA. Son rôle sera, entre autres, de faciliter l'accès des entreprises aux ressources de calcul et aux

[27] Plan d'action pour un continent de l'IA, p. 12.

ressources de données des fabriques d'IA. D'autres initiatives en matière d'IA sont envisagées comme les bacs à sable réglementaires et les installations de test et d'expérimentation.

L'investissement massif dans la recherche fondamentale est ce qui permettra, selon la Commission, de compléter et renforcer les initiatives envisagées.

IV. COMPETENCES ET TALENTS DE L'IA

La Commission est convaincue que la plus grande force de l'Europe reste sa population bien formée et qualifiée. Dans la mesure où l'IA est susceptible d'affecter tous les secteurs d'activités professionnelles, elle doit devenir un élément clé de l'éducation afin d'améliorer le « réservoir » de spécialistes de l'IA, de retenir les talents de l'IA dans l'Union et d'attirer ceux issus de pays tiers. Cela devrait se refléter dans les programmes éducatifs tant en IA que dans le domaine des technologies clés en général. A cet égard, est envisagé le lancement de l'académie des compétences en matière d'IA, guichet unique fournissant un enseignement et une formation sur les compétences liées au développement et au déploiement de l'IA, notamment l'IA générative.

Par l'intermédiaire de l'académie, la Commission indique qu'elle pilotera un programme d'apprentissage dans le domaine de l'IA dans l'objectif de préparer une réserve de spécialistes de l'IA formés à des projets réels et prêts à intégrer ou réintégrer le marché du travail de l'Union.

Couplé aux fabriques d'IA, c'est ainsi tout un environnement dynamique qui sera créé pour les chercheurs de haut niveau encourageant l'innovation et la collaboration dans le développement et le déploiement de solutions d'IA pour des secteurs stratégiques.

V. RESPECT ET SIMPLIFICATION DE LA RÈGLEMENTATION

Un cadre réglementaire solide est primordial pour créer un environnement propice à l'innovation en matière d'IA. C'est en ce sens que l'AI Act a été adopté. Pour la Commission, *« le succès du règlement sur l'IA dépendra avant tout du bon fonctionnement de ses règles dans la pratique »*[28]. Cet objectif de réussite pourra être atteint par une combinaison de plusieurs mesures.

Dans un premier temps, la Commission prévoit le lancement du service d'assistance dans le cadre du règlement IA qui sera intégré au Bureau de l'IA mis en place par l'AI Act. Ce service d'assistance servira de centre d'information central pour les mesures liées à la législation sur l'IA, où les fournisseurs et déployeurs de solutions d'IA pourront demander de l'aide et trouver des réponses sur mesure.

Dans un second temps, la Commission recensera les mesures supplémentaires nécessaires pour faciliter l'application *« harmonieuse, rationalisée et simple du règlement sur l'IA »*[29]. Cela passera par l'analyse des résultats de la consultation des parties prenantes sir la stratégie pour l'application de l'IA lancée en même temps que la présente communication. La rationalisation et la simplification de la réglementation découleront de modèles, orientations, webinaires et formations.

Ce plan d'action pour un continent de l'IA représente une étape ambitieuse vers le positionnement de l'Union en tant que *leader* mondial de l'IA. Les possibilités de financement offertes aux entreprises sont non négligeables et devraient leur permettre de s'impliquer encore davantage dans le développement et le déploiement de l'IA.
L'approche de l'Union européenne crée un environnement unique au monde pour le développement de l'IA. Même si les exigences de conformité et le cumul des réglementations peuvent sembler lourds, de prime abord, elles favorisent, sans nul

[28] Plan d'action pour un continent de l'IA, p. 26.

[29] Plan d'action pour un continent de l'IA, p. 27.

doute, un cadre stable et prévisible pour les investissements à long terme dans les capacités de l'IA.

Les entreprises doivent s'engager dans ces initiatives, évaluer les exigences de conformité et affirmer leur positionnement pour tirer parti des multiples ressources mobilisées au sein de l'Union européenne. Et comme conclut la Commission, *« l'Europe a aujourd'hui une occasion unique d'agir rapidement en vue de façonner l'avenir de l'IA et de créer un avenir meilleur pour tous les Européens, pour devenir en définitive un continent de premier plan dans le domaine de l'IA »*[30].

Communication de la Commission du 4 février 2025 – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), *C(2025)* 884 final

Annexe de la communication de la Commission du 4 février 2025 – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), *C(2025)* 884 final

[30] Plan d'action pour un continent de l'IA, p. 29.

EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, 9 September 2024

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH, Université Toulouse Capitole & CERPOP, Université de Toulouse, UMR 1295 Inserm, équipe BIOETHICS

Le 20 janvier 2025, l'Agence européenne du médicament (EMA) a publié un document conceptuel (*concept paper*) sur l'élaboration d'une ligne directrice relative à l'évaluation et à la communication des résultats des modèles mécanistiques utilisés dans le cadre du développement de médicaments fondé sur des modèles. Plus précisément, ce document a été élaboré en collaboration entre le comité des médicaments à usage humain (CHMP) de l'EMA et son groupe de travail sur la méthodologie (MWP)[31].

Ce travail s'inscrit dans une volonté européenne d'accompagner le déploiement du numérique, de l'intelligence artificielle et des méthodes innovantes pour le développement de médicaments. Ainsi, dans une logique de transparence et de proximité avec les diverses parties prenantes, un appel à consultation publique a été ouvert le 14 février dernier, jusqu'au 31 mai 2025. Plus précisément, avec ce travail préliminaire, l'EMA revient sur les prémices d'accompagnement des acteurs dans le domaine du développement de médicaments fondé sur des modèles (*model informed drug development)*, initiées en 2018 mais qui n'avaient pas atteint le succès escompté[32].

Ce court document de quatre pages, est ainsi orienté sur l'appréhension des « modèles mécanistiques, c'est-à-dire les modèles mathématiques ou informatiques qui intègrent les processus biopharmaceutiques, physico-mécaniques, (patho)physiologiques et pharmacologiques, ainsi que les caractéristiques de la population »[33] qui sont de plus en plus utilisés dans toutes les phases du cycle de recherche et de développement des médicaments. Précisant la faiblesse de l'encadrement et l'accompagnement relatifs au déploiement de ces méthodes, les points d'attention essentiellement identifiés résident dans la possibilité pour les régulateurs d'anticiper et de prévenir les risques propres à ces méthodes afin d'être en mesure de soutenir leurs usages. Dès lors, le point de discussion, tel qu'il est actuellement rédigé, apparaît quelque peu concis mais devrait être approfondi au regard des commentaires qui seront adressés à ses rédacteurs à l'issue de la consultation publique. De plus, il est précisé dans le document qu'une complétion du groupe de rédaction principal sera mise en œuvre via la composition d'une équipe de rédaction de 4 à 6 personnes, dont des experts cliniques[34]. Un groupe plus large, de

[31] EMA/CHMP, "Revised consolidated 3-year work plan for the Methodology Working Party (MWP)", 15 January 2024, EMA/CHMP/478317/2023.

[32] EMA/CHMP, "Guideline on the reporting of physiologically based pharmacokinetic (PBPK) modelling and simulation", 13 December 2028, EMA/CHMP/458101/2016.

[33] EMA, "Concept paper on the development of a Guideline on assessment and reporting of mechanistic models used in the context of model informed drug development", 20 January 2025, EMA/5875/2025, p.1 [notre traduction].

[34] EMA, "Concept paper on the development of a Guideline on assessment and reporting of mechanistic models used in the context of model informed drug development", *op. cit.,* p.3.

93 contributeurs, se réunissant tous les deux mois, sera également réuni pour la discussion et la révision finale du document[35]. Enfin, courant 2025, l'EMA prévoit l'organisation d'un atelier public sur cette thématique, accompagné par un webinaire à destination des parties prenantes engagées[36].

L'objectif final de ce document est clairement mentionné : la rédaction de lignes directrices sur l'évaluation et la communication des résultats des modèles mécanistiques utilisés dans le cadre du développement de médicaments fondé sur des modèles[37]. Espérons que, cette fois-ci, l'EMA parvienne à fournir des documents suffisamment adaptés aux attentions des parties prenantes tout en assurant un respect élevé des règles et principes de l'Union européenne en la matière, afin d'assurer un haut niveau de protection, sans pour autant freiner l'innovation.

EMA, Concept paper on the development of a Guideline on assessment and reporting of mechanistic models used in the context of model informed drug development, 20 January 2025

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH, Université Toulouse Capitole & CERPOP, Université de Toulouse, UMR 1295 Inserm, équipe BIOETHICS

Le 9 septembre dernier, l'Agence européenne du médicament (EMA) a rendu publique la version finale de son document de réflexion sur l'usage de l'Intelligence Artificielle (IA) dans le cycle de vie des médicaments. Pour rappel, ce document, dont la version initiale (draft) avait été publiée en juillet 2023, a été développé en liaison entre le comité des médicaments à usage humain (CHMP)[38] de l'EMA et son comité des médicaments vétérinaires (CVMP), s'inscrivant dans les initiatives conjointes du groupe de pilotage *Big Data* (BDSG) HMA-EMA qui vise à développer la capacité du réseau européen de réglementation des médicaments en matière de réglementation basée sur les données[39].

Cette version consolidée a été retravaillée grâce aux commentaires reçus lors de l'ouverture à consultation publique de juillet 2023 à décembre 2023, relevant alors d'une réelle volonté d'ouvrir un dialogue avec les développeurs des systèmes algorithmiques, les universitaires et l'ensemble des régulateurs[40]. De plus, deux ateliers de réflexions ont été organisés en novembre 2023 afin de préciser les enjeux en la matière.

Le point essentiel de ce document de réflexion réside dans l'identification des utilisations qui peuvent être faites de l'IA tout au long du cycle de vie du médicament, mais également des opportunités et risques qui en découlent[41]. Nous avions d'ores et déjà explicité le fond et les enjeux du document dans le précédent bulletin[42].

[35] *Ibid.*
[36] *Ibid.*
[37] *Ibid.*
[38] Site officiel de l'Agence Européenne du Médicament, [Disponible ici], (Consulté le 05/06/2024).
[39] HMA-EMA, Big Data Steering Group, "Big Data Workplan 2022-2023", Adopted in July 2022, 9p.
[40] Site officiel de l'Agence Européenne du Médicament, « Reflection paper on the use of artificial intelligence in the lifecycle of medicines », News, 19 July 2023, [Disponible ici], (Consulté le 05/06/2024).
[41] *Ibid.*
[42] Noémie dubruel, « EMA, Reflection paper on the use of the Artificial Intelligence (AI) in medicinal

Certaines modifications et précisions réalisée entre la version initiale et celle consolidée méritent notre attention. Tout d'abord, l'introduction du document a été considérablement remaniée afin de mieux cibler les enjeux de l'usage de l'IA dans le cycle de vie des médicaments et, notamment, de cibler davantage les risques qui peuvent exister[43]. De même, l'orientation du document a été modifié pour tenir davantage compte du champ de compétences de l'EMA, considération qui pouvait être reprochée au document initial[44].

De plus, l'EMA est venue préciser ce qu'elle entend par intelligence artificielle et a choisi pour cela de se reporter à la définition donnée par l'OCDE : « un système d'IA est un système mécanique conçu pour fonctionner avec différents niveaux d'autonomie et pouvant faire preuve d'adaptabilité après son déploiement.

À des fins explicites ou implicites, il déduit, à partir des données qui lui sont fournies, comment générer des résultats tels que des prévisions, du contenu, des recommandations ou des décisions



susceptibles d'influencer un environnement physique ou virtuel »[45], précisant alors que ce sont ces innovations qui sont concernées par ce document de réflexion.

En outre, les points « protection des données » et « aspects liés à l'intégrité des données »[46] ont été fusionnés afin d'apporter une réflexion large et complète relative à l'ensemble des préoccupations liées à la collecte et à l'usage des données. Considérant cela, de nouvelles réflexions ont été soulevées concernant les ensembles de données tests ainsi que des données de formations[47].

Le point sur le déploiement du modèle a été considérablement modifié en tenant compte de la perspective d'une évaluation par le risque. En ce sens, l'EMA précise désormais la nécessité de qualifier l'utilisation d'une méthode pour un contexte d'utilisation identifié en fonction des risques pour les personnes ou de « l'impact réglementaire élevé »[48]. En ce sens, il a également été ajouté des mentions quant à l'importance de réaliser une analyse d'impact dès les débuts du recours à l'IA dans le cycle de vie des médicaments ainsi que d'intégrer une analyse juridique et éthique *by design* (notamment relative à la protection de la vie privée).

Une autre modification importante réside dans la précision des destinataires du document : le promoteur et le fabricant, en plus du demandeur et du titulaire de l'autorisation de mise sur le marché, sont concernés par l'usage de l'IA. Cet ajout insiste sur la particularité des possibles usages de l'IA à chaque étape du cycle de vie et de développement d'un médicament et sur les inévitables collaborations que cela entraîne.

Ce document marque ainsi la forte volonté de l'EMA d'accompagner le déploiement d'innovation dans le domaine

product lifecycle, 13 July 2023 », *in* Nathalie De Grove-Valdeyron (dir) et Claire Bories (coord.), « Bulletin de l'EDiHL », n°1, Juin 2023 – Juin 2024, p.19. Accessible ici.

[43] EMA/CHMP/CVMP, "Reflection paper on the use of the Artificial Intelligence (AI) in medicinal product lifecycle", 9 September 2024, EMA/CHMP/CVMP/83833/2023, p. 3.

[44] *Ibid.*

[45] *Ibid.*

[46] EMA/CHMP/CVMP, "Reflection paper on the use of the Artificial Intelligence (AI) in medicinal product lifecycle", *op. cit.,* pp.08-11.

[47] *op. cit.,* p. 9.

[48] *op. cit.*, p. 5.

du médicament. Bien entendu, ce document de réflexion doit être interprété en accord avec les exigences nationales ainsi que les principes généraux de l'Union européenne et aux récentes adoptions réglementaires (telles que l'IA Act par exemple). De plus, les acteurs concernés doivent se saisir de l'ensemble de ces réflexions afin de se positionner sur des approches collaboratives et respectant les principes éthiques et l'intégrité réglementaire en vigueur. C'est notamment ce qu'a souhaité faire l'European Federation of Pharmaceutical Industries and Associations (EFPIA) en publiant en octobre 2024 un document de positionnement en réponse au document de réflexion de l'EMA[49]. Reste à voir quelles seront les prochaines orientations qui seront prises pour accompagner au mieux cette révolution numérique

[49] EFPIA, "EFPIA position on the use of artificial intelligence in the medicinal product lifecycle, October 2024", 9p.

Note conjointe sous HMA-EMA, *Big Data Steering Group (BDSG), 2024 report*, EMA/471579/2024, 13 December 2024 ; HMA-EMA, *Joint HMA-EMA Network Data Steering Group*, EMA/419729/2024, 3 October 2024 et ; HMA-EMA, *Seizing opportunities in a changing medicines landscape - The European medicines agencies network strategy 2028*, 18 March 2025

par Valentine DURAND

Doctorante en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole

Fin 2024, le groupe de pilotage conjoint HMA[50]-EMA[51] sur les données massives, le 'Big Data Steering Group' (BDSG)[52] laisse place au groupe de pilotage conjoint HMA-EMA sur les données du réseau, le 'Network Data Steering Group' (NDSG[53]).

Le BDSG a poursuivi l'application de son plan d'action[54] inscrit dans la Stratégie du Réseau des agences européennes des médicaments (ci-après le Réseau) pour 2025[55]. Dans son rapport 2024, il présente son bilan et les évolutions à venir, qui seront désormais dirigées par le NDSG.

I. EN 2024, LE BDSG POSE LE BILAN

Le BDSG fait son rapport annuel et souligne le progrès vers une réglementation davantage axée sur les données[56]. Il présente les avancées marquantes de son année 2024. Comme pour son rapport 2023, les onze initiatives semblent toutes en bonne voie.

Pour reprendre une présentation similaire à la note[57] de l'année précédente, elles seront présentées ici en cinq catégories : les initiatives portant sur les données et leurs caractéristiques (**1**), les initiatives portant sur le réseau réglementaire, ses capacités et son cadre de gouvernance (**2**), les initiatives portant sur la collaboration avec les parties prenantes (**3**), les initiatives vétérinaires (**4**) et enfin, dans une nouvelle catégorie, l'avancée du plan d'action sur l'intelligence artificielle (ci-après IA) (**5**).

[50] Le réseau des Chefs des agences du médicament (Heads of Medecines Agencies, HMA) est le réseau des directeurs des agences nationales, compétentes en matière de réglementation des médicaments et des produits de santé à usage humain et vétérinaire au sein de l'espace économique européen.

[51] L'Agence européenne des médicaments (EMA) est une agence décentralisée de l'Union européenne (UE) chargée de l'évaluation scientifique, de la supervision et du contrôle de la sécurité des médicaments dans l'UE.

[52] EMA, Mandat du groupe de pilotage conjoint HMA-EMA sur les données massives (Joint HMA-EMA Big Data Steering Group), EMA/96120/2023, 12 juin 2023 [disponible en ligne ici]

[53] EMA, Mandat du groupe de pilotage conjoint HMA-EMA sur les données du réseau (Joint HMA-EMA Network Data Steering Group), EMA/419729/2024, 3 octobre 2024 [disponible en ligne ici].

[54] HMA/EMA Joint Big Data Steering Group, Plan de travail sur les données massives 2023-2025, version 1.4, juin 2024 [disponible ici].

[55] EMA, European medicines agencies network strategy to 2025, EMA/85501/2020, 2020. [disponible en ligne ici].

[56]Conformément à la stratégie du réseau à l'horizon 2025, au plan de travail BDSG et au plan de travail pluriannuel sur l'IA.

[57] Valentine Durand, Note sous EMA, Big Data Steering Group (BDSG):2023 Report,18 January2024et Multi-annual AI workplan 2023-2028. HMA-EMA Big Data Steering Group, November 2023, *Bulletin de l'EDiHL*, *European Digital Health Law*, N°1, Juin 2023 – Juin 2024.

1. S'agissant des initiatives sur les données et leurs caractéristiques

Le projet DARWIN EU prend de l'ampleur et aspire à augmenter son nombre de partenaires de données à 40, contre 20 actuellement, pour pouvoir mener jusqu'à 100 recherches par an à compter de 2025. En parallèle, sa gouvernance et son fonctionnement se clarifie.

S'agissant de la qualité et de la représentativité des données, le chapitre portant sur l'application, aux données de vie réelle, du cadre de qualité des données pour la réglementation européenne sur les médicaments a été publié fin 2024. Le prochain chapitre portera sur les données relatives aux réactions indésirables aux médicaments. Dans le même domaine d'expertise, le BDSG a collaboré avec le projet QUANTUM pour MaSanté@EU qui vise à élaborer un label de qualité et d'utilité des données pour préparer l'Espace européen des données de santé.

Pour l'accessibilité des données, le BDSG partage l'avancée des catalogues HMA-EMA de sources de données et d'études de vie réelle[58] et les discussions sur la potentielle utilité de nouvelles sources de données comme l'expérience des patients, la santé mobile et les médias sociaux.

2. S'agissant des initiatives portant sur le réseau, ses capacités et son cadre de gouvernance

Le Réseau continue à se former sur les sujets numériques (IA, données massives, données de vie réelle, etc.). Les curricula portant sur les données massives s'étoffent de deux nouveaux modules, un sur les protocoles d'étude et les rapports et un sur les méthodes statistiques appliquées aux données de vie réelle. L'instauration d'un forum de discussions et d'échanges, « l'Académie de Vie Réelle », permet aux experts d'échanger sur le sujet. Un curriculum de science de la donnée a également été développé et cinq modules ont vu le jour en 2024, accompagnés par la création d'une Académie numérique, « Digital Academy ».

S'agissant des procédures du Réseau, le focus 2024 a été sur l'utilisation des données de vie réelle et sur les cas d'usage des données relatives à l'expérience patient et des données génomiques. Le travail méthodologique sur l'utilisation par le Réseau des données de vie réelle est bien avancé et plusieurs délivrables ont été publiés en 2024. Le travail sur les données d'expérience patient semble au même point que celui sur les données de vie réelle un an auparavant, ce qui laisse espérer une avancée rapide.

Fin 2024, le premier projet de Stratégie pour les données du Réseau[59] a été publié. Les principaux objectifs de la stratégie portent sur la gouvernance, l'analyse, la qualité, l'interopérabilité, le catalogage des données et la gestion des métadonnées, et enfin, la gestion des connaissances et du changement. Pour suivre cette stratégie, les deux organes de gouvernance des données du Réseau, le Big Data Steering Group et le Network Data Board, fusionnent pour créer le Network Data Steering Group. Le champ de données couvert par le NDSG est précisé.

Sur la capacité du réseau à analyser les données massives, trois thématiques sont abordées. D'abord, le pilote sur les données d'essais cliniques (anciennement pilote sur les données brutes, ou « raw data »), aux premiers résultats prometteurs, a été étendu. Ensuite, la norme « SEND », sur l'échange de données non-cliniques brutes a été utilisée pour une première demande d'autorisation de mise sur le marché en

[58] Le terme donné de vie réelle est « un terme générique désignant les données relatives aux effets des interventions de santé qui ne sont pas collectées dans le cadre d'essais cliniques randomisés hautement contrôlés » - Horizon Europe, Work Programme 2021-2022, 4. Health (European Commission Decision C(2022)2975 of 10 May 2022) Part 4, page 145 (Disponible ici). Les preuves de vie réelle sont les preuves basées sur ces données.

[59] EMA, The European Medicines Agencies Network Data Strategy (draft), EMA/458778/2024, 6 septembre 2024.

septembre 2024. Enfin, une enquête, menée auprès des acteurs du Réseau, sur les données utilisées pour la prise de décision réglementaire et les capacités informatiques techniques, permettra d'étayer les futurs axes de travail du NDSG et une éventuelle stratégie du Réseau en matière d'analyse de données.

3. S'agissant des initiatives portant sur la collaboration avec les parties prenantes

Le BDSG fait le bilan d'une année riche d'initiatives internationales et de mobilisation des parties prenantes.

S'agissant des initiatives internationales, parmi d'autres sujets, la coopération autour des données de vie réelle et les données patient se renforce et plusieurs documents de réflexion ont été publiés par le Conseil international d'harmonisation des exigences techniques pour l'enregistrement des médicaments à usage humain. Certaines agences, comme Health Canada, la FDA[60] et l'EMA, ont appelé à une collaboration internationale renforcée sur le sujet.

Pour mobiliser les parties prenantes, le BDSG a participé à pas moins de six ateliers sur des sujets variés (analyse des essais cliniques, registres patient, qualité des données, méthodologies portant sur les données de vie réelle, etc.) et à plusieurs forums et rendez-vous avec diverses parties prenantes. Pour informer les différents acteurs, la newsletter trimestrielle sur les données massives de l'EMA a continué à être publiée en 2024. Une évaluation de la communication du BDSG a été lancée et un plan de mise en œuvre des activités de gestion du changement, a été publié en juillet 2024. Ce plan vise à faciliter la transition vers une réglementation des médicaments davantage axée sur les données.

4. Sur les initiatives vétérinaires

La mise en œuvre de la Stratégie[61] vétérinaire avance à grands pas. Le BDSG souligne des avancées en matière de cadre de qualité des données, de formations et d'analyse du paysage vétérinaire en matière de données et notamment sur l'identification des sources de données de vie réelle.

5. Sur l'avancée du plan d'action sur l'IA

Les progrès du plan IA sont présentés en quatre axes : (1) les orientations, politiques et soutien aux produits, (2) les outils et technologies, (3) la collaboration et la gestion du changement et (4) l'expérimentation.

Sur le premier axe, plusieurs délivrables significatifs ont été publiés en 2024. C'est le cas des Lignes directrices sur l'utilisation des grands modèles de langage (LLM en anglais) dans la science réglementaire et pour les activités de réglementation des médicaments[62] et du document de réflexion sur l'utilisation de l'intelligence artificielle (IA) dans le cycle de vie des médicaments[63]. Un travail préparatoire à l'entrée en application du Règlement sur l'intelligence artificielle[64] est également en cours, avec la création d'un Observatoire de l'IA.

Deuxièmement, s'agissant des outils et de la technologie, le BDSG a soutenu des initiatives nationales. Plusieurs projets ont abouti, comme le service AI@MPA, une initiative de l'agence suédoise du médicament, au profit de tout le Réseau, qui

[60] Food and Drug Administration, agence étatsunienne du médicament

[61] EMA, Veterinary Medicines Division, European Veterinary Big Data strategy 2022- 2027, EMA/648865/2021, 30 juin 2022

[62] EMA, Guiding principles on the use of large language models in regulatory science and for medicines regulatory activities, 29 août 2024.

[63] EMA, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, EMA/CHMP/CVMP/83833/2023, 9 septembre 2024.

[64] Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle), JOUE n° L 2024/1689 du 12 juillet 2024.

utilise l'intelligence artificielle pour identifier, parmi les publications de l'EMA, les documents pertinents. Est aussi citée l'IA de recherche réglementaire scientifique basée sur les ressources du Réseau, nommée « Scientific Explorer », lancée en mars 2024. Le Réseau compte s'appuyer sur les initiatives nationales afin de définir les outils pertinents et des enquêtes sont menées afin de trouver des cas d'usage.

Troisièmement, au sujet de la collaboration et de la conduite du changement, un groupe de travail sur l'IA, auquel l'EMA est partie, a été mis en place au niveau de la Coalition internationale des autorités de réglementation des médicaments (ICMRA). L'EMA se forme à l'IA et aux sciences des données, tout en mettant en place un groupe d'experts sur l'IA (et sujets annexes comme les sciences des données, les biostatistiques, les données de vie réelle etc.) au sein du groupe de travail méthodologique (MWP). Un atelier[65] rassemblant de multiples parties prenantes a eu lieu fin 2024, au sujet de l'utilisation sûre et responsable de l'IA. Cet atelier devrait aboutir à la révision du programme de travail pluriannuel sur l'IA, et à la rédaction d'une feuille de route sur les priorités du Réseau en matière de recherche.

Enfin, sur l'expérimentation, l'atelier permettra également d'identifier les expérimentations à mener. En 2024, les sujets explorés en profondeur ont été l'explicabilité et la transparence.

Ce bilan 2024 est très riche, tant par le nombre d'initiatives que par la quantité de délivrables. Ces sujets seront repris par la suite par le groupe de pilotage conjoint HMA-EMA sur les données du réseau, le 'Network Data Steering Group' (NDSG).

II. PLACE AU NDSG, SUCCESSEUR AU CHAMP D'ACTIVITES ELARGI

Le mandat du Network Data Steering Group est très similaire à celui de son prédécesseur le BDSG. Il se concentre sur l'interopérabilité, l'échange et l'utilisation des données au sein du Réseau HMA-EMA. Elément à noter : ce mandat définit deux catégories de données, sur lequel le groupe mettra un accent particulier. D'une part, les données réglementaires[66], qualifiées comme telle par leur inclusion dans une procédure administrative, et d'autre part, les données à l'appui des preuves relatives aux médicaments[67], catégorie beaucoup plus large de données qui comprennent les données réglementaires.

Ses missions sont stratégiques et diverses, centrées sur la mise en place de stratégies portant sur les données, l'interopérabilité et l'intelligence artificielle. Il se penchera sur la gestion des données du Réseau et de sa capacité d'analyse. Ses tâches comprennent également de la veille technologique, la collaboration internationale et le suivi des évolutions des besoins en matière

[65] EMA, HMA/EMA Multi–stakeholder workshop on Artificial Intelligence (AI) - enabling the safe and responsible use of AI, Workshop Report, 15 janvier 2025

[66] [Traduction non-officielle] Données réglementaires : données soumises, créées ou contrôlées dans le cadre de procédures réglementaires tout au long du cycle de vie des médicaments humains et vétérinaires. Cela inclut les données de base essentielles pour les opérations interopérables du réseau et la surveillance des pénuries et de la sécurité des produits, les soumissions réglementaires et les données relatives aux procédures.

[67] [Traduction non-officielle] Données à l'appui des preuves relatives aux médicaments : données utilisées pour produire des preuves sur l'utilisation, la sécurité, la qualité ou l'efficacité des médicaments. Cela inclut les données brutes des essais cliniques, les données regroupées des essais cliniques, les données réelles telles que celles des dossiers médicaux électroniques, des registres et des demandes d'indemnisation, les ensembles de données concernant les effets indésirables suspectés des médicaments signalés spontanément et les ensembles de données génomiques, protéomiques et métabolomiques. Il peut également s'agir de données non cliniques, de données relatives à la chimie, à la fabrication et aux contrôles (CMC), ainsi que de données relatives à l'approvisionnement.

d'infrastructures numériques et de compétences internes du Réseau.

Le NDSG rassemble, comme le BDSG avant lui, un large éventail de parties prenantes, notamment des représentants des Etats membres, des payeurs, de la Commission, de l'EMA et de ses comités, ainsi que de certaines initiatives comme ACT EU, des parties prenantes à l'Espace européen des données de santé ou du Réseau européen d'innovation. Des rencontres ad hoc avec des experts ou autres parties prenantes comme les universitaires ou l'industrie seront également organisées au besoin.

III. STRATEGIE DU RESEAU EUROPEEN DES AGENCES DU MEDICAMENT POUR 2028

La stratégie du Réseau des agences du médicaments évolue. Après avoir « [protégé] la santé publique à une époque de changements rapides », titre de la stratégie pour 2025[68], le Réseau souhaite désormais, pour 2028, « Saisir les opportunités dans un paysage pharmaceutique en mutation »[69].

Pour ce faire, le Réseau présente six objectifs portant sur l'accessibilité (1), l'exploitation des données, la numérisation et l'intelligence artificielle (2), la science réglementaire, l'innovation et la compétitivité (3), la résistance antimicrobienne et les autres menaces pour la santé (4), la disponibilité et l'approvisionnement (5) et la durabilité du réseau (6).

Ces objectifs sont alignés avec la Stratégie pharmaceutique pour l'Europe[70] et avec le projet de réforme de la législation pharmaceutique européenne[71].

1. L'accessibilité

Au sujet de l'accessibilité, le focus est fait sur la génération de preuves. Pour permettre de réduire les délais entre l'obtention de l'AMM et la mise effective sur le marché en quantité suffisante, il faut que la négociation de prix et remboursement se fasse rapidement. Or, si, d'une part, le développement du médicament permet la génération de preuves pour les deux évaluations et que, d'autre part, ces évaluations prennent en compte des éléments similaires, le délai serait réduit. Pour cela, le réseau compte contribuer à faciliter la mise en œuvre du règlement sur l'évaluation des technologies de santé[72], permettre la communication entre les différents décisionnaires et engager des recherches pour mieux comprendre les problématiques liées à l'accès ainsi que les points de vue des parties prenantes.

2. Exploiter les données, la numérisation et l'intelligence artificielle

Plusieurs axes de travail sont présentés dans le pilier exploitation des données, numérisation et IA.

Tout d'abord, le Réseau ambitionne de travailler sur l'harmonisation des données de base (master data). Plusieurs initiatives portent sur la gestion des données, avec un accent sur les aspects techniques (interopérabilité, normalisation, qualité, gestion des biais, etc.).

Ensuite, le Réseau souhaite maximiser l'utilisation des données et la production de preuves pour soutenir la prise de décision, notamment grâce au projet DARWIN EU et à la mise en place de l'Espace européen des

[68] EMA, European medicines agencies network strategy to 2025, EMA/85501/2020, 2020. [disponible en ligne ici]

[69] HMA-EMA, Seizing opportunities in a changing medicines landscape - The European medicines agencies network strategy 2028, 18 mars 2025 [disponible en ligne ici]

[70] Communication de la Commission européenne du 22 novembre 2022 « La stratégie pharmaceutique pour l'Europe », *COM(2020)* 761 final.

[71] Communication de la Commission européenne du 26 avril 2023 « Réforme de la législation pharmaceutique et mesures de lutte contre la résistance aux antimicrobiens », *COM(2023)* 190 final,.

[72] Règlement n° 2021/2282/UE du Parlement européen et du Conseil du 15 décembre 2021 concernant l'évaluation des technologies de la santé, *JOUE* n° L 458 du 22/12/2021.

données de santé. Pour ce faire, les potentielles utilisations des données seront étudiées, y compris des données de natures nouvelles comme les données synthétiques ou les données relatives à l'expérience des patients. La Stratégie précise ce qui va sans dire : "alors que le réseau progresse dans son utilisation et sa génération de données, il est également important de souligner que les détenteurs d'autorisations de mise sur le marché et les demandeurs restent responsables de la génération des données nécessaires pour soutenir ou justifier leurs demandes."

Enfin, pour ne pas manquer la transition vers l'IA et les nouveaux outils numériques, le Réseau souhaite mettre en place une culture de l'expérimentation tout en assurant la numérisation de son infrastructure et de ses activités. Cette expérimentation des nouvelles technologies, et en particulier de l'IA, par le Réseau, permettra d'en tirer les pleins bénéfices.

Cet objectif est soutenu par le NDSG[73]. A noter que ce pilier peut en soutenir d'autres. Par exemple, la numérisation des informations produit peut rendre les médicaments plus accessibles.

3. Science réglementaire, innovation et compétitivité

Ces aspects sont centraux dans la réforme de la législation pharmaceutique européenne telle que présentée par la Commission européenne en 2023[74], qui semble déjà prise en compte par l'Agence. Ici, la Stratégie présente l'ambition d'un environnement réglementaire favorable à la recherche et à l'innovation. Pour cela, les dialogues avec et entre les parties prenantes sont primordiaux et doivent être facilités. En parallèle, il faut tendre vers la simplification de la recherche et développement, avec des initiatives comme ACT EU[75] et rendre le système d'information sur les essais cliniques plus simple d'utilisation.

S'agissant de la compétitivité, le Réseau ambitionne de soutenir les acteurs de la chaîne de l'innovation, des chercheurs aux financeurs, à travers la mise en place de groupes de travail, de formations et de cadres de collaboration.

Ce pilier fait également une mention étonnante à l'environnement, seule mention de cette stratégie, en précisant que le Réseau doit promouvoir des pratiques durables et conformes au Pacte vert pour l'Europe[76] et au règlement sur l'industrie « zéro net »[77].

4. Résistance antimicrobienne et autres menaces pour la santé

Cet axe est particulièrement urgent et permet de faire une piqure de rappel quant aux différentes initiatives en la matière. S'agissant des antimicrobiens, la crise est gérée en trois parties : rationaliser l'utilisation des antimicrobiens existants, favoriser le développement de nouveaux antimicrobiens et assurer la capacité d'adaptation réglementaire face aux menaces sanitaires.

5. Disponibilité et approvisionnement

Sur la gestion des pénuries, en plus d'en étudier les causes, l'objectif est d'impliquer tous les acteurs, jusqu'au pharmacien d'officine et au patient. Pour cela, le Réseau compte travailler avec les acteurs publics et privés et améliorer la circulation des informations pour éviter la duplication des efforts et les risques de certaines pratiques.

[73] Mandat du NDSG, *op. cit.*, page 1, paragraphe 4
[74] *COM(2023)* 190 final, *op. cit.*
[75] V. ACT EU workplan 2025 – 2026, version 3, décembre 2024 : « L'initiative 'Accelerating Clinical Trials in the European Union' (ACT EU) soutient des essais cliniques plus intelligents par le biais d'innovations réglementaires, technologiques et de processus ».
[76] Communication de la Commission du 11 décembre 2019 portant sur « Le pacte vert pour l'Europe », *COM(2019)* 640 final.
[77] Règlement n° 2024/1735/UE du Parlement européen et du Conseil du 13 juin 2024 relatif à l'établissement d'un cadre de mesures en vue de renforcer l'écosystème européen de la fabrication de produits de technologie « zéro net », *JOUE* n° L 2024/1735 du 28/06/2024.

La Stratégie mentionne également la collaboration avec la Commission dans le cadre du « Critical Medicines Act », qui, bien que non encore adopté, commence à être évoqué.

Le deuxième pan de cette gestion des pénuries porte sur les contrôles. La Stratégie prévoit d'améliorer la capacité du réseau en matière d'inspection en formant les inspecteurs, en établissant une approche par les risques des inspections, en renforçant la surveillance des chaines d'approvisionnement, en adaptant les bonnes pratiques de fabrication à l'évolution des technologies et en améliorant et liant les bases de données sur le sujet.

6. Durabilité du réseau

La gestion des ressources est une question fondamentale pour toute entité. Dans le cas des autorités du médicaments, il s'agit d'assurer le maintien des activités et développer les compétences nécessaires au suivi de leurs évolutions.

Pour développer les capacités du Réseau, est mentionnée la numérisation de ses activités, l'allocation de ressources à la création de centres d'excellence parmi les autorités nationales compétentes ou la préparation de la réforme de la législation pharmaceutique européenne notamment en termes de capacités d'analyses de données et d'infrastructures numériques.

Il s'agit pour le Réseau d'assurer sa montée en compétence sur les nouvelles technologies et les sujets d'actualité, comme la lutte contre la désinformation, tout en embarquant les parties prenantes et en assurant une collaboration internationale notamment au sujet des chaînes d'approvisionnement.

Ainsi, le Réseau se veut facilitateur, collaborateur et chercheur en sciences réglementaires. La transformation numérique et les nouveaux outils comme l'intelligence artificielle tiennent une place importante de la stratégie, en cohérence avec les enjeux actuels. Les ambitions affichées sont alignées avec la proposition de réforme de la législation pharmaceutique générale[78] et soutiennent plusieurs initiatives législatives récentes comme le règlement pour une Europe interopérable[79] ou le règlement sur l'évaluation des technologies de santé[80].

.

[78] *COM(2023)* 190 final, *op. cit.*

[79] Règlement n° 2024/903/UE du Parlement européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union, *JOUE* n° L 2024/903 du 22/03/2024.

[80] Règlement n° 2021/2282/UE du Parlement européen et du Conseil du 15 décembre 2021 concernant l'évaluation des technologies de la santé et modifiant la directive 2011/24/UE, *JOUE* n° L 458 du 22/12/2021.

Note conjointe sous HMA-EMA, *Network Data Steering Group*, EMA/419729/2024, 3 October 2024 et HMA-EMA, *Seizing opportunities in a changing medicines landscape - The European medicines agencies network strategy 2028*, 18 March 2025

par Winnie DONGBOU WAMBA

Doctorant en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole
et Juriste en protection des données de santé My Data-TRUST

La pandémie de COVID-19 a rappelé combien les menaces sanitaires obscurcissent les frontières nationales. L'ampleur de la crise a révélé les limites structurelles de la chaîne du médicament et de la coordination réglementaire en Europe[81]. À la suite de cette crise sanitaire, le législateur européen a renforcé le rôle de l'Agence européenne des médicaments[82]. Cette mutation du paysage pharmaceutique n'est pas uniquement dictée par l'urgence sanitaire. Elle est également marquée par l'essor du numérique, de l'intelligence artificielle (IA), des données massives (*big data*) et de la médecine de précision[83]. C'est dans ce même contexte qu'en octobre 2024, deux documents importants ont été publiés par l'Agence européenne des médicaments (EMA) et le réseau des agences nationales (HMA). Il s'agit, d'une part, du projet de stratégie du réseau des agences européennes du médicament à l'horizon 2028[84], et d'autre part, du mandat du groupe de pilotage conjoint HMA-EMA sur les données[85]. Ces textes dessinent les contours d'un système fondé sur la donnée, l'innovation et la collaboration à la fois transnationale et intersectorielle.

I. LA STRATEGIE EMA-HMA POUR 2028 : UNE AMBITION DECLINEE EN SIX PRIORITES AUTOUR DE LA DONNEE ET DE LA COLLABORATION

Le document *Seizing opportunities in a changing medicines landscape* présente la vision commune de l'Agence européenne des médicaments (EMA) et du réseau des agences nationales (HMA) pour faire évoluer la régulation pharmaceutique d'ici 2028 ('EMANS 2028'). Il s'articule autour de six objectifs stratégiques interconnectés. La stratégie vise à garantir un accès égal et rapide aux traitements pour tous les citoyens européens. Elle cherche à réduire les disparités entre États membres, accélérer les évaluations des médicaments et développer des solutions pour les besoins non satisfaits. L'EMANS 2028 met l'accent sur le réseau EMA-HMA pour renforcer la solidarité réglementaire et améliorer la coordination des politiques d'accès.

Dans la continuité des enseignements de la pandémie de COVID-19, la stratégie vise à améliorer la capacité du réseau à prévenir, détecter et répondre aux menaces sanitaires

[81] Communication de la Commission et du Parlement européen du 25 novembre 2020 sur la stratégie pharmaceutique pour l'Europe, *COM(2020)* 761 final.

[82] V. règlement n° 2022/123/UE 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, *JOUE* n° L 20/1 du 31 janvier 2022, considérants 1-10.

[83] Communiqué de presse IP/24/2523 de la Commission européenne sur une Union européenne de la santé plus solide et mieux préparée pour l'avenir, Bruxelles le 22 mai 2024. Disponible ici.

[84] EMA and HMA, *Seizing opportunities in a changing medicines landscape* (draft), EMA/376542/2024, 3 October 2024.

[85] Joint HMA-EMA *Network Data Steering Group Mandate, EMA/419729/2024*, 3 October 2024.

émergentes. Cela comprend des mécanismes pour maintenir la continuité des chaînes d'approvisionnement, une meilleure surveillance des signaux de pharmacovigilance, et une mobilisation coordonnée en cas de crise. Une priorité est également accordée à la lutte contre la résistance aux antimicrobiens (RAM) par une approche intégrée « *One Health* » qui inclut la santé humaine, animale et environnementale.

La transformation de la régulation en un système fondé sur les données (*data-driven regulation*) est l'un des éléments clés de la stratégie. Cela consiste à utiliser de manière optimale les données provenant des essais cliniques, des données du monde réel (RWD) et des registres de patients grâce à des technologies telles que l'intelligence artificielle et l'analyse prédictive.

L'EMANS 2028 vise à faire de l'Europe un hub attractif pour l'innovation pharmaceutique. Cela inclut l'adaptation des cadres d'évaluation aux nouvelles thérapies et technologies, et le renforcement du soutien aux projets innovants via le *regulatory science hub*. La stratégie s'aligne aussi avec les initiatives européennes de recherche et d'investissement. La pérennité du réseau EMA-HMA a un rôle important à jouer. Pour y arriver, le défi pressenti est la mobilisation des ressources humaines, technologiques et financières adéquates. La stratégie prévoit ainsi des investissements dans la montée en compétences des experts, la mutualisation des infrastructures numériques et l'harmonisation des pratiques entre agences nationales. Elle vise à garantir une prise de décision cohérente, efficace et alignée avec les objectifs de santé publique.

Enfin, la stratégie met également en lumière les défis croissants sur la disponibilité et l'approvisionnement en médicaments. Pour y remédier, l'EMANS 2028 prévoit le développement d'outils de surveillance des pénuries, la diversification des sources d'approvisionnement, et une coopération renforcée avec les industriels pour sécuriser la fabrication et la distribution à l'échelle européenne.

II. LE ROLE CENTRAL DU GROUPE DE PILOTAGE CONJOINT HMA-EMA SUR LES DONNEES

Le groupe de pilotage conjoint HMA-EMA sur les données (ci-après « Le groupe ») a pour objectif de coordonner les initiatives autour de la donnée au sein du réseau EMA-HMA. Il est par conséquent vital pour l'EMANS 2028.

Le document précise surtout les modalités de composition, de nomination et de renouvellement des mandats des membres du groupe de pilotage institué conjointement par l'EMA et le HMA, le groupe de pilotage rassemble un nombre restreint de membres afin de garantir l'efficacité opérationnelle des travaux. Il inclut des représentants issus des autorités nationales compétentes, de l'EMA, ainsi que des experts pertinents dans les domaines stratégiques liés à la donnée, tels que la gouvernance de l'information, la science des données, les technologies numériques et l'intelligence artificielle appliquées à la régulation pharmaceutique. Nous déplorons l'absence d'experts en droits de la protection des données personnelles de santé.

Les membres sont nommés sur la base de leurs expertises techniques et stratégiques pour un mandat de trois ans, avec la possibilité d'un renouvellement unique pour une durée équivalente. Le groupe prévoit une rotation partielle des membres afin d'assurer à la fois continuité institutionnelle et renouvellement des compétences. Des observateurs issus notamment d'autres groupes stratégiques ou techniques du réseau EMA-HMA ou de la Commission européenne peuvent être invités en fonction des sujets traités. Ce cadre organisationnel a pour objectif d'assurer une gouvernance stable, experte et agile, capable de diriger la transformation numérique de la législation pharmaceutique au sein de l'Union européenne

Commission européenne, DG santé, *Frequently Asked Questions on the European Data Health Space*, 5 March 2025

par Winnie DONGBOU WAMBA

Doctorant en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole, et Juriste en protection des données de santé My Data-TRUST

Le document *Frequently Asked Questions on the European Health Data Space* publié par la Commission européenne le 5 mars 2025 constitue une réponse structurée aux nombreuses interrogations soulevées lors des trois webinaires organisés plus tôt la même année[86] dans le cadre des discussions sur le Règlement sur l'espace européen des données de santé (EEDS)[87]. Ces webinaires, destinés aux parties prenantes du secteur de la santé, de la recherche, des autorités nationales et du secteur privé, ont permis de tenir compte des préoccupations concrètes, toutes très diverses, exprimées par les acteurs appelés à appliquer le règlement. Le format FAQ a donc été conçu comme un outil pédagogique pour renforcer la compréhension du texte législatif, tout en illustrant la complexité des changements induits par le règlement.

La majorité des questions abordées dans ce document peut être regroupée autour de trois grands axes thématiques. Premièrement, un nombre significatif d'interrogations porte sur la gouvernance et les responsabilités des différents acteurs, notamment sur le rôle de la Commission, des organismes tels que les organismes responsables de l'accès aux données de santé (ORAD ou *Health Data Access Bodies* – HBABs), des utilisateurs de données (*data users*) et détenteurs de données (*data holders*) et de l'impact sur les patients et autres individus concernés. Ces questions révèlent l'inquiétude des acteurs visés quant à la répartition des obligations juridiques et techniques dans le nouveau système.

Deuxièmement, le document répond aux multiples questions relatives aux données susceptibles d'être rendues disponibles et aux conditions d'accès à ces données pour la réutilisation, que ce soit à des fins de recherche, d'innovation, de politique publique ou de sécurité sanitaire. Les questions portant sur les garanties à apporter et le rôle des environnements de traitement sécurisés traduisent également le besoin d'un encadrement clair et opérationnel des modalités de traitement des données dont l'accès est autorisé par les HDABs.

Troisièmement, un ensemble important de questions concerne la compatibilité du Règlement EEDS avec les autres Règlements européens applicables aux données, à la recherche et à l'intelligence artificielle. Cette dimension reflète la

[86] Il s'agissait des « European Health Data Space (EHDS) Webinar Series » organisés les 18 et 27 février et le 6 mars 2025. Ils portaient respectivement sur les utilisations première et secondaire des données et sur l'implementation, la gouvernance et les responsabilités des différents acteurs. Un replay est disponible ici.

[87] Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement n° 2024/2847, *JOUE* n° L 2025/327 du 5 mars 2025 et le règlement n° 2024/2847/UE du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements n° 168/2013/UE et n° 2019/1020/UE et la directive n° 2020/1828/UE (règlement sur la cyberrésilience), *JOUE* n° L 2024/2847 du 20 novembre 2024.

préoccupation constante des acteurs en ce qui concerne l'interaction et la complémentarité entre les différents textes du paquet législatif européen.

En définitive, ce document illustre les besoins d'interprétation et de clarification autour d'un texte fondateur qui réorganise profondément l'écosystème européen des données de santé. Les questions recensées mettent en évidence non seulement la complexité du Règlement, mais également les attentes fortes en matière de sécurité juridique, de clarté procédurale et de protection des droits des patients et autres individus.

Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement n° 2024/2847/UE, *JOUE* n° L 2025/327 du 5 mars 2025



Vers une opérationnalisation de l'espace européen des données de santé (EEDS). Première analyse des projets de lignes directrices de l'action conjointe TEHDAS2 sur l'accès, l'utilisation et la sécurisation des données

par Winnie DONGBOU WAMBA

Doctorant en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole
et Juriste en protection des données de santé My Data-TRUST

Introduction

La construction d'un Espace européen des données électroniques de santé se précise de plus en plus après l'entrée en vigueur du règlement sur l'EEDS en mars 2025[88]. Dès le mois de janvier, l'action conjointe TEHDAS2 (Towards a European Health Data Space-2) dont l'objectif est d'accompagner la Commission Européenne dans la conception de lignes directrices visant à opérationnaliser l'utilisation secondaire des données de santé, a soumis ses quatre premiers projets de lignes directrices, disponibles uniquement en anglais, à consultation publique[89]. Il s'agit du projet de lignes directrices pour les détenteurs de données sur la description des données (ci-après « projet M5.1 »)[90], accompagné par le projet de spécifications techniques sur le catalogue national de

[88] Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement n° 2024/2847/UE, *JOUE* n° L 2025/327 du 5 mars 2025.

[89] Pour plus d'informations sur la consultation publique qui s'est déroulé du 20 janvier au 28 février 2025. Disponible ici uniquement en anglais.

[90] Draft guideline for data holders on data description, disponible ici.

métadonnées (ci-après « projet M5.3 »)[91], du projet de lignes directrices pour les utilisateurs de données sur les bonnes pratiques d'application et d'accès (ci-après « projet M6.2 »)[92] et du projet de lignes directrices pour les utilisateurs de données sur la manière d'utiliser les données dans un environnement de traitement sécurisé (ci-après « projet M7.1»)[93].

Bien que souvent technique, le contenu des quatre projets de lignes directrices traduit des ambitions cruciales notamment l'opérationnalisation des principes d'accessibilité, d'interopérabilité et de sécurité poursuivies par le Règlement. Ce commentaire aborde plus en détail les projets M5.1, M6.2 et M7.1.

I. LA DISPONIBILITE COMME PREALABLE À L'ACCESSIBILITE DES DONNEES DE SANTE AU SEIN DE L'EEDS

Les questions de disponibilité et d'accessibilité des données sont abordées dans le projet de ligne directrice M5.1. Ce projet vise à répondre à deux questions essentielles : quelles données devraient faire partie du catalogue de données disponibles au sein de l'EEDS, et surtout comment celles-ci devraient apparaître dans les catalogues de données. L'objectif est dès lors de proposer aux personnes qualifiées de détenteurs de données par le Règlement (*data holders*)[94] d'harmoniser la description des jeux de données mis à disposition des utilisateurs de données (*data users*)[95] grâce aux permis délivrés par les organismes responsables de l'accès aux données de santé (*Health Data Access Body* ou HDAB). Le projet de lignes directrices propose un vocabulaire commun de description des jeux de données à travers un modèle de métadonnées appelé HealthDCAT-AP[96].

Le modèle HealthDCAT-AP[97] classifie les informations constitutives des métadonnées en trois catégories. Les informations obligatoires, considérées comme indispensables à la description des jeux de données (par exemple, l'identification du HDAB compétent pour l'accès aux données, le cas échéant, la catégorie de données de santé à laquelle appartiennent les données du catalogue…)[98]. Les informations recommandées quant à elles sont fortement encouragées car elles apportent des indications supplémentaires sur les jeux de données disponibles (par exemple, la base légale justifiant le traitement des données, une déclaration sur la qualité du jeu des données, y compris le certificat de qualité)[99]. La dernière catégorie concerne les informations optionnelles qui peuvent être inclues dans les métadonnées sans que leur absence n'impacte l'objectif de standardisation de la description de données à l'échelle européenne (entre autres, la durée pour laquelle les données du catalogue sont disponibles pour une utilisation secondaire)[100].

L'harmonisation des catalogues nationaux selon un modèle européen permettra d'abord de mieux identifier les données disponibles pour une utilisation secondaire auprès du détenteur de données. Il s'agit de l'étape initiale de la procédure de demande d'accès.

II. QUELQUES BONNES PRATIQUES POUR UNE

[91] Draft technical specification on the national metadata catalogue, disponible ici.
[92] Draft guideline for data users on good application and access practice, disponible ici.
[93] Draft guideline on how to use data in a secure processing environment, disponible sur ici.
[94] Les détenteurs de données de santé sont définis à l'article 2(2), t), du Règlement sur l'EEDS.
[95] Les utilisateurs de données de santé sont définis à l'article 2(2), u), du Règlement sur l'EEDS.
[96] Draft guideline for data holders on data description, p. 13 et s.
[97] Ce modèle est expliqué en détail ici.
[98] Draft guideline for data holders on data description, p. 16 et 17.
[99] *Ibid.*
[100] *Ibid.*

DEMANDE D'ACCÈS EFFICACE

Une demande d'accès est efficace si le *data user* respecte les exigences de forme quant au choix du type de demande et les exigences relatives aux informations devant figurer dans la demande. En effet, le projet M6.2 vise principalement les utilisateurs de données et propose une série de bonnes pratiques pour soumettre une demande d'accès aux données dans le cadre de l'EEDS[101]. Il met l'accent sur trois principaux objectifs. Premièrement, le document devrait permettre aux demandeurs (potentiels utilisateurs de données) d'accroître leurs chances d'accéder aux données en fournissant des informations correctes tout au long de la procédure[102]. L'exactitude des données devrait alors faciliter, dans un second temps, l'examen ou la revue des HDAB[103]. Le tout dans le but de réduire considérablement les délais de traitement des demandes d'accès et d'assurer la conformité aux législations applicables.

Le *data user* doit préliminairement identifier le type de demande à introduire. Le projet de ligne directrice distingue la demande d'accès aux données de santé[104], de la demande de données de santé[105]. La différence réside dans le type de données sollicités par le Data User. La demande de données de santé est privilégiée par le Règlement car elle implique des résultats statistiques ou des données agrégées anonymisées lorsqu'elles suffisent à la finalité poursuivie par le *data user*[106]. Ce serait par exemple le cas « d'un chercheur intéressé par la prévalence du diabète et de l'hypertension dans un groupe d'âge spécifique dans les États membres »[107]. A ce stade il n'a besoin que de statistiques (chiffres) à l'échelle européenne sans qu'un accès à des données personnelles ne soit relevant.

Lorsque des données de santé anonymisées ou pseudonymisées sont nécessaires[108] au projet, le *data user* peut poursuivre la voie de la demande d'accès aux données de santé. Celle-ci implique des jeux de données susceptibles de permettre l'identification d'individus, dont l'accès peut être demandé à l'échelle nationale ou dans plusieurs Etats membres[109]. La demande d'accès peut dépasser les frontières nationales dans deux cas. Soit parce que les données sont rendues disponibles par un réseau unique de bases de données à l'échelle européenne[110], soit parce que la demande concerne plusieurs bases de données disponibles dans plusieurs États membres[111]. Dans les deux cas, la plateforme centrale européenne conçue pour connecter les différents catalogues nationaux pourra recevoir les demandes complètes émises par les *data users*[112].

Le projet de ligne directrice fournit également des illustrations et des captures d'écran relatives à l'étape de remplissage du formulaire de demande d'accès[113], des possibles scénarios de réponses des HDAB après évaluation de la demande[114] et des obligations applicables aux *data users* lorsque l'accès aux données est autorisé

[101] Draft guideline for data users on good application and access practice, p. 4.
[102] *Ibid.*, p. 7.
[103] Draft guideline for data users on good application and access practice, p. 7.
[104] *Ibid.*, p. 10 et 11.
[105] *Ibid.*, p. 11.
[106] V. également Règlement sur l'EEDS, considérant 73.
[107] Draft guideline for data users on good application and access practice, p. 10.
[108] La nécessité d'avoir accès aux données identifiantes doit être justifiée par le demandeur à la fois dans la requête d'accès aux données de santé et dans le protocole de l'étude, s'il s'agit d'un projet de recherche clinique.
[109] Draft guideline for data users on good application and access practice, p. 11.
[110] Draft guideline for data users on good application and access practice, p. 15.
[111] Draft guideline for data users on good application and access practice, p. 16.
[112] *Ibid.*
[113] V. Draft guideline for data users on good application and access practice, pp. 16 – 32.
[114] Draft guideline for data users on good application and access practice, p. 39.

notamment via un environnement sécurisé (*Secured Processing Environment* -SPE)[115].

III. UNE OPERATIONALISATION DE L'ENVIRONNEMENT SECURISÉ DE TRAITEMENT DES DONNEES (SPE)

Le dernier projet de ligne directrice vise à opérationnaliser le « SPE », un espace numérique sécurisé où seules des personnes autorisées peuvent accéder aux données, dont seules des statistiques ou des données agrégées peuvent être extraites. Il répond à trois principales questions. Comment définir l'environnement sécurisé approprié ? qui est responsable du traitement des données effectué au sein de l'espace ? enfin, quelles suites sont réservées aux données après analyse au sein de l'environnement sécurisé ?

Le caractère approprié d'un SPE est évalué par l'organisme d'accès aux données en fonction de la demande d'accès reçue. Il est donc recommandé au demandeur[116] de consulter l'organisme avant de démarrer la procédure car le remplissage du formulaire de demande d'accès impose de fournir les informations quant aux ressources techniques nécessaires à l'analyse des données au sein de l'environnement[117]. Encore faudrait-il que tous les demandeurs aient les compétences suffisantes pour décrire ces ressources avec précision. Dans tous les cas, il est relativement facile de deviner que plus les ressources seront importantes, plus les frais d'utilisation du SPE seront élevés[118].

La question de la responsabilité des traitements au sein du SPE ne peut être traitée sans clarifier les modalités d'accès à l'environnement sécurisé. Ledit accès n'est envisagé que si le demandeur a obtenu une autorisation délivrée par le HDAB compétent[119] et qui liste les personnes autorisées à accéder au SPE pour le compte du demandeur[120]. Ces personnes ne peuvent alors effectivement accéder à l'environnement sécurisé qu'en se connectant à l'aide d'une identification personnelle et d'un mot de passe robuste[121]. Il est également précisé que tout changement dans le personnel autorisé devra faire l'objet d'une notification et d'une nouvelle autorisation auprès du HDAB[122]. Le demandeur est donc pleinement responsable des traitements effectués au sein du SPE[123], par son personnel ou par toute autre personne autorisée et listée dans le permis[124]. Cette responsabilité l'oblige à s'assurer que les personnes précédemment mentionnées respectent la législation applicable en complément aux mesures techniques (chiffrement, journalisation, restrictions d'export) et organisationnelles (audit et traçabilité des opérations, notification des violations des données) déjà prévues.

La fin des analyses effectuées sur les données déclenche plusieurs actions. Tout d'abord, le HDAB évalue le risque de réidentification des données dont l'extraction du SPE est requise[125]. Une évaluation qui représentera un défi majeur

[115] Draft guideline for data users on good application and access practice, p. 33.
[116] Le demandeur ici fait référence au potentiel data user avant que le permis d'accès aux données soit délivré.
[117] Draft guideline on how to use data in a secure processing environment, p. 11.
[118] Pour plus de développement sur les coûts générés par l'établissement d'un SPE, v. Draft guideline on how to use data in a secure processing environment, p. 12.
[119] Draft guideline on how to use data in a secure processing environment, p. 9.
[120] *Ibid.*, p. 11.
[121] *Ibid.*, p. 13.
[122] *Ibid.*
[123] Ce principe de responsabilité correspond au même principe inhérent aux responsable du traitement tel que défini à l'article 4, paragraphe 7, du Règlement n° 2016/679 relatif à la protection des données à caractère personnel.
[124] Draft guideline on how to use data in a secure processing environment, p. 14 et 15.
[125] Cette évaluation permet à l'organisme responsable de l'accès de décider si les résultats peuvent sortir du SPE.

vu l'évolution d'une construction européenne de l'anonymisation considérée comme efficace d'un point de vue légal. En ce qui concerne les données ne pouvant pas être extraites, le SPE pourra les mettre à disposition du *data user* via une fonctionnalité d'archivage nécessitant moins de ressources et par conséquent moins coûteuse[126]. Dans tous les cas, les données ne seront conservées que pour la durée nécessaire au projet du demandeur sans excéder la durée de validité d'un permis, soit 10 ans renouvelable une fois après justification pertinente. Les données seront supprimées du SPE six mois après l'expiration du permis[127].

Enfin, les demandeurs alors devenus des *data u*sers ont l'obligation de publier les résultats de leur utilisation des données et d'informer les organismes d'accès de toute découverte intéressante pour la santé des individus[128].

Conclusion

Les projets de lignes directrices dessinent une architecture cohérente, où la transparence, l'harmonisation et la sécurité sont les piliers d'un accès encadré aux données de santé. Ils posent les fondements opérationnels de l'EEDS, en comblant partiellement le vide entre la norme européenne et les réalités nationales. Toutefois, ces documents pourraient être améliorés afin de garantir une mise en œuvre prévisible et cohérente à la taille et à la nature du demandeur. C'est d'ailleurs dans ce souci d'amélioration qu'ils ont été ouverts à consultation publique durant une année. Des questions subsistent notamment en ce qui concerne les garanties de soutenabilité technique et financière pour les États, les *data holders* et les *data users* ou encore une personnalisation des risques et des usages dans les environnements sécurisés.

Il est incontestable que l'implémentation de l'EEDS dépendra moins de la perfection du Règlement que de sa capacité à accompagner, sur le terrain, ceux qui détiennent ou utilisent les données de santé. Ces projets de lignes directrices en représentent les premières pierres.

[126] Draft guideline on how to use data in a secure processing environment, p. 17.

[127] *Ibid.*

[128] *Ibid.,* p. 18.

Le Règlement (UE) 2024/1860 du 13 juin 2024 : vers une mise en œuvre efficace d'EUDAMED ou une complexité accrue ?

par Kévin MINGOT

Étudiant en Master 2 Droit de la santé, Université Toulouse Capitole

Introduction

La réglementation des dispositifs médicaux dans l'Union européenne a été renforcée avec les règlements (UE) 2017/745 (MDR) et (UE) 2017/746 (IVDR), lesquels visent à améliorer la transparence, la traçabilité et la sécurité des dispositifs. Au cœur de cette réforme, EUDAMED[129] assure un suivi centralisé de chaque dispositif, de sa mise sur le marché à sa surveillance post-commercialisation. Elle centralise les informations relatives aux acteurs économiques, aux certificats, aux incidents, aux dispositifs eux-mêmes, ainsi qu'aux investigations cliniques. Ce rôle, encadré par l'article 33 du Règlement (UE) 2017/745, constitue le fondement juridique d'EUDAMED.

Le Règlement (UE) 2024/1860 du Parlement européen et du Conseil[130] est venu encadrer la mise en œuvre d'EUDAMED de manière progressive et sécurisée. Avant cette réforme, l'absence d'harmonisation entre les États membres avait mis en lumière des failles majeures dans le suivi des dispositifs médicaux, comme l'a révélé le scandale des prothèses mammaires PIP en 2010[131]. Cette crise sanitaire a précipité une révision complète du cadre réglementaire européen afin d'unifier des procédures entre États membres, tant pour la mise sur le marché que pour la surveillance, la vigilance et la traçabilité.

EUDAMED constitue l'un des piliers de cette réforme, aux côtés du renforcement des exigences de conformité[132] et du rôle accru des organismes notifiés[133]. Toutefois, la transition vers ce nouveau cadre a été marquée par des retards successifs. Initialement prévue pour 2020, sa mise en œuvre a été repoussée à plusieurs reprises. Notamment en raison de difficultés techniques liées au développement des modules, à leur interconnexion et à la préparation inégale des infrastructures nationales[134].

Le règlement de 2024 encadre ce déploiement progressif tout en imposant de nouvelles obligations d'information, notamment pour prévenir les risques de rupture d'approvisionnement des dispositifs médicaux de diagnostic in vitro[135] (DIV). Il

[129] EUDAMED, pour *European Database on Medical Devices*, désigne la base européenne dédiée au suivi des dispositifs médicaux.

[130] Adopté le 13 juin 2024, le Règlement (UE) 2024/1860 est paru au Journal officiel de l'Union européenne le 26 juin suivant.

[131] Des milliers de femmes ont été implantées avec des prothèses contenant du silicone industriel. L'affaire PIP (Poly Implant Prothèse), révélée en 2010, a mis en lumière l'absence d'un dispositif européen de traçabilité unifié pour les implants à l'époque.

[132] L'annexe I du Règlement (UE) 2017/745 fixe les exigences essentielles de sécurité, de performance clinique et de conception, auxquelles tout dispositif médical doit se conformer pour être mis sur le marché.

[133] Les articles 35 à 44 du Règlement (UE) 2017/745 précisent les conditions de désignation, d'évaluation conjointe et de contrôle continu des organismes notifiés, garants de la conformité réglementaire des dispositifs.

[134] En 2025, la Commission européenne indique que plusieurs modules d'EUDAMED, notamment celui relatif aux incidents, ne sont pas encore opérationnels (source : DG SANTE).

[135] L'article 9 du Règlement (UE) 2024/1860 impose aux fabricants une notification préalable aux

prévoit également un alignement des exigences d'enregistrement avec les bases nationales existantes, afin d'éviter une double charge administrative[136] pour les fabricants et les autorités de surveillance. Concrètement, les fabricants doivent enregistrer leurs dispositifs via un identifiant unique (UDI), et fournir l'ensemble des informations concernant leur structure, leurs mandataires, leurs importateurs et les certificats délivrés[137]. Chaque module d'EUDAMED sera activé individuellement après validation par un audit mené par la Commission européenne[138]. Cette mise en œuvre par étapes vise à éviter une entrée en vigueur brutale qui pourrait désorganiser le marché. Reste à déterminer si cette réforme facilite réellement l'utilisation d'EUDAMED ou si elle engendre au contraire une complexité accrue, notamment en matière de cybersécurité et de mise en conformité[139].

I. UN CADRE REGLEMENTAIRE EN MUTATION : ENTRE HARMONISATION ET INCERTITUDES

Une transition progressive face aux défis techniques. - Le Règlement (UE) 2024/1860 envisage un déploiement échelonné des modules d'EUDAMED afin de remédier aux retards techniques constatés depuis 2020 et de garantir une transition maîtrisée vers le nouveau système. L'objectif est d'éviter les perturbations du marché, tout en laissant aux opérateurs le temps nécessaire pour s'adapter.

EUDAMED comprend sept systèmes électroniques interconnectés[140], dont quatre sont finalisés, deux proches de l'être, et un consacré aux investigations cliniques et aux études de performance qui demeure en retard. Ce module incomplet bloque l'activation globale de la base et justifie donc la mise en œuvre progressive retenue par le législateur[141]. Comme précédemment évoqué, chaque module ne pourra être activé qu'après validation technique de la Commission européenne. Ce mécanisme permet de sécuriser la transition tout en évitant une mise en service prématurée ou instable du système.

Cybersécurité et conformité au RGPD : des défis persistants. - Le déploiement d'EUDAMED soulève des interrogations majeures en matière de sécurité des données, notamment de santé. Celles-ci doivent respecter le RGPD (Règlement (UE) 2016/679) et le Règlement (UE) 2018/1725, applicable aux institutions européennes[142]. En effet, la numérisation croissante des données de santé, couplée à leur caractère hautement sensible, rend impératif le renforcement des garanties de sécurité à chaque niveau du traitement.

autorités en cas de risque de pénurie de dispositifs de diagnostic in vitro.

[136] Certains États membres disposent déjà de bases de données nationales performantes, comme l'ANSM en France ou le BfArM en Allemagne, rendant un double enregistrement potentiellement contre-intuitif.

[137] L'identifiant unique UDI (Unique Device Identification) exigé par les articles 27 et 28 du MDR, permet de suivre chaque dispositif à toutes les étapes de son cycle de vie, renforçant ainsi la traçabilité.

[138] Conformément à l'article 10, chaque module ne peut être activé qu'après un audit de la Commission européenne attestant sa conformité technique, notamment en matière de cybersécurité et d'interopérabilité.

[139] La concentration des données dans EUDAMED accroît les risques d'intrusion. L'ENISA (Agence européenne pour la cybersécurité) alerte régulièrement sur ces enjeux depuis 2021.

[140] Les sept modules couvrent : les acteurs économiques, les dispositifs, les certificats, les incidents, la surveillance post-commercialisation, les investigations cliniques et la vigilance.

[141] En juin 2025, seul le module sur les investigations cliniques et les études de performance reste incomplet.

[142] Le RGPD s'applique aux opérateurs privés et publics nationaux, tandis que le règlement 2018/1725 encadre la gestion des données personnelles au sein des institutions de l'Union.

Par ailleurs, les retards observés dans les projets EES[143] et ETIAS[144] illustrent les difficultés récurrentes d'interopérabilité et de coordination entre les systèmes nationaux[145]. Ces projets ont été ralentis par l'hétérogénéité des systèmes nationaux, la complexité des protocoles de sécurité et un manque de gouvernance commune.

Ces obstacles, que l'on retrouve également dans le cas d'EUDAMED, soulignent que le succès technique repose autant sur la qualité des outils que sur la volonté politique d'harmoniser les infrastructures numériques[146]. Le Règlement (UE) 2024/1860[147] prévoit que la base ne pourra être pleinement activée tant que le module relatif aux investigations cliniques et aux études de performance n'est pas achevé.

Bien que des audits indépendants soient prévus pour valider chaque module d'EUDAMED conformément à l'article 34 du Règlement (UE) 2017/745 modifié, la multiplication des cyberattaques et l'interopérabilité encore incomplète soulèvent une question centrale : ces garanties techniques suffiront-elles à instaurer une confiance durable chez les fabricants, les autorités et les patients [148] ?

Interopérabilité avec l'EHDS : un défi majeur. - L'un des enjeux les plus sensibles reste l'interopérabilité entre EUDAMED et l'Espace Européen des Données de Santé (EHDS). Ces deux initiatives poursuivent des objectifs complémentaires mais s'appuient sur des logiques différentes : EUDAMED centralise des données réglementaires sur les dispositifs médicaux, tandis que l'EHDS vise à améliorer l'accès et la portabilité des données médicales des patients dans toute l'Union[149].

Une coordination technique étroite entre les deux systèmes est essentielle pour prévenir la fragmentation des normes et assurer une circulation fluide des données de santé. En l'absence d'interopérabilité, l'accès harmonisé aux données pourrait être entravé, réduisant l'impact des dispositifs pourtant conçus pour améliorer la transparence et la traçabilité[150].

II. UNE GESTION DE L'APPROVISIONNEMENT ENCORE PERFECTIBLE

Une obligation d'information en cas de rupture d'approvisionnement. - Le Règlement (UE) 2024/1860 introduit un nouvel article 10 bis, lequel impose aux fabricants de dispositifs médicaux une obligation d'information préalable, notamment en cas de cessation d'approvisionnement susceptible d'entraîner un préjudice grave pour la santé publique. L'objectif est d'anticiper les pénuries critiques et de permettre aux autorités compétentes de déployer des mesures de gestion adaptées. Les fabricants doivent ainsi informer les autorités

[143] Le Entry/Exit System (EES), instauré par le Règlement (UE) 2017/2226, enregistre électroniquement les entrées et sorties des ressortissants de pays tiers dans l'espace Schengen à l'aide de données biométriques.

[144] Le système ETIAS (European Travel Information and Authorisation System), créé par le Règlement (UE) 2018/1240, impose une autorisation de voyage préalable aux ressortissants de pays tiers dispensés de visa court séjour.

[145] Leurs mises en œuvre ont été retardées, illustrant les faiblesses des systèmes européens d'interopérabilité et les difficultés techniques récurrentes.

[146] Ces retards s'expliquent notamment par les différences techniques entre États membres et l'absence d'un pilotage technique clair à l'échelle européenne.

[147] Le considérant 2 indique que l'activation complète d'EUDAMED reste conditionnée à la finalisation du module dédié aux investigations cliniques.

[148] L'ENISA (Agence européenne pour la cybersécurité) identifie régulièrement les données de santé comme hautement sensibles et souligne les vulnérabilités croissantes liées à leur centralisation numérique.

[149] L'EHDS vise à établir un espace commun de données de santé dans l'UE, facilitant l'accès transfrontalier pour les citoyens et leur réutilisation encadrée pour la recherche et les politiques publiques.

[150] Une incompatibilité entre les deux systèmes pourrait entraîner des doublons, des pertes d'informations ou limiter l'interopérabilité, réduisant l'efficacité globale du dispositif européen.

nationales, ainsi que les autres opérateurs économiques concernés, au moins six mois avant la cessation prévue et justifier les raisons de cette interruption[151] (défaillance technique, rupture de matière première, retrait volontaire, etc).

Toutefois, l'effectivité de cette obligation dépend largement de la capacité des États membres à traiter et surveiller ces signalements. Or des écarts persistent : certains États peinent à déployer les ressources humaines et numériques nécessaires afin de garantir une surveillance réactive et homogène[152]. De plus, l'absence d'outils harmonisés au niveau européen complique davantage la détection rapide des risques d'approvisionnement.

Prolongation des délais transitoires : un risque de saturation des organismes notifiés ? - Pour éviter une rupture réglementaire brutale et limiter les risques de pénurie, le Règlement 2024/1860 prévoit également une prolongation des délais de mise en conformité des dispositifs médicaux avec les nouvelles exigences du MDR. Les nouvelles échéances[153] sont désormais fixées au 31 décembre 2027 pour les dispositifs de classe *D*, au 31 décembre 2028 pour ceux de classe *C*, et au 31 décembre 2029 pour les dispositifs de classe *B* ainsi que pour les dispositifs de classe *A* stériles.

Cette transition prolongée vise à maintenir la disponibilité des dispositifs critiques sur le marché, tout en laissant aux fabricants le temps de s'adapter. Toutefois, cela soulève un risque important : seulement quarante-neuf organismes notifiés sont actuellement désignés pour gérer un volume considérable de demandes de certification[154]. Ce déséquilibre pourrait engendrer une saturation préoccupante, ralentissant l'entrée en conformité des dispositifs.

La lourdeur administrative et le manque de moyens de certains organismes font craindre une saturation, risquant de retarder l'accès à des dispositifs essentiels, en particulier pour les établissements de santé. La prolongation des délais est néanmoins conditionnée à plusieurs exigences. Les fabricants doivent démontrer qu'ils respectent encore les règles des directives antérieures (93/42/CEE ou 98/79/CE) et que leur dispositif ne présente pas de risque supplémentaire pour la santé publique. Enfin, les démarches doivent avoir été engagées avant le 26 mai 2025 pour les dispositifs des classes *D* et *C*[155].

Reste une incertitude : ces délais permettront-ils réellement d'absorber toutes les demandes de certification ? Ou faudra-t-il envisager, à moyen terme, de nouveaux ajustements réglementaires pour éviter une crise d'approvisionnement d'envergure ?

Conclusion

Ce règlement reflète la volonté de l'Union de garantir la sécurité des patients tout en préservant la transparence du marché et la capacité d'adaptation des acteurs économiques. En prévoyant un déploiement progressif d'EUDAMED, de nouvelles obligations d'information et un allongement des délais transitoires, le texte cherche à éviter les ruptures brutales tout en renforçant la régulation.

Toutefois, son efficacité dépendra directement d'une mise en œuvre harmonisée entre les Etats membres, d'un soutien logistique renforcé des autorités

[151] L'obligation ne s'applique que si l'interruption est susceptible d'affecter la santé publique ; des dérogations sont prévues en cas d'urgence ou de force majeure.

[152] Certains États ne disposent pas de systèmes d'alerte numérique aussi réactifs que celui de l'ANSM, ce qui limite la capacité à gérer les signalements en temps réel.

[153] Ces nouvelles dates figurent en annexe du Règlement (UE) 2024/1860 et étendent les délais initiaux prévus à l'article 120, §3 du MDR.

[154] Les 49 organismes notifiés recensés doivent pouvoir certifier tous types de dispositifs, ce qui représente une contrainte forte, surtout dans les pays disposant de peu de structures agréées.

[155] Les fabricants doivent avoir engagé la procédure avant cette date, soit par la signature d'un contrat, soit par le dépôt formel d'une demande auprès d'un organisme notifié.

nationales et d'une mobilisation suffisante des organismes notifiés. *A contrario*, la charge administrative pourrait rapidement devenir un facteur de blocage, en particulier pour les petites structures[156].

La diversité des systèmes nationaux et des capacités techniques soulève un autre point de vigilance : celui d'une interprétation variable des obligations, laquelle pourrait menacer l'uniformité du cadre juridique. Des fabricants pourraient alors contester certaines dispositions techniques ou demander des ajustements, sans pour autant remettre en cause l'objectif fondamental de libre circulation des dispositifs médicaux sur le marché intérieur[157]. Dès lors, le respect des principes de subsidiarité et de proportionnalité demeure essentiel. Ces principes imposent que l'action de l'Union n'excède pas ce qui est nécessaire pour atteindre les objectifs fixés[158]. Afin que la réglementation reste à la fois ambitieuse et applicable, il est alors nécessaire de trouver un équilibre entre intégration européenne et adaptation au terrain. Sans ajustements adaptés, EUDAMED pourrait se heurter à des limites structurelles compromettant son efficacité réelle.

Règlement n° 2024/1860/UE du Parlement européen et du Conseil du 13 juin 2024 modifiant les règlements n°s 2017/745/UE et 2017/746/UE en ce qui concerne un déploiement progressif d'EUDAMD, l'obligation d'informer en cas d'interruption ou de cessation d'approvisionnement et les dispositions transitoires applicables à certains dispositifs médicaux de diagnostic in vitro,
***JOUE* n° L 2024/1860 du 9 juillet 2024**

[156] Le coût élevé et la complexité des démarches de certification pèsent particulièrement sur les PME, souvent moins armées pour absorber ces contraintes réglementaires.

[157] Le règlement peut faire l'objet d'un contrôle juridictionnel via des recours en annulation ou des questions préjudicielles, notamment en cas de divergences d'interprétation entre États membres.

[158] Prévu à l'article 5 TUE, le principe de subsidiarité limite l'action de l'Union à ce que les États ne peuvent accomplir seuls ; la proportionnalité impose de ne pas excéder ce qui est nécessaire pour atteindre les objectifs de l'Union.

Directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH,
Université Toulouse Capitole & CERPOP,
Université de Toulouse, UMR 1295 Inserm,
équipe BIOETHICS

En octobre 2024, la Commission européenne a souhaité mettre à jour sa directive relative à la responsabilité du fait des produits défectueux. Ainsi, la nouvelle directive (UE) 2024/2853 abrogera et remplacera la directive 85/374/CEE[159] dès son entrée en vigueur prévue en décembre 2026. Nous précisons que ce texte ne sera alors applicable que pour les produits qui seront mis sur le marché après cette date.

Cette directive conserve le fondement même de finalité initiale, c'est-à-dire l'harmonisation des pratiques et règles juridiques afin de préserver la libre circulation de marchandises et le bon fonctionnement du marché intérieur[160]. Cependant, cette mise à jour règlementaire s'explique en raison des évolutions technologiques, et notamment du déploiement de la mise sur le marché d'innovation telles que les intelligences artificielles (IA). En ce sens, il est précisé, dès le troisième considérant de la directive, que cette révision a été rendue nécessaire « à la lumière des évolutions liées aux nouvelles technologies, y compris l'intelligence artificielle (IA) »[161]. De même, il apparaissait important de réaffirmer des principes nécessaires pour garantir une sécurité juridique suffisante, notamment au regard de certains termes dont la définition même du « produit »[162]. La sécurisation du cadre juridique sera alors propice aux déploiements des technologies innovantes, mais devra, cette fois-ci, tenir davantage compte la protection de la santé, des biens des consommateurs ainsi que des autres personnes physiques[163].

La mise à jour de cette directive ne présente pas d'impact sur le fondement de la responsabilité. Ainsi, **la responsabilité sans faute est affirmée**, considérée comme un moyen suffisant face aux risques de production et de mise sur le marché de technologies nouvelles[164].

Par ailleurs, cette adoption règlementaire établit une mise au point concernant son **champ d'application**. Dès lors, il est rappelé que l'ensemble des produits, corporels ou incorporels, sont concernés, ceci comprenant notamment les systèmes d'intelligence artificielle ainsi que les logiciels, que ces derniers soient commercialisés comme des produits autonomes ou bien des composants d'un produit spécifique. La redéfinition du produit permet d'écarter certains éléments dont les informations telles que les fichiers numériques, les codes sources d'un logiciel ou bien encore les livres électroniques qui ne sont alors pas considérés comme des produits et n'entrent donc pas dans le champ d'application de la directive[165]. En somme, pour entrer dans le champ d'application du texte, il est rappelé la nécessité que le produit soit commercialisé, que ce dernier soit qualifié comme tel et que son fabriquant soit identifié.

La directive autorise **la réparation des dommages** allant au-delà des biens matériels pour inclure également les atteintes aux personnes. Dès lors, afin de protéger les individus, il est nécessaire de prévoir une compensation pour les pertes

[159] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, JOUE 18.11.2024. Accessible ici.
[160] *Op. Cit.,* considérant 8.
[161] *Op. Cit.*, considérant 3.
[162] *Op. Cit.*, considérant 3 et art. 4, 1).
[163] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, considérant 1.
[164] *Op. Cit.*, considérant 2.
[165] *Op. Cit.*, considérant 13 et art. 5.

matérielles découlant non seulement de la mort ou de blessures corporelles - comme les frais funéraires, médicaux ou de la perte de revenus par exemple – mais aussi de la destruction ou de la dégradation de données, ce qui les relie à la première catégorie de dommages. En plus des atteintes aux biens, le texte prévoit que « le droit à réparation couvre également les pertes immatérielles résultant des dommages visés […], dans la mesure où ils peuvent être indemnisés en vertu du droit national »[166]. Toutes ces pertes doivent être indemnisées, que ce soit pour la victime immédiate ou pour des victimes indirectes.

Concernant les défauts de produit, la **défectuosité** est définie comme l'insuffisance de sécurité que l'on peut légitimement attendre, conformément au droit de l'Union ou national[167]. La directive indique que le défaut ne se réfère pas à la sécurité qu'une personne peut raisonnablement espérer. La substitution du pronom « on » par « une personne [168]» dans l'ancien texte a des implications, insistant sur le fait que la détermination de la défectuosité nécessite une évaluation objective de la sécurité à laquelle le grand public peut s'attendre. Cela implique que l'analyse intègre des éléments concrets relatifs au groupe d'utilisateurs visé. De plus, cette nouvelle directive vient confirmer la jurisprudence de la Cour de Justice de l'Union Européenne (CJUE), établissant qu'un tribunal pourrait conclure à la défectuosité d'un produit sans preuve directe, si celui-ci provient d'une série de production dont un produit a déjà été déclaré défectueux[169].

De plus, un changement notable est à prendre en compte : il ne sera plus possible pour un patient de se voir opposer le risque mentionné dans une notice pour contester le caractère défectueux d'un produit[170]. Ainsi, les avertissements ou informations fournies avec celui-ci ne suffiront pas à garantir la sécurité d'un produit défectueux. Avec cet ajout, le texte vise à interdire les « notices parapluies » que les producteurs pourraient utiliser pour échapper à leur responsabilité.

Enfin, il est précisé que « l'utilisation raisonnablement prévisible englobe également la mauvaise utilisation qui n'est pas déraisonnable dans les circonstances »[171], comme celle d'un utilisateur d'appareil due à un manque d'attention ou celle de groupes particuliers tels que les enfants, doit être envisagée. Cela pourrait par exemple se référer à l'usage d'un médicament à des fins différentes de celles autorisées. Les producteurs doivent prévoir un mauvais usage et ne peuvent pas se défendre à ce sujet si cela était prévisible et causait un dommage.

Le point clé de la directive réside dans la **charge de la preuve** et les procédures de preuve[172]. Elle entérine la jurisprudence de la CJUE selon laquelle la preuve de la défectuosité ainsi que celle du lien de causalité est libre, ce qui implique qu'elle peut être apportée par présomptions[173]. Le texte va plus loin encore, en définissant des situations où la défectuosité ou le lien de causalité peuvent être présumés et où la charge de la preuve est inversée. Par exemple, si un produit est établi comme défectueux et que le type de dommage supporté est généralement causé par cette défectuosité. Pour infirmer cette présomption, la défense doit prouver que le dommage a une autre cause. Cela s'applique également lorsque la défense ne fournit pas les informations demandées par les plaignants. Ces derniers peuvent exiger que les informations soient intelligibles

[166] *Op. Cit.*, art. 6, 2.
[167] *Op. Cit.*, art. 7, 1.
[168] *Ibid*.
[169] CJUE, 05 mars 2015, Boston Scientific Medizintechnik, aff. Jointes C-503/13 et C-504/13.
[170] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, considérant 31.
[171] *Ibid.*
[172] *Op. Cit.*, art. 10.
[173] CJUE, 21 juin 2017, aff. C-621/15.

pour faciliter leur action. Dans ces cas, la charge de la preuve repose sur le défendeur[174]. En ce sens, la directive reconnaît que l'asymétrie entre producteurs et demandeurs nuit à une juste réparation du dommage causé. Ce sont les juridictions nationales qui jugeront de la légitimité des demandes de transmission d'informations, s'assurant que l'accès soit « nécessaire » et « proportionné »[175] pour protéger le secret professionnel. En conséquence, cette faculté des demandeurs de demander des preuves détenues par le défendeur a des implications sur la charge de la preuve, pouvant également s'appliquer aux défendeurs pour contrer une demande de réparation. Dans tous ces cas, ce sont les tribunaux qui évalueront la légitimité des demandes et leur caractère nécessaire. Considérant cela, il y a fort à croire que le secret médical sera l'une des principales cibles de telles requêtes.

Une autre nouveauté significative de ce texte est **l'exonération pour risque de développement**[176]. Ce faisant, la directive confirme, là encore, la jurisprudence de la CJUE en la matière[177], probablement rendu nécessaire face au caractère incertain et mouvant des évolutions technologiques actuelles. En effet, ce risque de développement est objectivement imprévisible – ne reposant donc pas sur les connaissances subjectives que le fabricant peut avoir en sa possession mais sur l'état des connaissances scientifiques et techniques objectivement connu au regard de l'objectif poursuivi lors de la mise sur le marché du produit.

En outre, nous soulignons que la directive maintient le **délai de prescription** de trois ans prévus par le texte antérieur, qui court à compter du moment où la victime a raisonnablement dû avoir connaissance du dommage, du défaut du produit et de l'identité du producteur[178]. De plus, ce nouveau texte prévoit également un délai de forclusion de vingt-cinq ans afin de prévenir les cas particuliers d'apparitions lentes des symptômes de lésions corporelles[179]. Par cet ajout, l'Union européenne souhaite apporter une réponse la plus suffisante possible aux victimes qui ne peuvent pas encore avoir connaissance de leurs maux.

Enfin, nous précisons que la directive conserve son caractère exclusif : ce régime de responsabilité étant le seul applicable aux produits défectueux, sans pouvoir être concurrencé par des dispositions nationales[180]. Pour autant, des dérogations sont prévues afin de laisser une marge de manœuvre aux Etats membres. Il faut maintenant voir comme les juridictions nationales parviendront à se saisir de ce texte.

Directive n° 2024/2853/UE du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive n° 85/374/CEE du Conseil, *JOUE* n° L 2024/2853 du 18 novembre 2024.

[174] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, art. 10.
[175] *Op. Cit.*, art. 9.
[176] *Op. Cit.*, art. 18.
[177] CJCE, 29 mai 1997, aff. C-300/95, §27.
[178] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, art. 16.
[179] *Op. Cit.*, art. 17, 2.
[180] Directive (UE) 2024/2853 du Parlement et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, considérant 1.

Communication de la Commission du 15 janvier 2025 relative au « Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé », *COM(2025)* 10 final

La Commission européenne présente son premier plan d'action visant à améliorer et à renforcer la cybersécurité et la résilience des hôpitaux et prestataires de soins. Car, si le numérique transforme en profondeur le secteur de la santé, en permettant de meilleurs services aux patients grâce à des outils numériques tels que les dossiers médicaux électroniques, la télémédecine et les diagnostics alimentés par l'intelligence artificielle[181]*, ceux-ci deviennent des « potential targets »*[182] *[« cibles potentielles »] pour la cybercriminalité et les cyberattaques. Désormais, les établissements de santé sont obligés de composer « with an increasingly complex and dynamic threat landscape » [« avec un paysage de menaces de plus en plus complexe et dynamique »]*[183]*, ce qui les exposent à des risques graves pour la sécurité de leurs réseaux et systèmes d'informations, et causant des dommages directs*[184] *et inacceptables*[185] *à la vie des patients.*

Ainsi donc, pour protéger au mieux les établissements de santé contre les cyberattaques tout en soutenant le déploiement complet (« *full deployment* »)[186] de l'Espace européen des données de santé (EHDS)[187], le plan d'action de la Commission préconise le renforcement des capacités de préparation, de détection et de réponse des hôpitaux et des prestataires de soins de santé. Il propose en particulier à l'Agence de l'Union européenne pour la cybersécurité (ENISA), de créer en son sein un **Centre européen d'appui en matière de cybersécurité** (« ***European Cybersecurity Support Centre for hospitals and healthcare providers*** »)[188]. Ce centre fournira aux infrastructures de santé des conseils, des outils, des services personnalisés et des formations spécifiques en matière de préparation, de prévention, de détection et de réaction aux cyberattaques, leur permettant de construire progressivement un catalogue complet de services répondant à leurs besoins en la matière (« ***comprehensive service catalogue catering to the[ir] needs*** »)[189].

[181] Communication de la Commission du 15 janvier 2025, *op. cit.*, p. 1.
[182] Tels que « *delaying medical procedures, causing gridlocks in emergency rooms and (…), in extreme cases, lead to the loss of life* » [« causer des dommages directs aux patients, retarder les procédures médicales, provoquer des blocages dans les salles d'urgence et (…), dans des cas extrêmes, entraîner la perte de vies humaines »] », *ibid.*, p. 4.
[183] *Ibid.*, p. 3.
[184] *Ibid.*, p. 1.
[185] *Ibid.*, p. 16.
[186] *Ibid.*, p. 1.
[187] Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement n° 2024/2847/UE, *JOUE* n° L 2025/327 du 05/03/2025.
[188] Communication de la Commission du 15 janvier 2025, *op. cit.*, p. 6.
[189] *Ibid.*

Présentées en gras dans le texte, les **priorités** de ce plan d'action sont les suivantes :

- « ***prevent*** *cybersecurity incidents in the first place, because prevention is always better than the cure* » [« **prévenir** les incidents de cybersécurité en premier lieu, car il vaut toujours mieux prévenir que guérir »] ;
- « ***detect*** *cyber threats, allowing a faster reaction* » [« **détecter** les cybermenaces, de manière à réagir plus rapidement »] ;
- «*better* ***respond*** *to incidents, and (…)* ***recover*** *from them* » [« mieux **réagir** aux incidents et (…) s'en **remettre** »] ;
- « ***deter*** *cyber threat actors from launching attacks against health systems in Europe* » [« **dissuader** les acteurs de la cybermenace de lancer des attaques contre les systèmes de santé en Europe »][190].

Renforcer la prévention[191]

Le plan d'action propose plusieurs options aux États membres pour qu'ils accroissent la capacité de leur secteur de la santé à prévenir les incidents de cybersécurité. Ils pourront ainsi s'appuyer sur les « conseils clairs et ciblés » [« ***clear targeted guidance*** »][192] émanant du Centre d'appui de l'ENISA, et qui porteront sur la façon dont les infrastructures de santé mettent œuvre des bonnes pratiques en matière de cybersécurité, et bénéficier des « modules de formation en ligne » (« ***online training modules*** »)[193] traitant spécifiquement de la gestion des cyber-risques, créés et diffusés par ce même conseil. Les États membres sont également invités à user d'autres démarches, par exemple d'offrir aux micro-hôpitaux et prestataires de petite ou moyenne taille des « ***Cybersecurity Vouchers*** » [« **chèques cybersécurité** »][194] afin les aider financièrement à mettre en place des mesures de prévention et de réaction adaptées.

Améliorer la détection des cyber-menaces

Échanger de l'information et collaborer les uns avec les autres sont deux actions essentielles pour améliorer l'identification des cyber-menaces et leur détection. Il incombe alors au Conseil d'appui de mettre en place, d'ici à 2026, un service d'alerte précoce à l'échelle européenne en cas de cyber-attaques visant le secteur de la santé (« ***EU-wide early warning subscription service for the health sector*** »)[195], qui émettrait des notifications d'alertes en temps quasi réel. Dans le même temps, les États membres sont fortement encouragés à notifier au Centre de d'appui de l'ENISA tous les incidents de cyber-sécurité ayant affecté leurs établissements de santé[196].

Mieux réagir aux cyber-attaques

Pour relever les défis qui se posent en matière de réponse aux cyber-attaques, le plan d'action propose par exemple la création d'un service de réaction rapide spécifiquement destiné au secteur de la santé (« *Rapid Response Service specifically for the health sector* »). Il s'agira de l'intégrer à la réserve de cybersécurité de l'UE, composée de fournisseurs de services de sécurité gérés de confiance capables d'aider les États membres ou les institutions européennes « à réagir aux incidents de cybersécurité importants (…) ou à fournir une assistance à cet effet,

[190] *Ibid.*, p. 2.
[191] *Ibid.*, p. 7 et suivants.
[192] *Ibid.*, p. 8.
[193] *Ibid.*, p. 12.
[194] *Ibid.*, p. 9.
[195] *Ibid.*, p. 13.
[196] *Ibid.*, p. 12.

et à amorcer le rétablissement après de tels incidents »[197] et dont la création et la mise en œuvre sont régis par les dispositions du règlement sur la cybersolidarité[198]. En outre, des exercices nationaux de cybersécurité (« ***national cybersecurity exercises*** »)[199] seront parallèlement menés à l'édition et la diffusion de guides/manuels d'aide (« ***playbooks*** »)[200], qui aideront les infrastructures de santé à répondre aux cyber-menaces, en particulier les attaques par rançonlogiciel (« ransomware »). Sur ce point précis, le plan d'action recommande aux États membres de demander à certains établissements de santé[201] « *to report on any ransom payments made and on ransom payments they intend to make* » [« de déclarer tout paiement de rançon effectué et tout paiement de rançon qu'ils ont l'intention d'effectuer »][202], afin de mieux coordonner le soutien et les actions des autorités répressives.

Dissuader les cyber-attaques

Enfin, ce plan d'action inclut également des mesures dans le domaine de la dissuasion des cyber-menaces ciblant le secteur de la santé à travers l'utilisation de la « boîte à outils cyberdiplomatique » (« ***The Cyber Diplomacy Toolbox*** »)[203]. Élaboré dans le cadre de la politique étrangère de sécurité commune (PESC), cet outil concourt à la prévention des actes de cyber-malveillance à l'échelle de l'Union et de ses États membres et permet, si nécessaire, d'imposer des sanctions aux personnes ou entités qui se rendraient coupables de tels actes[204].

La Commission européenne a lancé une **consultation publique** autour de ce plan d'action visant à renforcer la cybersécurité des hôpitaux et des prestataires de soins, dont la date limite de dépôt des contribution est fixée au lundi 30 juin 2025.

Cybersolidarity Act[1]

Entré en vigueur le 4 février 2025, le règlement européen sur la cybersolidarité devrait contribuer à renforcer les capacités de détection et de réaction de l'Union face aux risques liés à la cyber-sécurité et à la cyber-criminalité, dont sont victimes, parmi d'autres, les établissements de santé français. Il faut donc des **mesures phares**, qui doivent voir le jour pour renforcer la solidarité au niveau de l'Union, consolider l'écosystème de cyber-sécurité, accroître la cyber-résilience des États membres et développer les aptitudes, savoir-faire et compétences dans le domaine de la cyber-sécurité[1].

a) Un **système européen d'alerte en matière de cybersécurité**, dont le but sera de mettre en place des capacités coordonnées en matière de détection des menaces et de partage des informations ;

b) Un **mécanisme d'urgence dans le domaine de la cybersécurité**, qui aidera les États membres, à leur demande, à se préparer aux incidents de cybersécurité, à y réagir et à amorcer leur rétablissement ;

c) Un **mécanisme européen d'analyse des incidents de cybersécurité**, afin d'examiner et d'évaluer des incidents de cyber-sécurité.

.

[197] Article 13, paragraphe 1, du règlement n° 2025/38/UE du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement n° 2021/694UE (règlement sur la cybersolidarité), *JOUE* n° L du 24 janvier 2025.
[198] *Ibid.*, articles 13 à 18.
[199] P. 14.
[200] *Ibid.*
[201] Ceux considérés comme « entités essentielles » ou « entités importantes » et tombant dans le champ d'application matériel de la directive NIS 2.
[202] P. 14.
[203] *Ibid.*, p. 16.
[204] V. à ce sujet, la décision (PESC) n° 2019/797/PESC du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, *JOUE* n° L 129I du 17/05/2019 et le règlement n° 2019/796/UE du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, *JOUE* n° L 129I du 17/05/2019.

Droit français

Mettre l'intelligence artificielle au service de la santé : l'état des lieux du Ministère de la santé et de l'Accès aux soins

par Joud GHARZEDDINE

Étudiante en Master 2 Juriste européen, Université Toulouse Capitole

Introduction

Le 11 février 2025, à l'occasion du Sommet pour l'action sur l'intelligence artificielle, Yannick Neuder, le ministre chargé de la Santé et de l'Accès aux soins, a annoncé la publication officielle de l'état des lieux de l'intelligence artificielle en santé en France. Ce rapport, intitulé *Mettre l'intelligence artificielle au service de la santé*, fait le point sur les avancées et les perspectives du déploiement de l'IA dans le système de santé français, dressant par la même occasion une vision globale des actions engagées.

L'IA, qui fait l'objet d'une stratégie nationale depuis 2018, constitue un enjeu stratégique majeur pour le domaine de la santé. En effet, son déploiement promet une nette amélioration de la qualité des soins avec la transition progressive vers une médecine plus préventive et une optimisation du temps médical, permettant une prise en charge plus efficace des patients. Ce document, articulé autour des quatre axes de la feuille de route du plan numérique de 2023-2027, présente ainsi les différentes actions dédiées à l'IA en santé dans chacun de ces axes, à savoir la prévention (1), la prise en charge (2), l'accès à la santé (3) et le cadre propice (4).

1. Développer la prévention et rendre chacun acteur de sa santé avec les systèmes de l'IA

« Mieux vaut prévenir que guérir ». Ce vieux dicton médical résume parfaitement ce premier axe, qui détaille les actions engagées en faveur d'une santé participative et préventive. Ces actions s'appuient en grande partie sur la stratégie d'accélération « Santé numérique » de France 2030 dont l'objectif est de faire de la France un leader de la e-santé. L'innovation est au cœur de cet objectif et est ainsi particulièrement soutenue, avec un investissement à hauteur de 500 M€ dédiés à des projets embarquant de l'IA ou encore avec des financements destinés à l'évaluation de l'IA en santé. Un accent est notamment mis sur la création de lieux permettant l'émergence d'innovations technologiques de l'IA en santé, alliant acteurs publics et privés. La Plateforme de données en santé (Health Data Hub) soutient au même titre de nombreux projets, dont 40% sont estimés faire usage de méthodes d'intelligence artificielle afin de développer des outils de diagnostic et de dépistage.

2. Redonner du temps aux professionnels de santé et améliorer la prise en charge des personnes avec l'appui de l'IA

La confiance est le maître mot de ce deuxième axe, qui fait le bilan des actions entreprises en faveur d'un recentrage de la santé sur l'humain. En effet, les systèmes

d'IA permettent l'automatisation de certaines tâches administratives et sont susceptibles de faciliter l'aide au diagnostic, tel qu'en atteste leur utilisation actuelle en imagerie par exemple. Toutefois, ce recentrage ne saurait s'opérer en l'absence de confiance de la part des professionnels de santé dans les dispositifs médicaux embarquant de l'IA. C'est ainsi qu'un accent particulier est mis sur la formation de ces professionnels aux opportunités et aux limites de l'IA, formation désormais obligatoire dans la majorité des études de santé. La Haute Autorité de santé (HAS) a notamment publié un guide d'aide au choix des dispositifs médicaux numériques à usage professionnel, dont ceux embarquant de l'IA[205]. Toujours dans cet esprit de mise en confiance à l'usage, un véritable accompagnement au déploiement de l'IA est prévu, avec l'élaboration de démarches qualité liées à l'utilisation de systèmes d'IA en contexte de soins et de conseils par l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP) sur la base de cas d'usages actuels et de retours d'expérience[206], visant à faciliter le recours à l'IA en établissement.

3. Améliorer l'accès à la santé pour les personnes et les professionnels qui les orientent, en intégrant les outils d'IA dans les parcours

Ce troisième axe recense les actions entreprises afin de répondre à des préoccupations de longue date des Français : la lutte contre les déserts médicaux et la disparité de l'offre médicale sur le territoire, dans un contexte de pénurie de professionnels de santé[207]. L'implémentation de l'IA en santé est perçue comme un moyen de retrouver du temps médical grâce à, *inter alia*, une meilleure gestion des rendez-vous médicaux et une meilleure orientation des patients. Cette implémentation ne saurait toutefois se passer d'un cadre réglementaire strict, à l'image de celui établi par le règlement sur l'intelligence artificielle[208], et de l'élaboration de référentiels éthiques, impératifs pour un usage en confiance. La cellule Éthique du numérique en santé du ministère de la Santé et de l'Accès aux soins a publié plusieurs documents à cet égard, émettant des recommandations de bonnes pratiques concernant par exemple *« l'éthique by design »*[209]. Cependant, les recommandations émises en ce domaine seraient dépourvues d'intérêt en absence d'une traduction concrète dans les pratiques professionnelles. C'est ainsi que la Haute Autorité de santé veille à améliorer l'impact de ses productions et à leur appropriation effective par les professionnels de santé. Enfin, l'usage de l'IA en santé se développe notamment du fait des initiatives portées par les Agences Régionales de santé (ARS) qui

[205] Haute Autorité de Santé, Guide d'aide au choix des dispositifs médicaux numériques à usage professionnel, Validé par le Collège le 22 juin 2023.
[206] Un guide intitulé *Déployer l'IA en toute confiance !* a été publié le 12 février 2025 sur le site de l'ANAP. Il contient les premiers conseils de déploiement d'une IA de confiance en établissement. Disponible ici. (Consulté le 18/04/2025).
[207] Cette préoccupation est d'actualité. V. à ce sujet, « Le Pacte de lutte contre les déserts médicaux, présentation par le Premier ministre du plan d'action pour renforcer l'accès aux soins des Français », dossier de presse, 25 avril 2025. Disponible ici. (Consulté le 27/04/2025)
[208] Règlement n° 2024/1689/UE du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements n° 300/2008, n° 167/2013, n° 168/2013, 2018/858, 2018/1139 et 2019/2144 et les directives n° 2014/90/UE, 2016/797 et 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* n° L 2024/1689 du 12/07/2024.
[209] L'éthique by design suppose de songer à l'éthique dès la conception, mais aussi à l'issue de la réalisation. Ce concept a fait l'objet d'un rapport de la Cellule éthique du numérique en santé de la délégation ministérielle au Numérique en Santé. V. à ce sujet : Ministère des Solidarités et de la Santé, « Recommandations de bonnes pratiques pour intégrer l'éthique dès le développement des solutions d'Intelligence Artificielle en Santé : mise en œuvre de *« l'éthique by design »* », avril 2022. Disponible ici (Consulté le 18/04/2025).

favorisent une intégration durable de l'IA en santé.

4. Déployer un cadre propice pour le développement des usages de l'IA en santé et construire un modèle économique durable de l'IA en santé sur la base de gains d'efficience

Ce dernier axe est consacré, tel que son nom l'indique, au développement d'un modèle économique garant d'une intégration efficace et durable de l'IA en santé. Cet objectif de durabilité exige que soient rendues accessibles les innovations faisant recours à l'IA, que ce soit pour les patients avec une prise en charge prévue par l'Assurance maladie ou pour les professionnels, à défaut de quoi leur adoption par les établissements de santé serait peu probable. Cet objectif de durabilité nécessite notamment, tel qu'évoqué dans le deuxième axe, de bâtir une IA digne de confiance. Cela rappelle le principal défi auquel est confronté le déploiement de l'IA en santé, à savoir l'accès aux données de santé. Les données de santé sont en effet indispensables à la validation de l'IA en santé en ce qu'elles permettent d'obtenir de meilleurs résultats en matière de soins. L'utilisation secondaire des données de santé fait ainsi depuis peu l'objet d'un règlement au niveau européen[210] qui, malgré le fait qu'il correspond aux objectifs de la stratégie nationale du numérique en santé, requiert néanmoins une adaptation du cadre législatif et règlementaire national. Enfin, cet axe revient sur la création de PariSanté Campus, un espace de formation, de recherche, d'innovation et d'entreprenariat dont l'objectif premier est, en écho avec l'ambition affichée du Sommet pour l'action sur l'IA, à savoir faire de Paris la capitale de l'IA.

Conclusion

Un constat s'impose à la lecture du rapport du Ministère de la Santé et de l'Accès aux soins : le déploiement de l'IA en santé est déjà une réalité qu'il faut poursuivre, soutenir et accélérer. Ce déploiement ne peut toutefois s'opérer, tel qu'il a été affirmé à plusieurs reprises, en absence d'un cadre règlementaire et économique facilitant l'appropriation des innovations embarquant de l'IA par les établissements, mettant en exergue la nécessité d'établir une stratégie nationale claire et cohérente sur l'IA. Le Ministère de la Santé et de l'Accès aux soins se saisit donc de l'opportunité, à travers cette présentation globale des actions déjà entreprises, de réaffirmer son engagement pour développer une IA souveraine, compétitive et de confiance. Cet engagement se traduira par une feuille de route de l'IA en santé, dont la publication est attendue avant l'été 2025.

Rapport du Ministère en charge de la santé, *Mettre l'intelligence artificielle au service de la santé – État des lieux de l'intelligence artificielle (IA) en santé*, Février 2025

[210] Règlement n° 2025/327/UE du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement n° 2024/2847, *JOUE* n° L 2025/327 du 05/03/2025.

Comité éthique de l'Inserm, *Guide de bonnes pratiques de l'Intelligence artificielle à l'Inserm,* Février 2025

par Noémie DUBRUEL

Doctorante en droit de la santé, IMH, Université Toulouse Capitole & CERPOP, Université de Toulouse, UMR 1295 Inserm, équipe BIOETHICS



En février 2025, l'Institut national de la santé et de la recherche médicale (Inserm) a publié un Guide de bonnes pratiques de l'Intelligence Artificielle (IA) à l'Inserm, intitulé : « Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence Artificielle dans la recherche à l'Inserm »[211]*. Cette publication est issue d'une note conjointe du Comité d'éthique de l'Inserm, du programme Lorier et du Conseil scientifique de l'Inserm et recoupe l'analyse d'experts extérieurs.*

Forte du constat relatif au déploiement de plus en plus rapide de l'IA – notamment des IA génératives – dans l'ensemble des secteurs de la vie humaine, dont celui de la santé et de recherche, sans encadrement spécifiques à leurs usages ou mésusages, l'Inserm a jugé important d'alarmer le grand public mais également les membres de l'institution sur les enjeux et questions éthiques qui y sont liés[212].

Le constat est alors établi : à l'Inserm, les IA soutiennent la démarche scientifique, mais leur usage s'étend aussi à l'administration, où ils pourraient à terme aider à la prise de décision concernant les projets, la gestion ou les ressources humaines. Ces systèmes offrent des avantages significatifs : ils permettent de traiter d'énormes volumes de données, d'accélérer la découverte de mécanismes pathologiques, de révéler de nouveaux biomarqueurs, de prédire l'apparition de maladies et d'envisager une médecine de plus en plus personnalisée. Ainsi, au quotidien, les IA sont des outils précieux pour la rédaction, en générant des résumés, des plans de documents, en améliorant le style, corrigeant l'orthographe et la grammaire, en aidant à la création et à la vérification de codes informatiques, ou encore en assurant la traduction, ce qui permet de gagner du temps sur des tâches à faible valeur ajoutée[213]. Toutefois, les auteurs de ce guide alarment rapidement sur les impacts négatifs, tels que son coût énergétique et ses conséquences écologiques, ainsi que de nombreuses interrogations sur les effets à moyen et long terme, les incertitudes et risques liés à la qualité et à la confidentialité des données, aux biais algorithmiques, à l'interprétation des résultats, à la dépendance aux technologies propriétaires, à la vulnérabilité des pratiques et infrastructures face aux attaques malveillantes, ou encore à la perte de souveraineté[214].

Face à ce constat, les auteurs ont souhaité examiner les conséquences des usages de l'IA, leurs avantages ainsi que les risques potentiels et questions non résolues.

---

[211] ATLAN H., BOURGAIN C., CHNEIWEISS H., EISINGER F., VIDAL C., et al., « Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence Artificielle dans la recherche à l'Inserm », Guide de bonnes pratiques de l'Intelligence Artificielle à l'Inserm / Février 2025, 2025, inserm-04975393f. Accessible ici : https://inserm.hal.science/inserm-04975393v1/document

[212] *Op. Cit.* pp.06.

[213] *Op. Cit.* pp.08.

[214] *Op. Cit.* pp.17-26.

L'objectif principal de ce guide réside dans l'émission d'un ensemble de recommandations prenant en compte les questions éthiques relatives à l'utilisation des IA à l'Inserm[215]. En sommes, ces recommandations sont variées et couvrent :

1- Les questions de divulgation et de transparence (des modèles, des données et des usages notamment ;
2- Des obligations de transparence relatives aux attributions et usages des modèles ;
3- L'utilisation de données synthétiques ;
4- La vérification des résultats : les auteurs recommandent notamment « la création d'une cellule nationale et transversale sur les usages du numérique pour les sciences pour la santé à l'Inserm »[216] ;
5- La documentation des données des algorithmes d'IA ;
6- Les notions d'intégrité et d'équité dans l'usage des IA ;
7- Le recours à un système de surveillance continue et de contrôle via des solutions alternatives et un engagement public affirmé ;
8- La mise en œuvre d'une formation continue pour l'ensemble du personnel, scientifique et administratif, pour l'usage du numérique et de l'IA ;
9- La création et l'usage d'un « passeport de données de santé », qui documenterait l'origine, la qualité et les biais des données ;
10- La création d'un portail de transparence.

Une telle initiative met en évidence les enjeux liés au déploiement des IA pour diverses finalités et les besoins croissants des scientifiques et chercheurs à bénéficier d'accompagnement dans leurs usages et considérations de ces innovations si facilement accessibles.

[215] *Op. Cit.* pp.02-.05.
[216] *Op. Cit.* pp.04.

Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence artificielle dans la recherche à l'Inserm : la nécessité d'un arbitrage consciencieux entre soutien au progrès scientifique et prise en compte des risques délétères sous-jacents

par Romane MASSIMI et Pierre-Emmanuel PARENT DE CURZON

Étudiants en Master 2 Juriste européen,
Université Toulouse Capitole

Suite à la constitution d'un groupe de travail rassemblant le Comité d'éthique de l'Institut national de la santé et de la recherche médicale (ci-après Inserm), du programme LORIER et du Conseil scientifique de l'Inserm, une note conjointe intitulée « Recommandation de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence Artificielle dans la recherche à l'Inserm » fut publiée en février 2025. Celle-ci a pour objectif de dresser un large panel des enjeux de l'application des systèmes d'intelligence artificielle (ci-après SIA) en santé ainsi que des recommandations quant à leur utilisation et son développement. Cette publication se subdivise en trois parties, la première expliquant son intérêt, la seconde référençant les questions éthiques majeures concernant l'utilisation des SIA à l'Inserm et la dernière présentant une liste de recommandations adéquates.

La finalité de cette note conjointe s'inscrit donc dans une récente montée en puissance de l'utilisation des SIA. En effet, l'incorporation de ces derniers au sein de l'Inserm tant dans ses activités de recherche que dans la gestion de son administration ne saurait se passer d'un encadrement. Ce cadre a été construit pour identifier les défis éthiques nés de l'utilisation des SIA au sein de l'Inserm (**I**), et les recommandations figurant à cette note ont pour but de conduire à un arbitrage approprié entre innovation et appréhension des risques (**II**).

I. L'IDENTIFICATION DES DEFIS INDUITS PAR L'UTILISATION DES SIA AU SEIN DE L'INSERM

Cette publication expose onze questions éthiques majeures. Il y a une réelle volonté pédagogique d'exposer tant les risques que les avantages entraînés par l'utilisation des SIA au sein d'un organisme national de recherche public tel que l'Inserm.

Ces problématiques se répartissent schématiquement en deux catégories, celles afférentes aux enjeux techniques et méthodologiques (**A**), et celles liées aux enjeux sociaux et environnementaux (**B**).

A. Les enjeux techniques et méthodologiques de l'emploi des SIA au sein de l'Inserm

Il est indéniable que les capacités de traitement de données sur le plan quantitatif offertes par les SIA, invitent les autorités compétentes à considérer de plus près sa démocratisation dans le cadre de la recherche. Cependant, un pas de recul invite à ne pas invisibiliser certains risques réels déjà observés dans d'autres secteurs. À titre d'exemple, l'existence de biais algorithmiques apparaît préoccupante. Il en va de même s'agissant des hallucinations liées à la langue utilisée ou à la reconnaissance vocale.

L'Inserm rappelle également que le fonctionnement des SIA nécessite un traitement de données préalablement recueillies. Celles-ci doivent être de qualité

suffisante au risque de fausser les résultats générés. Cela pose alors la question des atteintes à la vie privée et invite à distinguer correctement les notions d'anonymisation et de pseudonymisation qui sont souvent à tort confondues. Là où le premier est un processus irréversible, le second conserve des éléments qui suffisent à permettre la ré-identification des personnes concernées. Cette note rappelle également la place centrale de l'intégrité scientifique lors de l'utilisation des SIA. Il apparaît en effet nécessaire de s'assurer que leur emploi ne compromet pas d'une part la qualité et d'autre part la reproductibilité des résultats. Enfin, les SIA en tant que valeur au sein d'un marché concurrentiel ne peuvent s'émanciper des questions de propriété intellectuelle.

B. Les enjeux sociaux et environnementaux liés à l'emploi des SIA au sein de l'Inserm

Il est nécessaire de mentionner l'impact que peuvent avoir les données diffusées dans le cadre d'une utilisation des SIA. La diffusion se doit d'être maîtrisée, en cas de mauvaise gestion, la publication de ces données peut occasionner des dommages sociaux importants, notamment en renforçant des discriminations existantes. Sur le plan juridique une diffusion non contrôlée contrevient au Règlement général sur la protection des données 2016/679 (ci-après RGPD). L'utilisation des SIA inquiète aussi en ce que les professionnels doivent pouvoir comprendre et conserver un esprit critique sur les outils dont ils se servent. En effet, l'emploi des SIA ne doit pas ternir la qualité de la recherche en question et sa fiabilité.

Un autre impact important de l'utilisation des SIA réside dans son coût environnemental. En effet, la transition numérique s'oppose ici à la transition écologique en ce qu'elle s'accompagne d'émission de gaz à effet de serre, ainsi que d'une utilisation significative de l'eau nécessaire au refroidissement des SIA. De plus, il entraîne une pollution de l'eau exponentielle, faisant suite à l'extraction des terres rares pour la construction d'infrastructures fondamentales à leur développement.

En listant ces multiples problématiques, l'Inserm entend éduquer mais aussi prévenir et anticiper au mieux les répercussions de l'utilisation des SIA sans pour autant minimiser ses bienfaits. En effet, la réglementation des SIA en santé est cruciale dans la mesure où le règlement 2024/1689[217] harmonisant l'encadrement de l'intelligence artificielle (ci-après IA) ne trouve pas à s'appliquer pour des SIA conçues uniquement à des fins de recherche et de développement scientifique. C'est donc dans ce contexte général que l'Inserm dresse ses recommandations à propos de l'IA en santé.

II. PRESENTATION DES RECOMMANDATIONS SUSCEPTIBLES DE CONDUIRE A UN ARBITRAGE APPROPRIE ENTRE INNOVATION ET APPREHENSION DES RISQUES

Les mots clés de ce guide sont prudence (**B**) et transparence (**A**), il convient d'anticiper les risques sans pour autant priver l'organisme public des avantages de cette technologie.

A. La nécessité d'une transparence accrue

Dans le cadre d'une gestion courante des tâches administratives ou de l'accès aux soins, l'enjeu principal réside dans la transparence du fonctionnement des SIA,

[217] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (Texte présentant de l'intérêt pour l'EEE) PE/24/2024/REV/1 JO L, 2024/1689, 12.7.2024

notamment pour ce qui est de l'aide à la prise de décision, ou encore la gestion des ressources humaines. La transparence est un enjeu clé en ce qu'elle permet une meilleure traçabilité des données et des décisions mais aussi un encadrement réglementaire plus efficace. La compréhension du raisonnement des SIA est indispensable pour que les professionnels conservent leur autonomie, ce qui implique une formation spécifique et approfondie de ces derniers. Toujours en ce sens, il est recommandé de mettre en place une vérification systématique des analyses produites, celles-ci s'effectuant sous la responsabilité du personnel concerné. Dans le même sens, un système de reporting interne à l'Inserm permettrait de recenser les dysfonctionnements, limites de capacité, ou biais potentiels des SIA utilisés. Il s'agit donc d'encourager un usage sobre et éclairé des SIA.

Enfin, dans un souci de traçabilité des informations présentes au sein d'une publication scientifique, il serait également nécessaire d'indiquer explicitement l'implication des SIA dans le processus de recherche et son rôle afin d'éviter toute confusion avec des observations réelles.

B. La nécessité d'une prudence accrue.

L'utilisation de données dites synthétiques semble présenter une véritable innovation au sein de cette nouvelle technologie. Elles présentent l'avantage d'une plus grande sécurité quant à la confidentialité des données sous couvert du RGPD. En effet, la création de données d'entraînement pour des SIA, permet d'écarter la potentielle réidentification des personnes concernées suite à une pseudonymisation. Cependant, pour que leur utilisation reste pertinente les données synthétiques générées, doivent disposer d'une certaine verisimilitude. Le but étant qu'elles correspondent aux tendances que souligne l'analyse d'une base de données originale. La question de la confidentialité est donc bien évidemment au cœur de la question des données synthétiques, puisque celles-ci ne laissent pas en théorie la possibilité de remonter de façon certaine à des individus réels, sauf lorsque les données originales ont un caractère trop sensible. Dans cette situation, il sera nécessaire de procéder à une désensibilisation des données.

Aussi, dans le but de garantir la fiabilité des données, il est envisageable d'appliquer le principe de minimisation aux SIA, par exemple en privilégiant les Small Language Models (SLMs). Bien que ceux-ci disposent de ressources limitées de par leur échantillon de données plus restreints, ils permettent une plus grande maîtrise des SIA.

Pour conclure, il nous apparaît ici que l'élaboration d'un cadre éthique dans l'application de l'IA en santé est tout à fait salutaire. En effet, la démocratisation récente de l'IA nous amène à envisager une multitude d'interrogations auxquelles il convient d'y répondre rapidement. Celles-ci intervenant à la fois dans un contexte général propre à la régulation de l'IA, mais également en phase avec les contraintes techniques et les biais qu'induisent une généralisation d'un tel outil aussi bien dans le cadre de la recherche que dans l'accès aux soins.

Henry ATLAN et *al.*, *Recommandations de bonnes pratiques suite à l'analyse des questions éthiques soulevées par l'utilisation de l'Intelligence Artificielle dans la recherche à l'Inserm. Guide de bonnes pratiques de l'Intelligence Artificielle à l'Inserm*, Février 2025.

Consultation publique nationale « Construisons ensemble un patrimoine national des données de santé » et autres consultations en matière d'utilisation secondaire des données de santé

par Lisa FERIOL

Doctorante CIFRE, Ekitia et Équipe BIOETHICS,
CERPOP UMR1295 Inserm et Université Toulouse Capitole

Introduction

Le Ministère de la Santé et de l'accès aux soins a présenté le 30 septembre dernier une première version de la Stratégie nationale pour l'utilisation secondaire des données de santé[218] réalisée en concertation avec les acteurs concernés. Cette stratégie qui entend couvrir la période 2025-2028 se base sur les recommandations formulées dans le rapport de la mission Marchand-Arvier[219] intitulé Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé[220].

À la différence de l'utilisation primaire des données qui désigne l'utilisation de données de santé au bénéfice de la prise en charge médicale d'un patient, l'utilisation secondaire des données de santé, également couramment désignée par l'expression de « réutilisation », désigne l'utilisation de données de santé pour des finalités autres que celles prévues lors de la collecte initiale, comme la recherche, l'innovation, les politiques publiques ou encore le pilotage du système de santé. En mettant l'accent sur cette ambition, le gouvernement français se place dans le sillon de la Stratégie européenne pour les données présentée par la Commission européenne en 2020[221] qui vise à libérer le potentiel des données détenues sur le territoire de l'Union européenne de tous secteurs confondus, qu'elles soient personnelles ou non. Afin de créer les espaces communs de données sectoriels prévus par la stratégie européenne, le Règlement européen sur l'Espace européen des données de santé (ci-après Reg. EEDS)[222] a récemment été adopté. Pour rappel le Règlement sur l'Espace européen des données de santé ambitionne de développer un cadre de gouvernance européen commun au service de la circulation des données de santé permettant une meilleure prise en charge des citoyens européens sur le territoire de l'Union mais aussi d'améliorer l'accès aux données de santé détenues en UE au profit de leur utilisation secondaire pour des finalités d'intérêt public encadrées par le règlement.

[218] Dont le nom officiel est « Stratégie interministérielle pour construire notre patrimoine national des données de santé ». Disponible ici.

[219] Cette mission a été confiée en juin 2023 par le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, la ministre de l'Enseignement supérieur et de la Recherche et le ministre de la Santé et de la Prévention à Jérôme Marchand-Arvier, Stéphanie Allassonnière, Aymeril Hoang et Anne-Sophie Jannot avec le concours de l'Inspection générale des affaires sociales. Cette mission visait à poser les premières bases de la feuille de route en matière d'utilisation secondaire des données de santé.

[220] Inspection Générale des Affaires Sociales (IGAS), Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé, 5 décembre 2023, 150 p. Disponible ici.

[221] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2022 portant sur « Une stratégie européenne pour les données », *COM(2020)* 66 final. V. aussi, site de la Commission européenne, « Stratégie européenne pour les données de santé ».

[222] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847.

Ainsi, cette stratégie nationale pour l'utilisation secondaire des données de santé entend adresser à travers 37 recommandations formulées les enjeux nationaux liés aux données de santé personnelles et non-personnelles (incluant donc les données anonymisées) pour faire de la France un « leader dans le domaine de la santé numérique ». Les grands enjeux mentionnés sont le soutien à l'innovation, l'amélioration des collaborations entre acteurs, le fait de capitaliser sur le patrimoine dont dispose la France en la matière notamment à travers le Système National des Données de Santé, assurer les droits et la confiance des personnes concernés en créant un système socialement acceptable et accélérer les procédures d'accès aux données de santé. Par ce biais, cette stratégie entend également anticiper l'entrée en application progressive des obligations prévues par le Reg. EEDS, comprenant la mise à disposition obligatoire des données de santé détenues par les détenteurs désignés par le règlement, impliquant la mise en place à l'échelle des Etats membres du système de gouvernance imposé par le nouveau règlement.

L'approche de cette stratégie visant à organiser le paysage français, au-delà du cadre législatif, par la concertation des acteurs et la réflexion sur la manière d'encourager de meilleures synergies entre ces derniers fait écho à cette de la Stratégie européenne. En effet, la stratégie européenne pour les données présentée ambitionne de libérer le potentiel des données en créant « un meilleur accès aux données et un cadre assurant leur utilisation responsable » en combinant « une législation et une gouvernance adéquates ». Ainsi, au-delà du cadre législatif c'est un système de gouvernance européen qui devra permettre la réalisation des objectifs de la stratégie ; appelant alors les Etats membres à s'organiser en interne pour répondre aux futures obligations.

Afin de ne pas réitérer les écueils du passé et susciter l'adhésion des acteurs concernés à ce futur cadre, la construction de cette stratégie se veut fédératrice des multiples initiatives existantes en ce sens, autant dans les acteurs qui l'ont proposé[223] que dans les acteurs visés. Des rencontres auprès des différentes parties prenantes ont ainsi été organisées entre octobre et novembre dans toutes les régions de France pour recueillir leurs retours. Ces rencontres ont été couplées à une consultation publique proposée en ligne du 30 septembre au 5 novembre 2024[224]. L'objectif affiché étant de « façonner une trajectoire commune, cohérente et ambitieuse pour développer les bases de données et l'usage secondaire des données de santé, afin qu'ils soient à la hauteur des enjeux actuels et futurs. ». 55 contributions de 42 participants différents ont été recueillies à travers cette consultation publique. La typologie des contributeurs est variée puisque nous retrouvons des citoyens, des établissements de santé, des intégrateurs en informatique, des organismes institutionnels, des professionnels de la santé ou encore des associations de patients, des prestataires de services informatiques ou des industriels. A noter que parmi les auteurs anticipés comme potentiels répondant à la contribution, les structures médico-sociales, les maîtres d'ouvrage de services numériques mutualisés, les maisons pluriprofessionnelles ou centres de santé et

[223] En effet, la présentation de cette première version a réuni la Délégation au numérique en santé (DNS), la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES), la Direction générale de la recherche et de l'innovation (DGRI), la Plateforme des Données de Santé, la Caisse Nationale d'Assurance Maladie (CNAM), la Direction générale de l'offre de soins (DGOS), la Direction générale des entreprises (DGE) et l'Agence de l'innovation en santé (AIS) ainsi que des témoins de l'écosystème représentants les différents types d'acteurs concernés par le sujet (représentant des usagers du système de santé, représentant des centres hospitalo-universitaires, représentant des industriels, etc.).

[224] Site internet de l'Agence du Numérique en Santé, Consultation publique nationale « Construisons ensemble un patrimoine national des données de santé », disponible ici.

les laboratoires de biologie médicale n'ont pas formulé de contribution. On peut quand même estimer que la consultation réussi un premier pari : celui de toucher une diversité d'acteurs afin de représenter la diversité des intérêts et enjeux au regard des acteurs concernés. L'Agence du Numérique en Santé va prochainement proposer une synthèse de ces contributions qui seront intégrées au document de travail qu'est pour l'instant la proposition de stratégie.

Ce commentaire visera à présenter les thématiques dominantes formulées par les acteurs dans leurs contributions à cette consultation publique, et à faire le lien avec les autres mécanismes de consultation avec les parties prenantes mis en place à l'échelle française en lien avec l'entrée en application prochaine du Règlement sur l'Espace européen des données de santé qui oriente et impacte l'élaboration de cette stratégie nationale.

1. Les grandes orientations de la proposition de stratégie nationale

La première version de la stratégie mise en consultation publique entend proposer les grandes orientations pour mettre au service de finalités d'intérêt public le patrimoine important dont dispose la France en matière de données de santé ; ceci en proposant un cadre éthique et sécurisé au regard de la nature des données concernées et en s'inscrivant dans une démarche de transition écologique.

Les 4 grands axes déclinés en 10 actions permettant d'organiser les actions de la stratégie sont :

- Favoriser la transparence et la confiance des citoyens en mettant en place une gouvernance nationale de l'utilisation secondaire des données de santé lisible et représentative, en simplifiant l'exercice des droits, en améliorant l'information des citoyens et en construisant un cadre sécurisé et de confiance pour la réutilisation des données de santé,
- Constituer des bases de données conçues pour la réutilisation en enrichissant le patrimoine de bases de données d'intérêt, en anticipant le principe de mise à disposition des données dès la conception et en formant l'écosystème à la réutilisation des données de santé,
- Favoriser une mise à disposition efficace des données de santé en recensant les bases de données existantes et en construisant un modèle équilibré de partage de données,
- Faciliter l'utilisation des données de santé en simplifiant les procédures de mise à disposition.

La stratégie lie ces différentes actions avec les recommandations formulées au niveau national par le rapport de la mission Jérôme Marchand-Arvier ainsi qu'avec les travaux de l'action conjointe européenne TEHDaS (Towards European Health Data Space)[225] afin d'assurer une cohérence dans ses propositions[226].

2. Les principaux points d'attention relevés par les acteurs

Parmi les 55 contributions formulées, on retrouve des thématiques communes comme le modèle de gouvernance national à mettre en œuvre, la simplification des processus d'accès aux données de santé, les modalités d'exercice des droits individuels ou encore la qualité des données et les standards qui y sont appliqués.

[225] L'action conjointe TEHDaS (Towards European Health Data Space) a été lancée en février 2021 et est cofinancée par la Commission européenne et a mobilisé la coopération de 25 Etats membres de l'Union. L'objectif est de développer et promouvoir des concepts orientés sur le partage et l'utilisation secondaire des données de santé dans le cadre de l'Espace européen des données de santé. Une deuxième phase a été lancée en mars 2024. Disponible ici.

[226] V. Annexes Stratégie interministérielle pour construire notre patrimoine national des données de santé, 2025-2028, disponible ici.

Pour un modèle de gouvernance non-centralisé. On retrouve de manière répétée parmi les contributions l'invitation à adopter une approche fédérée ou décentralisée de la gouvernance nationale de l'utilisation secondaire des données de santé ; les deux termes étant utilisés de manière assez interchangeable mais plaidant pour la même chose : la reconnaissance de niveaux de gouvernance infranationaux. Cette défense de l'échelon infranational s'appuie sur des arguments différents : limitation de l'impact écologique en ne dupliquant pas les données, renfort de la sécurité des données, défense d'une possible gouvernance locale des données permettant une proximité avec les équipes ayant collecté ou généré les données et bases de données associées qui sont souvent des équipes de soin. Cette approche fédérée/décentralisée complémen -taire à l'approche centralisée que nous connaissons aujourd'hui avec le SNDS se place dans le sillon de ce qu'avait recommandé le rapport de la mission Marchand-Arvier, à savoir mettre en place une gouvernance davantage fédératrice et moins centralisatrice.

Reprenant les statuts introduits par le Reg. EEDS, les acteurs anticipent et proposent pour ce faire d'être qualifiés en tant qu'organisme d'accès aux données de santé[227] (ORAD) territorial permettant ainsi un certain maillage territorial possible. Au-delà de la proposition d'introduire des ORAD territoriaux, une autre proposition est celle de prévoir des ORAD thématiques, permettant par exemple de prendre en compte des instituts de recherche. Ce sont surtout les entrepôts de données de santé (EDS) existants comme par exemple les groupements interterritorial et/ou inter-régional qui se positionnent pour être reconnus ORAD territoriaux. Cependant, l'urgence à financer de manière pérenne le réseau d'EDS qui a commencé à être déployé est bien soulignée en parallèle, en défendant une approche globale des coûts que ces derniers impliquent pour les hôpitaux et autres acteurs concernés.

Cette gouvernance fédérée/décentra-lisée pourrait se matérialiser en une complémentarité entre un catalogue de données national (SNDS élargi par la loi du 24 juillet 2019[228]) et un catalogue des métadonnées des détenteurs de données de santé référencé dans le catalogue national. Cette recommandation des acteurs converge avec ce qui avait été préconisé par la mission Marchand-Arvier qui proposait de revoir la notion de catalogue telle qu'entendue aujourd'hui par notre Code de la santé publique[229] pour ne plus avoir cette approche centralisatrice et pouvoir ainsi référencer des métadonnées de données détenues à des niveaux plus locaux.

Cette reconnaissance de l'échelon territorial est également demandée dans les instances de gouvernance nationale comme au sein du Comité stratégique des données de santé[230] (Costrat) : une représentativité

[227] Les États membres devront désigner un ou plusieurs organismes d'accès aux données de santé (ORAD) dont les missions sont énumérées à l'article 57 du Reg. EEDS qui devront coopérer entre eux à l'échelle européenne ainsi qu'avec la Commission européenne. Leur mission principale peut être résumée par le fait de statuer sur les demandes d'accès aux données de santé et d'autoriser et délivrer les autorisations de traitement de données pour l'accès à des fins d'utilisation secondaire aux données de santé répertoriées dans le catalogue européen des données de santé prévu par l'Espace européen des données de santé et de donner accès aux données de santé électroniques aux utilisateurs de données.

[228] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

[229] Le rapport préconise en effet que la réplication des bases de données sur la plateforme technologique de la Plateforme des données de santé ne devrait plus conditionner leur inscription au catalogue du SNDS tel que le Code de la santé publique le prévoit actuellement à son article R1461-3. V. Inspection Générale des Affaires Sociales (IGAS), *Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé*, *op. cit*. p.11.

[230] Le comité stratégique des données de santé a été créé par un arrêté du 29 juin 2021. Il a pour mission d'apporter au ministre des éléments d'orientation et

des détenteurs de données de santé est plébiscitée afin de représenter leurs besoins particulièrement divers au regard de leurs différentes natures. Les établissements de soin, les organismes institutionnels comme les instituts de recherche mais aussi les industriels se sont positionnés en ce sens. De manière intéressante, il est recommandé par certains acteurs d'inclure des critères médicaux et scientifiques dans la gouvernance nationale de l'utilisation secondaire des données de santé, notamment à travers l'instauration de groupes de travail ou d'un comité scientifique permettant de définir des priorités scientifiques.

Dans la continuité d'une reconnaissance de l'expertise des acteurs à l'échelle territoriale, les établissements de santé demandent également à reconnaître le rôle central de formateur des centres hospitalo-universitaires, afin de structurer le paysage français de l'utilisation secondaire des données de santé. Les propositions portent ici sur le fait de souligner dans la stratégie la nécessaire formation des personnels de santé aux questions liées à l'utilisation secondaire des données de santé, mais aussi à l'ouverture de postes hospitalo-universitaires afin de soutenir ce besoin de formation ainsi que la recherche. Cette demande est à rapprocher du rattachement désormais quasi systématique des CHU à des entrepôts de données de santé.

Simplification des processus d'accès aux données de santé. Une thématique récurrente dans les contributions recueillies est celle de la simplification des processus d'accès aux données de santé. La lenteur des processus actuels présente selon les acteurs un risque pour l'avancée de la recherche et donc par ricochets pour les patients. Le rapport de la mission Marchand-Arvier faisait de ce sujet un des objectifs centraux que la stratégie nationale devait intégrer, notamment au regard des délais fixés par le nouveau règlement sur l'Espace européen des données de santé[231]. Cependant, certains acteurs avertissent du risque qui existe à trop simplifier les procédures, en soulignant la nécessité d'octroyer davantage de moyens à la CNIL pour ne pas mettre en péril les droits des personnes concernées par le traitement de leurs données personnelles.

Respect des droits individuels. Les citoyens ayant répondu à la consultation demandent davantage de transparence sur l'utilisation des données de santé grâce à une plateforme centralisant et engendrant un contrôle plus accru de leurs utilisations. Les mesures mises en place en faveur d'une information améliorée sont également nécessaires afin d'assurer une effectivité des droits des personnes concernées. Également, au-delà de l'information, la formation des citoyens aux enjeux de l'utilisation des données de santé afin de leur permettre de participer aux instances de gouvernance est mentionnée.

Standards et qualité des données. Il ressort également des commentaires une invitation à mettre en place des mesures dédiées à la collecte et la production des données afin d'assurer une utilisation secondaire des données de qualité, notamment en standardisant les systèmes d'information hospitaliers marqués aujourd'hui par une grande hétérogénéité entravant l'interopérabilité des données collectées. De manière plus générale, une réflexion doit être menée sur un standard à adopter lors de la collecte des données et sur la manière de soutenir les acteurs de terrain

de décision relatifs à la mise en œuvre et au développement du système national des données de santé. Il est composé d'une pluralité d'acteurs comprenant notamment les directeurs généraux des principales agences concernées par le numérique en santé, de directeurs généraux d'instituts de recherche ou encore de représentants d'établissements de santé désignés, et de représentants d'associations d'usagers du système de santé.

[231] Le rapport mentionne un délai moyen d'accès aux données du SNDS de 10 à 12 mois alors que le règlement prévoit un délai de trois mois pour que le détenteur de données mette à disposition au sein de l'environnement de traitement sécurisé les données pour lesquelles une autorisation d'accès a été délivrée par un ORAD (article 60 §2 Reg. EEDS). Ce délai peut être prolongé dans des cas justifiés de trois mois.

en tant que producteurs de données, ceci incluant les personnels soignants. L'amélioration de la collecte et de la qualité des données à la source est essentielle pour assurer une utilisation secondaire pertinente grâce à des données interopérables. Pour ce faire, le modèle décentralisé est plébiscité par les acteurs évoquant ces enjeux puisqu'il permet de faire collaborer et échanger utilisateurs et producteurs de données assurant une meilleure compréhension des données de santé utilisées et donc une utilisation secondaire de qualité.

Au-delà de la standardisation des systèmes d'information hospitaliers, le recours à des logiciels libres assurant une indépendance face aux solutions privées et le recours à des solutions européennes est aussi encouragé afin d'assurer une meilleure souveraineté de notre système d'utilisation secondaire des données de santé. Le corollaire est donc le recours à des solutions d'hébergement décentralisées et sécurisées certifiées SecNumCloud. L'impact environnemental des solutions envisagées est abordé, de manière cependant assez timide.

3. La construction de la stratégie nationale à la croisée d'autres consultations des parties prenantes sur l'utilisation secondaire des données de santé

L'entrée en application prochaine des dispositions sur l'utilisation secondaire des données de santé du Reg. EEDS a conduit la Délégation du Numérique en Santé (DNS) à déployer des actions spécifiques afin de recueillir les avis des parties prenantes sur ce sujet spécifique. Elle a dirigé ses actions vers la consultation de son comité citoyen et a lancé une consultation publique ouverte à tous les acteurs afin d'étudier les différents scénarios possibles afin de se conformer aux dispositions du Reg. EEDS.

Comité citoyen. La DNS a mobilisé son comité citoyen fin 2024 afin de recueillir les positions des citoyens sur les règles et conditions à mettre en œuvre pour permettre une bonne utilisation des données de santé tout en générant la confiance[232]. Ce comité citoyen a réuni pendant plusieurs weekends une trentaine de personnes représentatives de la population française. Les 52 recommandations formulées ont été présentées publiquement à l'occasion des 4ème assises Citoyennes du numérique en santé[233] et ont vocation à être reprises dans les orientations prises par le gouvernement pour se conformer au Reg. EEDS.

Les grandes thématiques de ces 52 recommandations sont les suivantes : propositions pour minimiser les risques identifiés concernant les données de santé, la nécessité d'une information facile à comprendre, transparente et accessible à tous, l'enjeu d'un dispositif simple et ergonomique permettant à chaque personne de décider de l'usage par des tiers de ses données de santé, le rôle des citoyens dans la gouvernance fonctionnelle et dans la définition de l'éthique de l'utilisation des données de santé (aux échelles locale, nationale et européenne) et la question de l'environnement, de l'utilisation des ressources et de la consommation d'énergies associée à la gestion des données de santé.

Des propositions particulièrement intéressantes sont à souligner : tout d'abord, afin de mettre en place un système de gouvernance inclusive, les recommandations ont été formulées en prenant en considération les différentes échelles qui sont impliquées dans ce sujet (allant de l'échelle locale à l'échelle européenne). Également, sur l'invitation à faire évoluer les modalités d'information et d'exercice des droits, les citoyens plaident

[232] Ministère du travail, de la santé, des solidarités et des familles, Délégation au numérique en santé, *Avis du Comité citoyen du numérique en santé*, saison 3, octobre-novembre 2024. Disponible ici.

[233] 4èmes Assises citoyennes du numérique en santé « Découvrez les préconisations du Comité citoyen à propos du règlement européen des données de santé », 22 janvier 2025. Disponible ici.

pour s'appuyer notamment sur Mon Espace Santé pour l'utilisation secondaire des données de santé, sur l'élaboration de vidéos explicatives pour comprendre les enjeux liés à l'utilisation des données, mais aussi sur la mise en place de questionnaires et sondages auprès des citoyens pour évaluer leur compréhension des mécanismes de droit de refus prévu par le Reg. EEDS en matière d'utilisation secondaire des données de santé. Il est aussi demandé de rendre la terminologie utilisée plus accessible en n'utilisant notamment plus d'anglicismes comme « opt-out » pour mentionner le droit de refus, et en simplifiant les expressions d'utilisation primaire et d'utilisation secondaire. L'éthique est considérée comme un véritable garde-fou par les citoyens puisqu'ils proposent notamment de rendre obligatoire la constitution d'un comité scientifique et éthique pour chaque entrepôt de données de santé et en centralisant les décisions rendues par l'ensemble de ces comités scientifiques et éthiques. A l'échelle européenne, une recommandation a été faite préconisant la création d'un Comité Ethique Européen qui pourrait avoir des missions de contrôle et d'audit. Ce comité pourrait se positionner en tant qu'interlocuteur que les citoyens pourraient interpeller. Enfin, les enjeux liés à l'impact environnemental de la mise en place de cet Espace européen des données de santé ont également été mis en avant.

Ces recommandations ont à ce sujet déjà été reprises par la DNS dans son travail de réflexion sur l'intégration des dispositions du Reg. EEDS dans le droit français (voir ci-dessous).

Concertation sur le Règlement relatif à l'Espace européen des données de santé. En anticipation des dispositions législatives au niveau national qui devront être adoptées d'ici mars 2027 dans le cadre de l'entrée en application du Reg. EEDS, la DNS a mis en place une consultation publique[234] visant à commenter 15 fiches thématiques basées sur 3 grandes thématiques (utilisation primaire, utilisation secondaire et gouvernance). L'objectif est de recueillir l'avis des acteurs concernés sur les scénarios envisagés par la DNS pour lesquels les Etats membres ont une certaine marge de manœuvre pour appliquer les dispositions du règlement. Afin d'illustrer le propos, les fiches sur l'utilisation secondaire portent sur la transparence et les droits des personnes, l'organisation des détenteurs de données, les redevances et le périmètre des données visées et les enjeux éthiques liés à la réutilisation des données de santé. La consultation était ouverte du 28 avril au 30 mai 2025 et a recueilli 173 contributions, confirmant l'intérêt des acteurs à être associés à l'élaboration du cadre normatif auquel ils seront soumis. Une partie de ces retours ont été discutés en mai avec les acteurs de terrain à l'occasion de l'évènement SantExpo qui réunit les acteurs du système de santé.

Conclusion

Les mécanismes de consultation mis en place dans le cadre de l'élaboration de cette stratégie démontrent une volonté des acteurs de participer à l'élaboration des priorités et normes qui encadreront leurs activités. Ces mécanismes participent à fluidifier l'entrée en application du Reg. EEDS, qui aura d'importantes conséquences pour l'activité des acteurs concernés. Ces efforts de consultation emportent aussi comme effet positif une première confrontation des acteurs au texte du règlement, leur permettant de réfléchir leurs activités au regard du futur cadre et système dans lesquels ils devront s'inscrire. Nous pouvons espérer que ces efforts de consultation seront institutionnalisés dans le système de gouvernance qui sera préconisé et adopté par la stratégie d'utilisation secondaire des données de santé française ; en considérant les acteurs locaux afin de valoriser l'expertise des initiatives existantes.

[234] Agence du Numérique en santé, Concertation sur le Règlement relatif à l'Espace européen des données de santé, concertation ouverte du 28 avril au 30 mai 2025. Disponible ici.

CNIL, RÉFÉRENTIELS SANTÉ. Retour sur les contributions reçues dans le cadre de la consultation publique, 10 décembre 2024

La Commission nationale de l'informatique et des libertés (CNIL) présente les résultats de sa consultation publique menée auprès des acteurs de la santé au sujet de la mise à jour et mise en cohérence de ses **référentiels en matière de données de santé**. Ces derniers sont des cadres de référence définissant les bonnes pratiques pour traiter les données de santé en conformité avec le RGPD. Il en existe deux types : les référentiels dits « de droit souple » (et guides pratiques) et les référentiels s'appliquant aux traitements soumis à autorisation. Les premiers facilitent la mise en conformité de l'organisme concerné par le(s) traitement(s) de données sans toutefois avoir une force contraignante, tandis que le respect des seconds dispense ledit organisme des formalités de demande d'autorisation auprès de la CNIL de telle sorte qu'il n'a qu'à effectuer une simple déclaration de conformité auprès de cette dernière. Néanmoins, à la suite de l'entrée en vigueur de plusieurs règlements européens (« essais cliniques »[1] et dispositifs médicaux) et compte tenu du déploiement du numérique et de l'intelligence artificielle (IA) dans les services de soins de santé, **leur actualisation est devenue une nécessité.**

Ouverte jusqu'au 12 juillet 2024, la première phase de cette **consultation publique** visait à recueillir les retours des parties prenantes sur l'utilisation et l'efficacité des référentiels, ainsi qu'à identifier les besoins d'évolution face aux nouvelles pratiques et technologies. Environ 140 entités – établissements de santé (30 participants), organismes de recherche (28), syndicats professionnels et fédérations (15), éditeurs de logiciels (14), avocats spécialisés (13), institutions publiques (9) et autres contributeurs anonymes (5) – y ont participé, une telle diversité de profils reflétant l'importance que tous les acteurs attachent à la protection des données et à l'évolution de ces référentiels. Parmi les axes de travail prioritaires identifiés par la CNIL elle-même, concernant la mise à jour des méthodologies de référence (MR), trois sujets majeurs se sont démarqués : la possibilité d'apparier les données, notamment avec celles du Système national des données de santé (SNDS) ; l'aménagement des modalités d'information des personnes concernés et ; l'extension des destinataires des données administratives et de santé. L'inclusion de nouvelles catégories de données, comme les enregistrements vocaux ou vidéo et les données géographiques, ainsi que la mise en place d'éléments de décentralisation et de dématérialisation (suivi des patients à domicile, contrôle qualité à distance, consentement électronique, téléconsultation), sont également citées comme étant des priorités (« priorité n°2 » et « priorité n°3 »). Par ailleurs, des besoins liés aux outils de conformité et à l'intelligence artificielle ont émergé et devraient aussi bénéficier d'un groupe de travail. À la suite de cette consultation, la CNIL a prévu de constituer des **groupes de travail** dès le premier semestre 2025. Ces groupes travailleront collectivement sur l'élaboration des nouveaux référentiels santé de la CNIL, en collaboration avec la Plateforme des données de santé (ou *Health Data Hub*) et les autres acteurs concernés.



VEILLE CONTENTIEUSE

Le Conseil d'État rappelle la **marge d'appréciation** dont dispose la CNIL dans le choix des mesures correctrices en cas de manquement au RGPD, en l'occurrence, le défaut de recueil effectif du consentement pour le **traitement de données de santé**.

Conseil d'État, 10ème chambre, 12 juillet 2024, n° 488687, ECLI:FR:CECHS:2024:488687.20240712

CONSULTATION PUBLIQUE

La CNIL lance une **consultation publique sur son projet de recommandation relative au dossier patient informatisé (DPI).** Le projet est divisé en 14 fiches proposant de concert des analyses juridiques et techniques. Les contributions des professionnels du domaine étaient attendues jusqu'au 16 mai 2025.

Arrêté du 12 décembre 2024 modifiant l'arrêté du 24 décembre 2019 portant approbation du référentiel relatif à l'identifiant national de santé, *JORF* n° 0294 du 13 décembre 2024.

Cet arrêté publié au Journal officiel le 13 décembre 2024 annule et remplace la version 2.0 du Référentiel de l'Identité Nationale de Santé (INS) publiée en annexe de l'arrêté du 27 mai 2021[235]. Cette mise à jour de l'INS du patient (V2.1 – 2023), son identité de référence auprès de l'ensemble des professionnels de santé, vise à renforcer l'identification fiable et rigoureuse des patients et à simplifier la gestion et les échanges de données, tout en s'adaptant aux évolutions technologiques, tel que le déploiement de l'appli « carte Vitale » qui portera l'INS de l'usager.
Voici les principales modifications apportées : clarification sur le lieu de naissance (matricule INS), récupération de l'INS désormais possible via l'application « carte Vitale » (exigence n° 10), inclusion obligatoire de la liste complète des prénoms et du lieu de naissance lors des échanges de données (exigence n° 15).

[235] Arrêté du 27 mai 2021 portant approbation des modifications apportées au référentiel « Identifiant national de santé », *JORF* n° 0131 du 8 juin 2021.

Aperçu général sur le Ségur du numérique en santé

Dans le cadre du Ségur Numérique en santé, l'État français met en œuvre un programme de financement destiné à encourager l'équipement numérique des acteurs de l'offre de soins en solutions logicielles en vue de généraliser le partage fluide et sécurisé des données de santé. Il constitue un formidable accélérateur pour mettre le numérique au service de la santé, avec des ambitions fortes pour permettre aux professionnels de santé de mieux prévenir, mieux soigner et mieux accompagner.

La **vague 1 du Ségur Numérique,** qui s'est achevée au mois de septembre 2023, a eu pour objectif principal d'**alimenter « Mon espace santé »,** le carnet de santé numérique dont bénéfice chaque citoyen français pour stocker et partager, de manière sécurisée, ses données de santé. Elle a permis d'équiper une large majorité d'établissements et professionnels de santé (hôpitaux, médecine de ville, imagerie et biologie).

La **vague 2 du Ségur Numérique** vient compléter le socle de la vague 1 pour faciliter la consultation de l'information disponible dans « Mon espace santé » et l'intégration des documents médicaux reçus par MSSsanté, tout en renforçant la sécurité des logiciels. Lancée d'abord pour les établissements hospitaliers en mai 2024, avec le déploiement des dispositifs Dossier Patient informatisé (DPI)[236] et Plateforme d'intermédiation (PFI)[237], cette seconde vague se poursuivra avec le lancement de dispositifs dédiés aux secteurs de l'imagerie médicale et de la médecine de ville ainsi qu'aux officines, biologistes, chirurgiens-dentistes, sages-femmes et professionnels paramédicaux.



[236] Arrêté du 16 mai 2024 relatif à un programme de financement destiné à encourager l'équipement numérique des structures hospitalières - Fonction « Dossier patient informatisé » Vague 2, *JORF* n° 0116 du 19 mai 2024.

[237] Arrêté du 16 mai 2024 relatif à un programme de financement destiné à encourager l'équipement numérique des structures hospitalières - Fonction « Plateforme d'intermédiation » Vague 2, *JORF* n° 0116 du 19 mai 2024.

LE SÉGUR DU NUMÉRIQUE DANS LE SOCIAL & MÉDICO-SOCIAL : clôture de la Vague 1

Lors du lancement de la **vague 1** du Ségur du numérique en santé, un financement de 630 millions d'euros avait été annoncé spécifiquement pour l'ensemble du secteur social et médico-social. L'objectif visé est d'équiper les établissements et services sociaux ou médico-sociaux (ESSMS) du « Dossier Usager Informatisé » (DUI). Interopérable et communicant, également compatible avec Mon espace santé, ce logiciel centralise toutes les informations administratives, socio-éducatives, médicales et paramédicales de la personne accueillie ou accompagnée. Il offre ainsi la possibilité de recueillir toutes les données et écrits professionnels utiles pour rendre compte des soins d'un usager, facilitant par la même la conception, la mise en œuvre et l'évaluation de plans personnalisés d'accompagnement.

Deux programmes de financement ont été mis en place à cette fin :

- le **programme ESMS**, pour financer l'acquisition (ou le renouvellement) d'un DUI et,
- le **programme SONS**, lequel est un mécanisme d'achat par l'État pour le compte des ESSMS qui disposent déjà d'un DUI. Cette « prestation Ségur » financée par l'État, couvrant six dimensions dont l'octroi au Client final des droits d'utilisation du DUI, l'installation, la configuration et le paramétrage de cette solution logicielle ainsi que les éventuels frais de maintenance, est précisée dans l'annexe 3 de l'arrêté du 2 février 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS)[238].



C'est en référence à cette annexe que les **trois arrêtés publiés le 18 décembre 2024** introduisent « une date limite de fin des prestations Ségur [éligibles au dispositif SONS] » et « reporte[nt] la date de clôture du guichet de financement de la vague 1 » dans les ESSMS du domaine de la protection de l'enfance, des personnes en difficultés spécifiques et pour les acteurs de l'aide et du soin à domicile, prévue initialement le 19 décembre 2024. Ils précisent en outre « les modalités de règlement de la prestation Ségur par le client final » et ajoutent « une interdiction d'annulation des commandes SONS après le dépôt des demandes de financement (solde) auprès de l'Agence de services et de paiement ». Enfin, ils « modifie[nt] les conditions de versement du solde de la prestation Ségur pour prendre en compte l'ajout de la date limite de fin des prestations Ségur ».

Arrêté du 12 décembre 2024 modifiant l'arrêté du 7 septembre 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour le domaine protection de l'enfance » – Vague 1, *JORF* n° 0298 du 18 décembre 2024

Arrêté du 12 décembre 2024 modifiant l'arrêté du 2 février 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour les domaines personnes âgées, personnes en situation de handicap et acteurs de l'aide et du soin à domicile » – Vague 1, JORF n° 0298 du 18 décembre 2024

Arrêté du 12 décembre 2024 modifiant l'arrêté du 16 août 2022 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements et services sociaux ou médico-sociaux (ESSMS) – Fonction « Dossier usager informatisé pour le domaine personnes en difficultés spécifiques » – Vague 1, *JORF* n° 0298 du 18 décembre 2024

[238] *JORF* n° 0227 du 30 septembre 2022.

LE SÉGUR DU NUMÉRIQUE POUR LES SPÉCIALISTES DE L'IMAGERIE : lancement de la vague 2



Les dispositifs DRIMbox et RIS : des outils essentiels pour l'imagerie médicale

Deux arrêtés publiés au Journal officiel participent respectivement au financement de la passerelle d'images médicales **DRIMbox** et des systèmes d'information de radiologie (**RIS**), deux dispositifs qui s'inscrivent dans le cadre de la vague 2 du volet numérique du Ségur de la santé.

Les financements prévus s'adressent aux établissements de santé, ainsi qu'aux médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale.

- **DRIMbox** est un logiciel de partage des images médicales, qui s'inscrit dans le projet DRIM-M (*Data Radiologie d'Imagerie Médicale & Médecine Nucléaire*). Celui-ci ambitionne de créer un réseau unique et national de diffusion des examens d'imageries au patient et au professionnel : le réseau DRIM-M.
  Concrètement, chaque service et cabinet de radiologie connectera son PACS (*Picture Archiving and Communication System*) à ce réseau via une plateforme nommée « DRIMbox ». La DRIMbox alimentera en images le Dossier Médical Partagé (DMP) des patients qui pourront les consulter depuis Mon espace santé (fonction source) et fournira aux professionnels la possibilité d'accéder à un examen provenant d'une autre structure à partir d'un lien reçu par messagerie MSSanté (fonction consommation).

- **RIS** est le logiciel métier du radiologue ou médecin nucléaire leur permettant de suivre les dossiers de leurs patients et l'avancée des examens, de planifier les rendez-vous et de produire les compte-rendu, de même que faciliter la communication entre radiologues et autres spécialistes.

Sans nul doute, l'intégration dispositifs DRIMbox et RIS apportent de nombreux **bénéfices aux professionnels de santé** : accès simplifié aux images médicales, consultation de l'historique des images médicales évitant notamment de refaire des examens redondants, visualisation des compte-rendu et images radiologiques réalisés n'importe où sur le territoire. Pour les patients, ils représentent aussi un véritable progrès en termes de **qualité et de rapidité des soins**. Grâce à l'accès immédiat et sécurisé aux images médicales, les délais d'attente seront susceptibles d'être réduits, favorisant une prise en charge plus rapide et, par conséquent, un diagnostic précoce et précis. La **continuité des soins** sera, elle, mieux garantie par le partage d'images entre les différents établissements.

Arrêté du 20 février 2025 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements, médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale – Fonction « partage d'images médicales » (= DRIMbox), *JORF* n° 0049 du 27 février 2025

Arrêté du 20 février 2025 relatif à un programme de financement destiné à encourager l'équipement numérique des établissements, médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale – Fonction « système d'information de radiologie » – Vague 2 (= RIS), *JORF* n° 0049 du 27 février 2025



Aperçu général sur les activités de télésurveillance médicales

La télésurveillance est un acte de télémédecine permettant à un professionnel médical – appelé « opérateur » – d'interpréter à distance les données nécessaires au suivi de son patient et, le cas échéant, de prendre des décisions relatives à sa prise en charge. Ces données sont collectées au moyen d'un dispositif médical numérique (DMN), lequel est mis à disposition dudit patient par un fournisseur de télésurveillance – appelé « exploitant ». Depuis le 1er juillet 2023, après neuf ans de phase d'expérimentation dans le cadre du programme ETAPES (Expérimentations de Télémédecine pour l'Amélioration des Parcours en Santé)[239], les activités de télésurveillance sont entrées dans le droit commun[240] et bénéficient à ce titre d'une prise en charge par l'Assurance maladie. Deux décrets publiés fin décembre 2022 encadrent les décisions relatives à cette prise en charge[241].

Conditions de prises en charge par l'Assurance maladie des activités de télésurveillance médicale

Pour être inscrites au remboursement, les activités concernées doivent être inscrites sur la liste des activités de télésurveillance médicale (LATM) prévue à l'article L. 162-52 du code de la sécurité sociale. Dans le cadre de sa demande d'inscription sur la LATM, l'exploitant peut choisir entre deux types d'inscriptions, selon que sa solution de télésurveillance médicale correspond à une ligne générique existante (inscription sous forme générique) ou non (inscription en nom de marque). Mais, dans tous les cas, l'inscription d'une activité de télésurveillance sur la liste est subordonnée l'obtention du marquage CE et d'un certificat de conformité au référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques[242]. L'intérêt de cette activité doit, en outre, être « supérieur[e] au suivi médical conventionnel ou [être] équivalent[e] à celui d'une activité de télésurveillance déjà inscrite »[243]. Cette inscription est finalement faite par arrêté du ministère du travail, de la santé, des solidarités et des familles.

La rémunération des exploitants et des opérateurs

La question des montants forfaitaires applicables à l'exploitant du DM permettant la télésurveillance ainsi qu'aux professionnels de santé réalisant l'activité de télésurveillance (« opérateurs ») est toujours précisée dans un second arrêté. Conformément aux dispositions de l'arrêté du 31 mars 2025[244], la rémunération des premiers est modulée selon le nombre de patients inclus en file active (de 1 à plus de 100 000 patients) et augmente selon le type de bénéfice apporté : intérêt organisationnel, impact sur la qualité de vie, impact sur la morbidité, et impact sur la mortalité (article 1). Pour les deuxièmes, deux tarifs mensuels sont appliqués : à 11 euros pour un « opérateur de niveau 1 » et à 28 euros pour un « opérateur de niveau 2 » (article 2)

---

[239] Prévu par l'article 36 de la loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale pour 2014 (1), *JORF* du 24 décembre 2013.

[240] Le passage à un remboursement de droit commun de la télésurveillance a été voté dans la loi de financement de la sécurité sociale (LFSS) pour 2022 (v. spéc. article 36 de la loi n° 2021-1754 du 23 décembre 2021 de financement de la sécurité sociale pour 2022 (1), *JORF* n° L 0299 du 24 décembre 2021). En outre, son entrée en vigueur initialement prévue en juillet 2022 a été décalée au 1er juillet 2023.

[241] Décret n° 2022/1767 du 30 décembre 2022 relatif à la prise en charge et au remboursement des activités de télésurveillance médicale, *JORF* n° 0303 du 31 décembre 2022 et décret n° 2022-1769 du 30 décembre 2022 relatif au contenu de la déclaration des activités de télésurveillance médicale aux agences régionales de santé, *JORF* n° 0303 du 31 décembre 2022.

[242] Conformément à l'arrêté du 22 février 2023 portant approbation du référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques, *JORF* n° 0053 du 3 mars 2023.

[243] Article 1, sous « Art. R. 162-74. II », du décret n° 2022/1767 du 30 décembre 2022 relatif à la prise en charge et au remboursement des activités de télésurveillance médicale, *JORF* n° 0303 du 31 décembre 2022.

[244] Arrêté du 16 mai 2023 fixant le montant forfaitaire de l'activité de télésurveillance médicale prise en charge par l'assurance maladie prévu aux II et III de l'article R. 162-95 du code de la sécurité sociale, ainsi que les modulations applicables à ces tarifs et la périodicité de leur révision, *JORF* n° 0118 du 23 mai 2023.

Inscription au remboursement du DMN de télésurveillance MyDiabby Healthcare pour le diabète gestationnel

Deux arrêtés publiés au Journal officiel (JO) le 31 décembre 2024 actent la prise en charge dans le droit commun du DMN de télésurveillance médicale MyDiabby Healthcare pour le diabète gestationnel non traité par insuline et en fixent le montant forfaitaire applicable par mois et par patient (50e). Déjà inclus dans l'expérimentation nationale ETAPES, ce logiciel contient deux interfaces, l'une destinée à l'équipe de télésurveillance l'autre dédiée aux patients. Son objectif est relativement simple : recueillir des paramètres destinés à surveiller à distances les résultats glycémiques des patients, avec l'émission d'alertes, notamment en cas de dépassement du seuil glycémique préalablement défini par le professionnel de santé. La date de fin de prise en charge est fixée au 1er juillet 2025.

Arrêté du 19 août 2024 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0199 du 22 août 2024

Arrêté du 19 août 2024 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0199 du 22 août 2024

Inscription au remboursement du DMN de télésurveillance Glooko XT pour le diabète gestationnel

Après MyDiabby Healhcare, c'est au DM numérique Glooko XT d'obtenir sa prise en charge dans la télésurveillance des patients ayant un diabète gestationnel non traité à l'insuline. Il s'avère que ce logiciel utilisé pour le suivi des données relatives au diabète par les personnes atteintes de diabète et leur équipe soignante présente un intérêt organisationnel équivalent au DM déjà inscrit sur la LATM dans l'indication retenue, soit en l'espèce, My Diabby Healthcare.

La télésurveillance est également prise en charge jusqu'au 1er juillet 2025, de même que le montant du fait technique assurant la rémunération de l'exploitant mettant à disposition ce DM de télésurveillance est fixé à 50 euros par patient et par mois.

Arrêté du 26 décembre 2024 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0309 du 31 décembre 2024

Arrêté du 26 décembre 2024 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0309 du 31 décembre 2024

Inscription au remboursement du DNM de télésurveillance Techcare pour le cancer

À la faveur de deux arrêtés publiés au Journal officiel, le logiciel Techcare de Cureety devient le deuxième DM numérique inscrit sur la LATM dans la surveillance des patients atteints d'un cancer sous traitement systémique. Il vient effectivement concurrencer Resilience Pro, premier DM ayant obtenu son inscription au remboursement fin 2023[245], pour la télésurveillance des adultes traités par traitements systémiques seuls, en combinaison, ou associés à une irradiation. Le montant forfaitaire technique applicable à l'exploitant est également précisé : entre 48, 43 euros et 50 euros par mois et par patient pour les cancers localisés, et entre 70, 20 euros et 73, 33 euros pour les cancers avancés ou métastatiques. Quant aux professionnels de santé réalisant la télésurveillance, le tarif de niveau 2 est appliqué, soit 28 euros par mois et par patient. Le DM est inscrit au remboursement pour trois ans.

[245] Arrêté du 24 novembre 2023 relatif à la prise en charge des activités de télésurveillance médicale en application de l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0275 du 28 novembre 2023 et arrêté du 24 novembre 2023 fixant le montant forfaitaire des activités de télésurveillance inscrites sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0275 du 28 novembre 2023.

Arrêté du 31 mars 2025 portant inscription d'activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0081 du 4 avril 2025

Arrêté du 31 mars 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0081 du 4 avril 2025

Inscription au remboursement du DNM de télésurveillance Satelio Cardio pour l'insuffisance cardiaque

Deux arrêtés publiés au Journal officiel (JO) le 1er avril 2025 inscrivent au remboursement le dispositif de télésurveillance de l'insuffisance cardiaque, Satelio Cardio, en nom de marque jusqu'au 1er juillet 2026. Il s'agit d'un logiciel prenant la forme d'une application web avec une interface destinée à l'équipe médicale et l'autre aux patients. Elle permet tout d'abord de collecter les données des patients via des questionnaires, analyse ensuite ces données en générant un score de l'état clinique des patients selon un algorithme, puis émet des alertes. Le forfait technique assurant la rémunération de l'exploitant a été fixé à 74,37 euros. Il tient compte de l'intérêt clinique de mortalité et de la file active mensuelle constatée de patients. Les opérateurs bénéficieront du tarif « opérateur de niveau 2 » (28 euros par mois).

Arrêté du 28 mars 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0087 du 1er avril 2025

Arrêté du 28 mars 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0087 du 1er avril 2025

Fin de la prise en charge du DNM de télésurveillance Moovcare poumon pour le cancer

Un arrêté publié au Journal officiel le 16 février 2025 met fin à la prise en charge du logiciel de télésurveillance Moovcare poumon (Sivan), qui a été le premier outil de télésurveillance remboursé de droit commun en France. La commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (Cnedimts) ayant émis un avis défavorable, le DM n'a pu être inscrit sur la LATM, et son inscription sur la liste des produits et prestations remboursables (LPP) en 2020 a expiré. La société israélienne Sivan a déjà déposé un recours devant le Conseil d'État afin de contester cette décision de radiation.

Arrêté du 14 février 2025 portant radiation d'un dispositif médical de la liste des produits et prestations remboursables prévue à l'article L. 165-1 du code de la sécurité sociale, *JORF* n° 0040 du 16 février 2025

Arrêté du 31 mai 2024 modifiant l'arrêté du 24 juin 2021 relatif à l'expérimentation de télésurveillance médicale des patients transplantés, *JORF* n° 0132 du 8 juin 2024

Cet arrêté modifie à la marge le cahier des charges de l'expérimentation sur la télésurveillance des patients transplantés, financée dans le cadre de l'article 51 de la LFFS pour 2018 et qui avait débutée en 2019 pour une durée initiale de 45 mois. Il prévoit notamment près de 350 000 euros de budget pour la prise en charge des forfaits associés pour la période de juin 2024 à janvier 2025.

La cybersécurité des établissements de santé financée grâce au programme CaRE

Les cybermenaces, définies comme « tout évènement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte au réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes », se multiplient d'une manière alarmante dans le secteur de la santé, ce qui peut être très certainement relié à l'augmentation de l'usage du numérique dans les établissements de santé, et donc de leur exposition aux risques de cyber-criminalité et cyber-malveillance. Au vu des conséquences graves sur les hôpitaux en termes de fonctionnement, de coûts et de prise en charge des patients, des programmes et des financements nationaux consacrés à la cybersécurité du système de santé ont été institués et sont désormais appliqués de façon énergique dans les établissements de santé. Le programme « Cyberaccélération et résilience des établissements » (CaRE) prévoit notamment un financement de 750 millions d'euros pour la période 2023-2027 au titre de la sécurisation des systèmes d'information des établissements hospitaliers. Ce programme est réparti entre quatre axes (1) Gouvernance et résilience ; 2) Ressources et mutualisation ; 3) Sensibilisation ; 4) Sécurité opérationnelle) et 20 objectifs dont la préparation et l'accompagnement des établissements à faire face aux cybermenaces (3), la mise en place d'équipes techniques (6), leur sensibilisation aux risques cyber (9) ainsi que le fait de disposer d'une équipe chargée des opérations de contrôle pour vérifier l'atteinte des objectifs par les établissements de santé pour tous les domaines prioritaires du programme CaRE (17)[246]. Cependant, le financement de ce programme n'est assuré que jusqu'à la fin de l'année 2024, ce qui soulève des inquiétudes sur la durabilité des efforts engagés et la capacité des établissements à maintenir un haut niveau de sécurité au-delà de cette échéance. En outre, à partir de 2028, une fois le programme CaRE terminé, le besoin de financement des établissements de santé pour assurer un niveau élevé de cybersécurité perdurera d'autant plus que la directive européenne SRI 2 (NIS 2)[247], adoptée le 12 décembre 2022 et toujours en cours de transposition dans le droit français, renforcera les exigences en matière de cybersécurité, et s'appliquera à un périmètre d'établissements de santé beaucoup plus large qu'aujourd'hui[248].





[246] Rapport de la Délégation ministérielle au numérique en santé (DNS), *Le plan d'action pour protéger nos établissements de santé*, Décembre 2023.

[247] Directive n° 2022/2555/UE 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 n° 910/2014/UE et la directive n° 2018/1972/UE, et abrogeant la directive n° 2016/1148/UE (directive SRI 2), *JOUE* n° L 333 du 27/12/2022.

[248] Les établissements de santé qui relèvent du champ d'application de cette directive sont appelés à être classés comme « entités essentielles » ou « entités importantes », « en fonction de la mesure dans laquelle [ils] sont critiques au regard du secteur ou du type de service qu'[ils] fournissent, ainsi que de leur taille » (considérant 15 de la directive SRI 2, *op. cit.*).

Cour des comptes, Observations définitives. La sécurité informatique des établissements de santé : un renforcement récent et à poursuivre, face à la multiplication des cyberattaques, Octobre 2024

Ce rapport de 80 pages fait la synthèse des cinq années de financement du programme CaRE, visant à soutenir la sécurité informatique des établissements de santé. D'emblée, celui-ci souligne l'augmentation significative des cyberattaques contre les établissements de santé entre 2019 et 2023, trop souvent victimes de rançonlogiciel ou d'une compromission de leurs systèmes d'information[249]. Selon la Cour des comptes, la complexité croissante des systèmes d'information hospitaliers, qui peuvent compter jusqu'à 1000 applications pour certains CHU, combinée à un sous-investissement chronique dans le numérique (1,7% du budget hospitalier contre 9% dans le secteur bancaire), l'obsolescence de plus de 20 % des équipements numériques[250] et une sensibilisation insuffisante du personnel, exposent particulièrement ce secteur. Or, on le sait, ces cyberattaques sont lourdes de conséquences[251], car elles perturbent le fonctionnement des services hospitaliers, pouvant entraîner la fermeture temporaire de services critiques, comme les urgences, la radiothérapie ou les laboratoires, ou exposer le patient ou le personnel au vol de données médicales et personnelles, sans doute le problème le plus dommageable pour la protection des données sensibles, et celui qui les expose aux risques d'usurpation d'identité et d'exfiltration de leurs données[252]. Lors d'attaques, les établissements de santé peuvent aussi être contraints de revenir à une gestion manuelle des processus, un tel « retour à l'utilisation du "papier et du crayon" »[253] entraînant sans conteste des retards et des risques accus pour les patients. Sans oublier de mentionner que les coûts pour un hôpital attaqué peut atteindre un montant considérable, 10 millions d'euros pour la gestion de la crise et jusqu'à 20 millions pour la perte de recettes d'exploitation[254].

Fort de ce constat et toujours pour améliorer la cybersécurité des établissements de santé, la Cour des comptes formule plusieurs **recommandations**.

Financer

Tout d'abord, elle préconise à la direction générale de l'offre de soins (DGOS) et à la Caisse nationale de l'assurance maladie (Cnam) deux séries de mesures répondant aux **besoins importants en financements** des établissements en matière de cybersécurité : la première invite à la création d'un groupe national d'expertise chargé d'évaluer les pertes financières en cas d'attaque majeure, la deuxième propose aux établissements les plus gravement affectés une dispense de codification a posteriori de leur activité médicale[255]. Elle recommande ensuite au secrétariat général des ministères sociaux (SGMAS) de « mettre fin à l'utilisation d'un fonds de concours pour le financement de la DNS [Délégation au numérique en santé] », et suggère à la DNS, à l'Agence du numérique en santé (ANS) et au SGMAS de tout mettre en œuvre pour mener le programme CaRE « à son terme », jusqu'en 2027 donc. La Cour des comptes insiste particulièrement sur la nécessité de pérenniser les financements prévus par ce programme et

[249] *Ibid.*, p. 14, spéc. encadré « Les attaques pouvant affecter un système d'information ».
[250] *Ibid.*, p. 22 et suivants.
[251] *Ibid.*, p. 25 et suivants.
[252] *Ibid.*, p. 28.
[253] *Ibid.*, p. 26.
[254] *Ibid.*, p. 5 et 28 et suivants.
[255]

préconise la mise en place d'un cadre budgétaire pluriannuel intégrant des ajustements pour suivre l'évolution des risques numérique[256].

Auditer

Elle plaide aussi pour des **audits** périodiques obligatoires et harmonisés de cybersécurité dans tous les établissements de santé, « qui pourraient être pris en compte dans le dispositif d'incitation à la qualité et dans la certification par la HAS [Haute autorité de santé] ». De même, la part de budget que chaque établissement consacre à la cybersécurité et aux infrastructures numériques doit sensiblement augmenter, et cela en fixant des objectifs clairs de dépenses[257] et en assurant un suivi régulier de l'utilisation des fonds alloués[258].

Former

En outre, le rapport insiste sur l'importance du développement des compétences numériques. Des modules obligatoires de **formation** à la cybersécurité doivent être intégrés dès 2024 dans la formation initiale des professionnels de santé[259]. La mise en place de « programmes de sensibilisation plus interactifs et personnalisés »[260] sont également fortement recommandés en vue de garantir une culture de sécurité durable dans le secteur hospitalier, en fonction des menaces émergentes. Une solution adaptée peut consister à réitérer l'expérience des « parcours de cybersécurité » ayant renforcé la cybersécurité de l'État et des établissements de santé sur la période 2022-2011, grâce aux financements France Relance portés par l'Agence nationale de la sécurité des systèmes d'information (Anssi). Concrètement, ces parcours permettent d'atteindre un objectif de cybersécurité de façon progressive, en plusieurs étapes : - un pré-diagnostic permet de s'orienter vers le parcours de cybersécurité le plus adapté au contexte et au enjeux de sa structure ; - un temps d'accompagnement d'une durée d'environ trois mois consiste en une série de prestations standardisées s'achevant par l'élaboration d'un plan de sécurisation et de l'obtention d'un indice de cybersécurité ; enfin, la mise en œuvre opérationnelle des mesures de sécurisation[261].



[256] *Ibid.*, p. 40 et suivants.
[257] « [A]u plus tard en 2027, les établissements sanitaires consacre[ront] au moins 2 % de leur budget au numérique, dont 10 % sur la cybersécurité et les infrastructures, avec la mise en place d'un forfait numérique pérenne dans la tarification », v. Direction ministérielle au numérique en santé (DNS), *Feuille de route du numérique en santé 2023-2027. Mettre le numérique au service de la santé*, Mai 2023, p. 33.
[258] DNS, *Le plan d'action pour protéger nos établissements de santé, op. cit.*, p. 24.
[259] *Ibid.*, p. 60 et 61.
[260] *Ibid.*, p. 25.
[261] *Ibid.*, p. 51, spéc. note de bas de page n° 101.

Instruction n° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires, p. 57-61

Publiée au Bulletin officiel du 17 février 2025, cette instruction demande aux établissements de santé de mettre en œuvre sept actions « urgentes ou prioritaires » afin d'améliorer non seulement la sécurité de leurs systèmes d'information, mais également leur résilience en cas de cyber-attaques. Tout d'abord, au titre des « mesures prioritaires de renforcement demandées aux établissements de santé »[262], ces derniers devront réaliser, chaque année, un exercice de crise cyber (**action n° 1**) et, parallèlement, effectuer des « audits de sécurité de certaines infrastructures IT » (**action n° 3**). Ils devront également procéder à leur auto-évaluation « vis-à-vis des mesures cyber dites prioritaires » et, intégrer les « actions relatives à ces mesures dans le plan d'amélioration de la qualité de l'établissement » (**action n° 2**). Une autre mesure demandée par l'instruction est plus largement l'intégration du volet cyber « dans la qualité et la gestion des risques de l'établissement » (**action n° 5**). Les établissements sont en outre invités à « [s]e conformer aux référentiels d'identification et d'authentification », opposables depuis mars 2022 (**action n° 6**), et à calculer la part du budget qu'ils consacrent au numérique ainsi que le nombre d'équivalents temps plein (ETP) dédié à la cybersécurité (**action n° 7**). Par ailleurs, d'ici à la fin juin 2025, un plan de continuité (PCA) et un plan de reprise d'activité (PRA) devront être formalisés. Les établissements auront ensuite jusqu'à fin juin 2026 pour réaliser des bilans d'impact sur l'activité (BIA) pour l'ensemble des services critiques et services médico-techniques, puis juin 2027, pour le reste des services (**action n° 4**). Ces actions s'inscrivent dans le cadre du programme de cybersécurité CaRE, dans la continuité de la mise en œuvre de la directive SIR 1 (NIS 1)[263] et également dans la perspective de la mise en application de la directive SIR 2 (NIS 2)[264] dont les dispositions toucheront la grande majorité des établissements de santé

[262] *Ibid.*, p. 2.

[263] Directive n° 2016/1148/UE 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, *JOUE* n° L 194 du 19/07/2016.

[264] Directive n° 2022/2555/UE, *op. cit.*

Ministère de l'action publique et de la Fonction publique et de la simplification, *Plan de résilience des services publics face aux crises. Dossier de presse*, Avril 2025



Ce plan s'adresse à l'ensemble des agents du service public, y compris ceux relevant de la fonction publique hospitalière (FPH). Il vise à renforcer la capacité de l'administration française à se préparer à faire face aux situations de crises, ciblées principalement sur les réseaux de l'État (4 386 cyberattaques en 2024)[265]. Sa stratégie s'articule autour de deux axes forts : la sensibilisation et la formation des agents publics, d'une part, et la préparation opérationnelle des services, d'autre part.

Informer et sensibiliser les agents publics

Le travail de sensibilisation des agents publics aux enjeux de résilience consistera à :

- introduire dans la **formation initiale** de l'ensemble des écoles du service public des **modules** destinés à « acculturer les élèves à la notion de résilience individuelle et collective ». En matière de **formation continue**, les agents publics seront vivement invités à suivre **les modules de résilience** qui existent déjà ou seront créés, afin d'être formés à ce sujet d'ici 2028.
- diffuser à chaque agent un **livret de résilience** (« Tous résilients »), qui rappellera notamment les fondamentaux de la continuité d'activité, de la gestion de crise et des bons réflexes à adopter ;
- mettre en place chaque année, à partir de 2026, des **initiatives mémorielles** nationales et locales présentant des actes remarquables ou des lieux de mémoires, afin de contribuer au développement de l'esprit de défense.
- **sensibiliser** davantage les agents publics à la gestion des **cyber-risques**.

Préparer les services publics à faire face aux crises

Pour améliorer la préparation et la réponse des différents services et des agents aux situations de crise, il s'agira :

- d'actualiser, dès l'année 2026, et de tester annuellement les **plans de continuité d'activité (PCA) et de reprise d'activité (PRA)** dans l'ensemble des services. Chaque plan comprendra en outre un scénario cyber ;
- d'identifier les **services publics à renforcer prioritairement** en cas de crise et également les mesures à mettre en œuvre pour assurer leur accessibilité auprès de tous les publics, en particulier les plus fragiles ;
- d'accroître drastiquement **l'engagement des agents publics dans les dispositifs de réserve citoyenne**, en prévoyant par exemple de simplifier les démarches d'engagement ou une valorisation de la réserve dans les parcours professionnels.
- de **mieux intégrer les enjeux de cybersécurité** dans la préparation des services publics aux cyber-attaques, en s'assurant notamment que « les services publics dont la criticité le nécessite, disposent d'accès aux systèmes d'information ministériels de gestion de crise et de moyens de communication de résilience »[266].

[265] *Plan de résilience des services publiques face aux crises. Dossier de presse, op. cit.*, p. 6.
[266] *Ibid.*, p. 18.

Loi n° 2025-199 du 28 février 2025 de financement de la sécurité sociale pour 2025 (1), *JORF* n° 0051 du 28 février 2025

La loi de financement de la sécurité sociale (LFSS) pour 2025, qui compte 103 articles, comprend plusieurs mesures relatives au numérique en santé.

Le renforcement de la lutte contre les plateformes numériques délivrant, par téléconsultation, des arrêts de travail – article 54

L'**article 54** de la LFSS complète, en ce qui concerne la lutte contre les plateformes de délivrance d'arrêts de travail en ligne, l'article L. 6316-1 du code de la santé publique qui définit la télémédecine comme « une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication [,] mett[ant] en rapport un professionnel médical (…) avec le patient ». Il prévoit explicitement deux interdictions : l'une à l'encontre des fournisseurs de service en ligne désireux de mettre en place des plateformes numériques ayant pour but de prescrire ou de renouveler, par téléconsultation, des arrêts de travail, l'autre pour les professionnels de santé qui exercent à titre principal à l'étranger et prescrivent des arrêts de travail, quelle qu'en soit la durée. Le principal objectif de cette mesure est de mettre fin aux dérives de sites internet, souvent implantés à l'étranger, et qui proposent aux internautes la délivrance d'arrêt de travail en ligne clé en main. Le Parlement avait déjà, avec l'article 65 de la LFSS pour 2024, franchi une première étape en limitant la durée des arrêts de travail prescrits à l'issue d'une téléconsultation à un maximum de trois jours[267]. L'Assurance maladie et l'ordre des médecins prennent cette question très au sérieux et continuent de lutter activement contre ces plateformes en ligne dont l'activité principale est de fournir des arrêts maladie. Un exemple récent en est la décision de la chambre disciplinaire nationale (CDN) de l'ordre des médecins, rendue le 29 février 2024[268]. Le médecin fondateur de la plateforme de télémédecine « DocteurSecu » (www.docteursecu.fr), par le biais de laquelle il délivrait des arrêts maladie à la demande avant d'être contraint de la fermer par ordonnance du juge du 6 novembre 2020[269], a été sanctionné de deux ans d'interdiction d'exercer dont un avec sursis. Les juges disciplinaires ont notamment retenu un manquement aux dispositions interdisant aux praticiens d'exercer la médecine comme un commerce (article R. 4127-19 du code de la santé publique)[270].

[267] Sauf exception « lorsque l'arrêt de travail est prescrit ou renouvelé par le médecin traitant ou la sage-femme référente mentionnée à l'article L. 162-8-2 du code de la sécurité sociale ou en cas d'impossibilité, dûment justifiée par le patient, de consulter un professionnel médical compétent pour obtenir, par une prescription réalisée en sa présence, une prolongation de l'arrêt de travail », v. article L. 6316-1 du Code de la santé publique.

[268] Cette décision a fait l'objet d'un pouvoir devant le Conseil d'État, qui a été rejeté dans son ensemble par celui-ci (v. Conseil d'État, 4ème chambre, 31 juillet 2024, n° 493577, ECLI:FR:CECHS:2024:493577.2024073).

[269] Tribunal judiciaire de Paris, 6 novembre 2020, n° 2054799.

[270] Au total, des manquements ont été relevés pour 10 articles du code de la santé publique: R4127-32 (qualité des soins), R4127-33 (diagnostic), R4127-76 (délivrance des certificats), R4127-28 (certificat de complaisance), R4127-53 (honoraires), R4127-19 (interdiction d'exercer la médecine comme un commerce), R4127-20 (usage du nom et de la qualité de médecin), R4127-3 (principes de moralité et de probité), R4127-31 (déconsidération de la profession) et R4127-83 (rédaction d'un contrat et transmission à l'ordre).

L'obligation pour les officines et les industriels de se doter d'un système d'information sur les ruptures d'approvisionnement de médicaments – article 76

L'**article 76** de la LFFS introduit une nouvelle obligation pour les pharmacies d'officine et les établissements pharmaceutiques dont le but principal est de mieux gérer les pénuries de médicaments : ils devront renseigner un système d'information sur la disponibilité des médicaments d'intérêt thérapeutique majeur. En cas de non-respect, des sanctions financières pourront être prononcées. Cette disposition propose même d'en confier le pilotage au Conseil national de l'ordre des pharmaciens, à travers l'utilisation de sa plateforme « DP-Ruptures ». Ce logiciel de gestion d'officine permet : - aux pharmacies d'officine et praticiens hospitaliers de signaler automatiquement les ruptures d'approvisionnement aux laboratoires exploitants qui utilisent ce service ; - aux laboratoires exploitants de consulter leur portefeuille de médicaments et d'apporter des réponses automatiques sur les ruptures d'approvisionnement remontées par les pharmaciens d'officine ; - aux grossistes-répartiteurs de consulter la liste des ruptures et les messages apportés par les laboratoires exploitants. Inutile de dire que cet outil améliore très nettement la circulation d'information entre les acteurs de la chaîne du médicament et facilite grandement la gestion des ruptures. Un décret et une convention viendront structurer son déploiement et imposer de nouvelles obligations aux pharmaciens comme aux industriels.

La prise en charge des DM numériques largement précisée – article 79

L'**article 79** de la LFSS modifie l'article L. 165-1-3 du code de la sécurité sociale, en précisant et en modifiant les modalités de recueil des données issues d'un DM numérique. D'une part, le recueil de telles données n'est désormais plus cantonné aux affections chroniques, ces mots, conformément à la deuxième ligne de cet article, étant « supprimés » du texte de l'article L. 165-1-3 du code de la sécurité sociale. D'autre part, leur utilisation est élargie à l'évaluation de la pertinence du dispositif, au-delà de la nécessité du traitement. Le deuxième alinéa de l'article L. 165-1-3 du code de la sécurité sociale est ainsi remplacé par l'alinéa suivant : « [c]es données [issues peuvent, avec l'accord du patient, être télétransmises au médecin prescripteur, au distributeur au détail et au service du contrôle médical [de l'assurance maladie]. Au regard de ces données, le prescripteur réévalue de façon régulière la pertinence et l'efficacité de sa prescription et le distributeur, en lien avec le prescripteur, engage des actions ayant pour objet de favoriser une bonne utilisation du dispositif médical ».

Concernant la prise en charge du dispositif médical ou sa modulation, celle-ci pourra dorénavant être subordonnée au respect de « conditions d'utilisation ». Il appartiendra alors à la commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (Cnedimts) de la Haute Autorité de santé (HAS) de se prononcer sur « les modalités selon lesquelles les données collectées s[eront] prises en compte ». Un décret en Conseil d'État précisera les conditions de transmission du distributeur à l'assurance maladie des données « permettant d'attester du respect d[e ces] conditions d'utilisation », après avis de la Commission nationale de l'informatique et des libertés (Cnil). Leur non-respect pourrait entraîner la suspension de la prise en charge s'il se prolonge au-delà d'une durée déterminée par décret. Si c'était le cas, le distributeur au détail et le prescripteur en seraient informés « sans délai ». Il est précisé, en outre, qu'en cas de refus opposé par le patient quant à la transmission de ses données d'utilisation, « le dispositif médical ne [pourra] faire l'objet d'une prise en charge ou d'un remboursement. Le défaut de transmission des données du fait du distributeur au détail est [en fait] inopposable au patient ». Enfin, l'article 79 de la LFSS prévoit que le distributeur devra signaler, au moment du recueil de l'accord du patient pour la transmission de ses données d'utilisation, que les données transmises peuvent le conduire à ne pas renouveler sa prescription s'il la juge non pertinente « au regard notamment de la faible utilisation du dispositif ».

Les mesures du numérique en santé censurées par le Conseil Constitutionnel

La LFSS pour 2025 a été publiée le 28 février 2025, quelques heures après la décision de non-conformité partielle rendue par le Conseil constitutionnel. Dans sa décision, il censure 14 articles dont plusieurs dispositions relatives au numérique en santé.

L'instauration de la « taxe lapin » – article 52

L'article 52 visait à instaurer une pénalité pour les patients n'honorant pas leurs rendez-vous médicaux, par l'insertion d'un nouvel article L. 1111-3-4-1 au sein du code de la santé publique. Surnommée « taxe lapin », cette caution financière était exigée par les établissements de santé, services de santé, centres de santé ou professionnels de santé exerçant à titre libéral, dans le cas où un de leurs patients ne se présentait pas à une consultation ou lorsqu'il annulait le rendez-vous sans respecter un délai de prévenance raisonnable. En somme, on attendait de la structure ou du professionnel de santé concerné non seulement qu'il informe au préalable son patient de l'application éventuelle de cette pénalité, mais aussi qu'il lui rappelle la date et l'horaire de ce rendez-vous au moins une fois. Une pré-autorisation bancaire était en outre requise pour permettre le paiement de cette pénalité. Si le Conseil constitutionnel ne remet pas en cause le principe d'une telle pénalité qui participe bien d'un objectif d'intérêt général – à savoir, « dissuader les comportements de patients qui n'honorent pas leurs rendez-vous médicaux et améliorer ainsi la possibilité pour les professionnels de santé de prendre en charge l'ensemble des patients en temps utile »[271], il considère cependant qu'« en s'abstenant de définir lui-même [s]a nature (…) d'encadrer son montant ainsi que les conditions de sa mise en œuvre »[272], le législateur ne l'a pas assez encadrée. Selon lui, en outre, « en subordonnant la prise d'un rendez-vous médical à la possibilité pour le professionnel ou l'établissement de santé d'exiger une telle caution financière, ces dispositions pourraient conduire à ce que des patients dont l'état de santé le nécessite se voient refuser l'accès à une consultation médicale en raison de leur situation financière »[273]. Toutes ces raisons font que le législateur a privé de garanties légales les exigences constitutionnelles découlant du onzième alinéa du Préambule de la Constitution de 1045, qui garantissent le droit à la protection de la santé. Dès lors, l'article 52 est contraire à la Constitution.

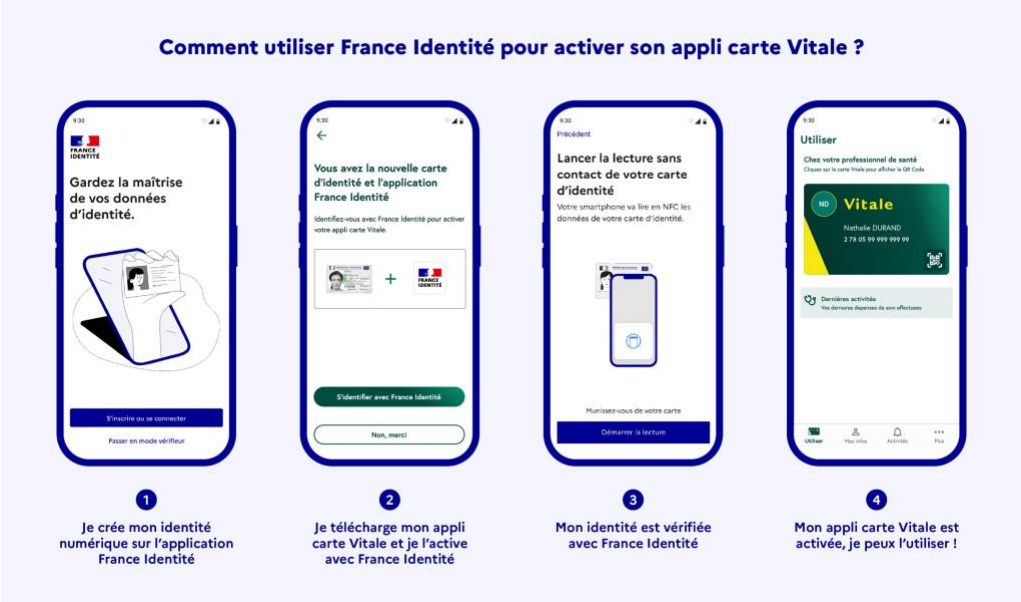
Conseil Constitutionnel, Décision du 28 février 2025 n° 2025-875 DC

[271] Point 41 de la décision du Conseil constitutionnel, *op. cit.*

[272] *Ibid.*, point 42.

[273] *Ibid.*, point 38.

La généralisation de l'application Carte Vitale - article 50



Le Conseil constitutionnel a également censuré l'**article 50**, qui prévoyait la généralisation de la carte Vitale dématérialisée sur l'ensemble du territoire au 1er octobre 2025. Cette mesure de modernisation du système de santé visait plusieurs objectifs : renforcer la sécurisation des échanges de données de santé, simplifier les démarches des assurés et lutter contre la fraude aux prestations. Concrètement, chaque assuré social devait pouvoir présenter sa carte Vitale via l'application carte Vitale (ApCV) installée sur son smartphone, en alternative à la carte physique traditionnelle ou aux feuilles de soins papier. Pour garantir la sécurité du dispositif, son activation nécessitait l'identité nationale de santé (INS) de l'assuré, à savoir sa carte d'identité électronique (CNIe), permettant une vérification d'identité réalisée directement via l'application France Identité numérique.

L'article prévoyait également des incitations financières pour les professionnels de santé afin de les encourager à s'équiper (lecteur QR code, mise à jour des logiciels métier) et à accepter cette carte dématérialisée. Pour le Conseil constitutionnel, ces dispositions « ne trouvent pas leur place dans une loi de financement de la sécurité sociale »[274]. Autrement dit, il juge que la généralisation de la carte Vitale dématérialisée n'avait pas un impact suffisamment direct sur les dépenses sociales pour figurer dans un texte d'équilibre financier de la Sécurité sociale. Il s'agit d'un cas typique de « cavalier social », à savoir : une disposition étrangère au domaine des LFSS[275]. Le déploiement de l'application carte Vitale (ApCV), déjà expérimenté dans 23 départements, est alors reporté, nécessitant un texte législatif spécifique pour permettre son adoption dans un autre cadre législatif.



[275] V. à ce sujet, Jean-François CALMETTE, « Les "cavaliers sociaux" dans la jurisprudence du Conseil constitutionnel : une autonomie à petit trot », *Revue française de droit constitutionnel*, vol. 1, n° 61, 2005, p. 171-188.

L'accélération du déploiement du Dossier Médical Partagé (DMP) – article 53

L'**article 53,** qui modifie l'article L. 162-14-1 du code de la sécurité sociale encadrant les conventions conclues entre professionnels de santé libéraux et assurance maladie, est aussi censuré. Cet article incitait ces derniers à utiliser le dossier médical partagé (DMP), car il introduisait la possibilité d'inclure dans ces conventions « les conditions de modulation de l[eur] rémunération, à la hausse ou à la baisse, (…) en fonction de la consultation et du renseignement du dossier médical partagé »[276]. Il existait aussi des mesures d'incitation à l'utilisation du DMP applicables aux établissements de santé, le « développement du numérique, la consultation et le renseignement des dossiers médiaux partagés des patients »[277] y étant érigé au rang des indicateurs clés du dispositif de financement à la qualité de ces établissements (dispositif IFAQ – incitation financière à l'amélioration de la qualité). Mais comme précédemment, le Conseil estime que cette disposition constitue un cavalier social, sans lien avec une LFFS, d'où sa censure pour des motifs de procédure.

DMP LE DOSSIER MÉDICAL PARTAGÉ

[276] Article 16 *bis* E (nouveau), numéro 3 du Projet de loi de financement de la sécurité sociale pour 2025 (PLFSS), Session ordinaire 2024-2025, texte n° 29 adopté par le Sénat le 26 novembre 2024,
[277] *Ibid.*, article 16 *bis* E (nouveau), numéro 4.

Droit belge

Arrêté royal du 15 décembre 2024 sur l'accès aux données de santé, M.B du 19 décembre 2024

L'arrêté royal publié au Moniteur belge du 19 décembre 2024 met en œuvre deux dispositions consacrées par la loi du 22 avril 2019 relative à la pratique qualitative des soins de santé (ci-après « loi Qualité »), qui traitent respectivement du consentement éclairé du patient pour permettre l'accès à ses données de santé (article 36) et des catégories de professionnels de santé qui, bien qu'ayant une relation thérapeutique avec le patient, n'ont pas accès à l'échange des données de santé (article 37).

Mise en œuvre de l'article 36 et précisions des règles applicables au consentement éclairé du patient au partage des données de santé

L'article 36, premier alinéa, de la loi Qualité prévoit que, pour avoir accès aux données de santé d'un patient qui sont détenues et conservées par d'autres professionnels de soins, un professionnel de santé doit préalablement obtenir le consentement éclairé du patient en question. Le présent arrêté royal établit en détail les règles supplémentaires pour l'obtention de ce consentement éclairé au partage des données, qui représente une « modalité essentielle [du] traitement spécifique de données à caractère personnel au sens du RGPD ». Son approche vise à atteindre un équilibre entre les objectifs suivants :

1) « garantir le droit à l'autodétermination du patient », en vertu duquel le patient choisit librement son prestataire de soins, décide librement des soins préventifs et curatifs qui lui sont proposés, et donne son consentement éclairé « uniquement pour le partage d'informations [structurées et] pertinentes » le concernant ;

2) « garantir des soins de qualité, intégré, continus, accessibles et sécures pour le patient », via une coopération multidisciplinaire entre tous les prestataires de soins de santé ayant une relation thérapeutique avec le patient. Il est important que ces derniers puissent consulter les données disponibles sur le patient (antécédents médicaux, facteurs de risque, résultats des examens précédents, calendrier des médicaments, statut vaccinal) ou en ajouter de nouvelles, cela pour des raisons de continuité, de qualité et de sécurité.

3) « éviter les charges ou formalités administratives inutiles », notamment la création et la conservation de documents formels (électroniques) et la saisie et le stockage multiples d'informations.

Dans ce contexte, il est précisé que le consentement éclairé peut être donné verbalement ou par écrit, mais uniquement à condition que le patient ait été correctement et suffisamment informé de la portée et du consentement éclairé visé à l'article 36, premier alinéa, de la loi Qualité. Il convient ainsi de l'informer à l'avance que « le partage de données n'a lieu que dans le but de [lui] fournir des soins de qualité, intégrés, continus, accessibles et sécures (…), et ne concerne que les informations pertinentes à cette fin ». S'il souhaite alors donner son consentement

éclairé au partage des données, il a le choix entre enregistrer son accord à l'échange de données directement sur la plate-forme eHealth[278], et demander à un prestataire de soins de le faire pour lui. Le patient dispose en outre du droit d'exclure de l'accès à ses données de santé un professionnel de la santé « nommément désigné », cette demande d'exclusion devant être introduite « dans le respect d'un délai de [préavis de] dix jours qui sont nécessaires au responsable du traitement pour s'organiser ».

Mise en œuvre de l'article 37 et désignation des catégories de professionnels de santé n'ayant pas accès aux données de santé

Faisant application de l'article 47, troisième alinéa, de la loi Qualité, cet arrêté royal désigne les catégories de professionnels de santé qui, bien qu'ayant une relation thérapeutique avec un patient, n'ont pas accès aux données de santé susceptibles d'être échangées. Il s'agit des professionnels de santé « chargés d'examiner le patient sans intention unique de préserver, de rétablir ou d'améliorer sa santé » et cela concerne des domaines tels que la médecine d'assurance, la médecine de contrôle et la médecine légale. Ces professionnels dont l'intervention vise uniquement à établir la santé n'ont donc pas accès aux données de santé détenues et conservées par les professionnels de la santé chargés de préserver, de rétablir ou d'améliorer la santé du patient, sauf à ce qu'un cadre légal spécifique en décide autrement.

Décret du 21 novembre 2024 relatif à la simplification administrative et aux communications par voie électronique entre les usagers et les autorités publiques wallonnes (1), M.B du 19 décembre 2024

Le décret publié au Moniteur belge du 19 décembre 2024 introduit un certain nombre de nouveautés et remplace le décret du 27 mars 2017 relatif aux communications par voie électronique entre les usagers et les autorités publiques wallonnes[279].

Premièrement, il fixe un nouveau cadre aux communications électroniques entre l'autorité publique et l'usager, lesquelles ne doivent pas être imposées[280] ni empêcher le public visé par une démarche d'y avoir accès[281]. En d'autres termes, « [l]'autorité publique doit maintenir et garantir le développement de communication hors ligne »[282] tout en sachant, par ailleurs, que « l'efficacité juridique d'une communication ne peut pas être contestée au seul motif qu'elle ait été réalisée par voie électronique »[283]. Au-delà du principe d'équivalence entre la forme électronique et la forme papier que le législateur wallon avait déjà exposé à l'article 2 dans son précédent décret[284], il s'agit ici de préciser que l'autorité publique peut autoriser automatiquement la communication par voie électronique « dès lors qu'elle met à disposition de l'usager un moyen

[278] Conformément à son objectif d'offrir aux acteurs des soins de santé « une plate-forme de collaboration pour l'échange électronique de données sécurisé, y compris un système pour l'organisation et le logging des échanges électroniques de données, et un système d'accès électronique aux données », v. article 5, 4°, sous *b)*, de la loi du 21 août 2008 relative à la création et à l'organisation de la plateforme eHealth, M.B du 13 octobre 2008.
[279] M. B. du 15 avril 2014.
[280] Article 2, alinéa 1, du décret du 21 novembre 2024, *op. cit.*
[281] *Ibid.*, article 3, paragraphe 4.
[282] *Ibid.*, article 2, alinéa 2.
[283] *Ibid.*, article 3, paragraphe 1.
[284] Selon la formule suivante : « À défaut de disposition légale, décrétale ou réglementaire contraire, l'efficacité juridique d'une communication ne peut être contestée au seul motif qu'elle a été réalisée par voie électronique », v. décret du 27 mars 2017, *op. cit.* Cette disposition a été reprise fidèlement à l'article 3, paragraphe 1, du décret du 21 novembre 2024, *op. cit.*

électronique qui lui permet d'être contacté »[285] et que cette communication électronique présente les qualités fonctionnelles de la communication papier[286]. Il s'ensuit logiquement que le consentement libre, éclairé, spécifique et préalable de l'usager à recevoir uniquement des communications électroniques[287] est nécessaire. Qu'il soit global à une autorité publique ou spécifique à une démarche[288], ce consentement peut être retiré à tout moment[289] et surtout par voie non électronique[290]. Le décret précise en ce cas que « [d]ès réception du retrait du consentement, le traitement de la démarche se poursuit via le nouveau moyen de communication choisi par l'usager, excepté pour les communications électroniques en cours que l'autorité publique ne pourrait plus techniquement arrêter »[291]. Ce principe est toutefois posé sous réserve d'une exception légale ou décrétale contraire « démontrant que le résultat escompté d'une démarche ne peut en aucun cas être atteint si elle devait être réalisée par la voie papier »[292] ou en ce qui concerne les personnes morales qui peuvent se voir imposer la communication électronique[293].

Deuxièmement, ce décret impose aux autorités publiques une obligation générale de proposer, poursuivre et coordonner toutes mesures en vue de lutter contre la complexité et les contraintes administratives imposées aux usagers des services publics et d'en améliorer le service rendu à ces derniers. Pour ce faire, l'autorité publique est invitée à « mettre à disposition des outils qui favorisent l'administration électronique », à l'image du portail numérique du Service publique de Wallonie qui fait l'objet du chapitre suivant. En effet, l'article 8 donne une base juridique à la mise en place du portail wallon « Mon Espace », qui évoluera prochainement pour devenir « ma.Wallonie »[294]. Cette plateforme d'administration numérique permet aux usagers d'initier et de gérer facilement leurs démarches administratives et d'en suivre efficacement l'état d'avancement et, ainsi, de communiquer régulièrement avec les autorités publiques via leur espace « personnel citoyen » ou professionnel[295]. Il s'agit donc d'une sorte de « guichet unique [en ligne] au travers duquel chaque citoyen devra aisément être en mesure d'accéder à un catalogue de services au travers d'un processus d'authentification digital »[296].

Troisièmement, des mesures relatives à la lutte contre la fracture numérique sont prévues par le présent décret. Outre l'interdiction, sauf exception légale, pour l'autorité publique d'imposer la voie électronique à l'usager[297], il lui appartient également de garantir à chacun d'entre eux : « 1° un soutien à la réalisation en ligne de ses démarches administratives ; 2° des solutions technologiques rendant toute démarche administrative ou communication en ligne plus facilement accessible aux personnes en situation de handicap ; 3° la possibilité de réaliser les démarches administratives ou les communications autrement qu'en ligne en prévoyant pour ses usagers un accueil physique, un service téléphonique et un contact par voie postale »[298].

Quatrièmement, enfin, la possibilité pour toute autorité publique d'utiliser « l'eBox », à savoir ce service proposé par

[285] *Ibid.*, article 3, paragraphe 2.
[286] *Ibid.*, article 5, alinéa 1.
[287] *Ibid.*, article 4, paragraphe 1, alinéa 1.
[288] *Ibid.*, article 4, paragraphe 1, alinéa 2.
[289] *Ibid.*, article 4, paragraphe 2, 3°.
[290] *Ibid.*, 4°.
[291] *Ibid.*, article 4, paragraphe 3.
[292] *Ibid.*, article 2, alinéa 1.
[293] *Ibid.*, alinéa 3.
[294] V. à ce sujet, projet de décret du Parlement Wallon du 12 septembre 2024 relatif à la simplification administrative et aux communications par voie électronique entre les usagers et les autorités publiques wallonnes, Session 2024-2025, n° 1, 33(2024-2025), p. 3.
[295] Article 9, alinéa 2, 1°, du décret du 21 novembre 2024, *op. cit.*
[296] Projet de décret du Parlement wallon du 12 septembre 2024, *op. cit.*, p. 3.
[297] Article 2, alinéa 1, du décret du 21 novembre 2024, *op. cit.*
[298] *Ibid.*, article 13.

le service public fédéral compétent en matière d'Agenda numérique et l'Office nationale de sécurité sociale permettant aux utilisateurs d'échanger des messages électroniques avec, respectivement, des personnes physiques ou leurs représentants et les titulaires d'un numéro d'entreprise[299], est maintenue à l'article 7 du décret.

Le même jour : décret du 21 novembre 2024 relatif, pour les matières réglées en vertu de l'article 138 de la Constitution, à la simplification administrative et aux communications par voie électronique entre les usagers et les autorités publiques wallonnes (1), M. B. du 19 décembre 2024.

[299] Article 2, 3°, de la loi du 27 février 2019 relative à l'échange électronique de messages par le biais de l'eBox (1), M. B. du 15 mars 2019.

Droit espagnol

Real Decreto 922/2024, de 17 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual, « BOE » núm. 226, de 18/09/2024

Ce décret royal modifie le décret royal 183/2004, du 30 janvier 2004, relatif à la carte individuelle de santé (« tarjeta individual de sanidad (TSI) »)[300], pour y intégrer le développement du numérique en santé en prévoyant la délivrance, par les autorités sanitaires compétentes, d'une carte individuelle de santé dans un format dématérialisÉ (« *Tarjeta Sanitaria Virtual* ») en plus du support physique traditionnel utilisé jusqu'à présent (« *Tarjeta sanitaria individual en soporte físico* »). Cette nouvelle carte « virtuelle », valable dans l'ensemble du système national de santé (« Sistema Nacional de Salud (SNS) »)[301], aura la même validité que la carte physique[302], mais présentera, en outre, l'avantage de faciliter l'accès aux services de santé, notamment lors de déplacements dans d'autres communautés autonomes, dans des situations d'urgence ou en cas de perte de la carte physique, et de réduire en conséquence les coûts et les charges administratives liés à l'utilisation des cartes physiques[303]. Le QR Code (« código QR ») ainsi généré contiendra les mêmes informations de base (« *datos básicos comunes* »)[304] que la bande magnétique de la carte de santé physique[305], lesquelles sont nécessaires pour identifier sans ambiguïté et de manière univoque le titulaire de la carte de santé ainsi que ses droits aux soins afférents. Il sera en outre possible d'y ajouter d'autres données dites « additionnelles » (« adicionales »), telles que les coordonnées de la personne à joindre en cas d'urgence[306]. Fort de ce nouveau contexte numérique, les autorités sanitaires compétentes sont explicitement invitées à « *adopt[ar] los medios técnicos que sean precisos par posibilitar la lectura (...) del codigo QR* »[307] [« adopter les moyens techniques nécessaires pour permettre la lecture du QR code »].

[300] « BOE » núm. 37, de 12/02/2004.
[301] Artículo (article) 2, párrafo (paragraphe) 2, del Real Decreto 922/2024, *op. cit.*
[302] *Ibid.*, artículo 2, párrafo 3.
[303] *Ibid.*, 8ème apartado (alinéa) : « Finalemente, se cumple con el principio de eficiencia al no imponer cargas administrativas y racionalizar la gestión de los recursos públicos al mejorar la interoperabilidad de la tarjeta sanitaria individual » [« Finalement, il [le décret royal] répond au principe d'efficacité en n'imposant pas de charges administratives et en rationalisant la gestion des ressources publiques par l'amélioration de l'interopérabilité de la carte individuelle d'assurance maladie »].
[304] *Ibid.*, artículo 3, párrafos 1. V. aussi, le paragraphe 2 de l'annexe II du Real Decreto 922/2024, *op. cit.* (ANEXO II Especificaciones de la tarjeta sanitaria individual en soporte virtual).
[305] Artículo 3, párrafo 5, letra b), del Real Decreto 922/2024, *op. cit.*
[306] *Ibid.*, artículo 2, letra b), del ANEXO II, *op. cit.*
[307] Artículo 2, párrafo 7 del Real Decreto 922/2024, *op. cit.*

Droit de l'Union européenne

Reconnaissance de la qualité à agir des concurrents de l'auteur présumé d'une violation du RGPD : la Cour de justice fait le choix d'un régime renforcé de protection

par Joud GHARZEDDINE

Étudiante en Master 2 Juriste européen, Université Toulouse Capitole

Dans un arrêt rendu le 4 octobre 2024, la Cour de justice de l'Union européenne (ci-après « CJUE ») clarifie la portée du système de voies de recours établi par le règlement général de protection des données[308] (ci-après « RGPD ») ainsi que la notion de « données concernant la santé ».

L'affaire débute en Allemagne avec l'introduction par DR, une personne physique exploitant une pharmacie, d'une action en cessation devant les juridictions civiles allemandes.

Fondée sur le droit allemand relatif à la concurrence déloyale, cette action avait pour objectif d'interdire à son concurrent, ND, la commercialisation sur la plateforme en ligne « Amazon Marketplace » de médicaments dont la vente est réservée aux pharmacies. Pour DR, une telle commercialisation est déloyale en ce qu'elle contrevient à une exigence légale prévue à l'article 9 paragraphe 2 a) du RGPD[309], à savoir l'obtention du consentement préalable des clients pour le traitement de leurs données concernant la santé. Les juridictions inférieures – le Landgericht Dessau-Roßlau (tribunal régional de Dessau-Roßlau) d'abord, suivi par l'Oberlandesgericht Naumburg (tribunal régional supérieur de Naumbourg) – ont fait droit à cette action. Selon elles, les informations recueillies lors de la vente sont des données concernant la santé et, par conséquent, DR est effectivement en droit d'invoquer – en tant que concurrent et conformément à la législation allemande relative à la concurrence – la violation d'une disposition légale visant à règlementer le comportement sur le marché.

ND s'est pourvu devant le Bundesgerichtshof, Cour fédérale de justice allemande, pour demander le rejet de l'action en cessation. Toutefois, pour le Bundesgerichtshof, une réponse claire et univoque ne peut être déduite de la simple lecture du RGPD, en ce que ses dispositions n'admettent ni n'interdisent formellement une telle action au profit d'un concurrent. C'est ainsi que le Bundesgerichtshof a décidé de surseoir à statuer et a posé deux questions préjudicielles à la Cour :

[308] Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données- RGPD), JOUE n° L 119 du 04/05/2016.

[309] Le paragraphe 2 de cet article 9 précise son paragraphe premier, qui interdit le traitement de certaines données à caractère personnel. Le traitement devient ainsi possible dès lors que *« la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ».*

Une première portant sur le système de voies de recours établi par le RGPD **(I)** ; Une deuxième relative à l'interprétation de l'article 9 paragraphe 1 du RGPD **(II)**.

I. LE RGPD : UN SYSTEME DE VOIES DE RECOURS COMPLET CERTES, MAIS NON-EXHAUSTIF

Le RGPD établit, à son chapitre VIII, un système de voies de recours visant à protéger les droits des personnes dont les données à caractère personnel auraient fait l'objet d'un traitement contraire à ses dispositions. Ces voies de recours ne sont ouvertes qu'aux personnes concernées au sens de l'article 4 point 1 de ce règlement[310] et les entités chargées de les représenter. Le Bundesgerichtshof le souligne ainsi à juste titre : aucune disposition de ce chapitre VIII ne prévoit expressément la possibilité pour le concurrent d'une entreprise d'introduire un recours devant les juridictions civiles sur le fondement de l'interdiction des pratiques commerciales déloyales et ce, en raison de la violation alléguée des dispositions matérielles du RGPD, mais force est de constater qu'un tel recours n'est pas pour autant exclu par le RGPD.

Pour répondre à cette première question, la CJUE rappelle l'importance de prendre en compte le contexte des dispositions ainsi que les objectifs poursuivis par la règlementation dont elles font partie aux fins de leur interprétation. Ainsi, si le chapitre VIII ne prévoit pas expressément un tel recours, c'est avant tout car il vise les seuls destinataires de la protection des données à caractère personnel. Il n'est pas pour autant exclu qu'une violation des dispositions matérielles du RGPD puisse porter atteinte à un tiers. Cette atteinte est certes *secondaire* à celle subie par les personnes concernées, mais demeure une atteinte dont la réparation est quant à elle explicitement prévue par le règlement[311].

De surcroît, cette affirmation ne contredit pas la jurisprudence antérieure de la CJUE[312], évoquée par la juridiction de renvoi. En effet, si le RGPD vise effectivement à assurer une *harmonisation complète* des législations nationales relatives à la protection des données à caractère personnel, il ne saurait en être déduit que le législateur de l'Union ait entendu procéder à une *harmonisation exhaustive* des voies de recours concourant à cette protection.

Cette interprétation est confirmée par les objectifs du RGPD, qui vise à *« assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union »*[313]. Selon la CJUE, une action telle que celle intentée en l'espèce ne porte pas préjudice au système des voies de recours prévu par le règlement, ni aux objectifs susmentionnés. Au contraire, elle peut s'avérer particulièrement efficace pour assurer un niveau élevé de protection des données à caractère personnel et est de nature à renforcer l'effet utile des dispositions du règlement. La Cour ne nie pas le fait que l'action en cessation reposerait de façon incidente sur la violation des dispositions matérielles du RGPD. Toutefois, visant à assurer une concurrence loyale – à savoir un objectif notablement distinct de ceux poursuivis par le RGPD tel que le souligne

[310] Aux termes de cet article, une personne concernée est toute *« personne physique identifiée ou identifiable […] 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 ».*

[311] Selon la CJUE, cette hypothèse est envisagée à l'article 82 point 1 du RGPD qui dispose que *« toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. ».*

[312] CJUE, 28 avril 2022, *Meta Platforms Ireland*, aff. C-319/20, EU:C:2022:322, point 57.

[313] Considérant 10 du RGPD.

l'Avocat général[314], elle ne constitue pas un obstacle à l'exercice par les personnes concernées ou les entités chargées de les représenter des voies de recours prévues par le règlement. Enfin, la CJUE juge qu'aucune atteinte n'est portée à l'objectif d'assurer un *« niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union »*[315], les dispositions du RGPD s'imposant de la même façon à tous les responsables de traitement et leur respect étant déjà assuré par les voies de recours prévues par lesdites dispositions.

Au vu de l'ensemble de ces éléments, la Cour conclut au caractère non exhaustif du système des voies de recours instauré par le RGPD, reconnaissant ainsi aux États membres la possibilité de prévoir, dans leur droit interne, un recours permettant aux concurrents d'un auteur présumé d'une atteinte à la protection des données à caractère personnel de la contester en justice, sur le fondement de l'interdiction des pratiques commerciales déloyales.

II. UNE CLARIFICATION BIENVENUE DE LA NOTION DE « DONNÉES CONCERNANT LA SANTÉ »

Les données concernant la santé sont définies, à l'article 4 point 15 du RGPD, 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 »*. Les données à caractère personnel, définies au point 1 de ce même article, désignent *« toute information se rapportant à une personne physique identifiée ou identifiable »,* une personne étant identifiable dès lors qu'elle est susceptible d'être identifiée directement ou indirectement.

En l'espèce, les clients de ND devaient saisir certaines informations, comme le nom, l'adresse de livraison ou encore des éléments nécessaires à l'individualisation des médicaments, lors de leur commande en ligne de médicaments dont *la vente n'est pas soumise à prescription médicale.* Il s'agissait de savoir si ces informations correspondaient à la définition de données concernant la santé exposée ci-dessus. La Cour de justice répond en deux temps à cette interrogation. Elle constate que ces informations constituent assurément des données à caractère personnel, avant de s'intéresser à la question de savoir si elles étaient *« de nature à révéler, par une opération intellectuelle de rapprochement ou de déduction, des informations sur l'état de santé de la personne concernée ».* La CJUE juge que c'est effectivement le cas, considérant qu'il est tout à fait possible d'établir, de par cette commande, un lien entre un médicament, ses indications thérapeutiques ou ses utilisations, et une personne physique.

La juridiction de renvoi s'était notamment interrogée sur le point de savoir si le fait que la vente des médicaments en question n'était *pas soumise à une prescription médicale* était pertinent, dans la mesure où les médicaments pouvaient ainsi être destinés à des personnes autres que les clients ayant procédé à la commande. La Cour de justice répond négativement à cette interrogation, considérant qu'il ne peut être exclu, même dans le cas de figure susmentionné, qu'une conclusion soit tirée sur l'état de santé de cette tierce personne. Toute autre interprétation contreviendrait, selon la Cour, à l'objectif de garantir un niveau

[314] Conclusions de l'Avocat général, Monsieur Maciej Szpunar, présentées le 25 avril 2024, *Lindenapotheke*, aff. C-21/23, ECLI:EU:C:2024:846, point 75 : *« Certes, le considérant 9 du RGPD évoque le fait que les différences de protection du droit à la protection des données personnelles à l'égard de leur traitement peuvent fausser la concurrence. Il n'en reste pas moins que, à mon sens, une telle précision ne saurait entre interprétée comme faisant de la garantie d'une concurrence libre et non faussée un objectif du RGPD. ».*

[315] Considérant 13 du RGPD.

élevé de protection des libertés et des droits fondamentaux des personnes physiques. Enfin, la Cour précise que leur qualification en tant que « données concernant la santé » ne prohibe pas dans l'absolu le fait qu'elles fassent objet d'un traitement, à condition que ce traitement réponde aux conditions établies à cet effet par le règlement.

Si la réponse de la Cour à cette deuxième question semble s'imposer comme une évidence, la lecture des conclusions de l'Avocat général Szpunar en révèle la véritable complexité[316]. La position de l'Avocat général diverge de celle de la Cour et ce pour deux raisons principales. Premièrement, selon lui, un certain degré de certitude doit être atteint quant aux conclusions pouvant être tirées sur l'état de santé de la personne concernée avant que la qualification de « données concernant la santé » ne puisse être octroyée. Des conclusions purement hypothétiques ne sauraient être considérées comme répondant à cette condition. Deuxièmement, une interprétation large des « données concernant la santé » - que la Cour de justice considère comme découlant de l'objectif de protection accrue que se fixe le règlement[317] – est susceptible d'y nuire, conduisant l'acheteur à dévoiler de façon paradoxale, plus d'informations sensibles sur l'utilisateur final du produit. La position contraire adoptée par la CJUE est ainsi particulièrement intéressante, en ce qu'elle traduit un choix assumé en faveur d'une protection renforcée des données de santé.

CJUE, 4 octobre, 2024, *Lindenapotheke*, aff. C-21/23, ECLI:EU:C:2024:846

[316] Conclusions de l'Avocat général, Monsieur Maciej Szpunar, présentées le 25 avril 2024, *Lindenapotheke*, aff. C-21/23, ECLI:EU:C:2024:846.

[317] CJUE, 6 novembre 2003, *Lindqvist*, aff. C-101/01, EU:C:2003:596, point 50.

Droit français

Note sous Conseil d'État, 13 novembre 2024, *Association INTERHOP et autres*, n° 475297, et Conseil d'État, 13 novembre 2024, n° 492895

par Maximilien MAUGEAIS

Étudiant en Master 2 Droit du numérique, Université Paris Panthéon-Sorbonne

Dans deux décisions connexes[318] en date du 13 novembre 2024, le Conseil d'État a eu à traiter de requêtes portant sur différents aspects de la légalité du contrat conclu en 2020 entre la Plateforme des données de santé (ci-après dénommée PDS ou Health Data Hub, ou HDH) et la société Microsoft Ireland, – filiale de la société étasunienne Microsoft Inc. –, relatives à l'hébergement des données de santé issues du système national des données de santé (SNDS), considérées comme sensibles au sens de l'article 9(1) du RGPD.

Dans la première affaire n°475297, les requérants – constitués par l'association Interhop, l'association Constances, le Syndicat de la médecine générale, la Fédération Sud Santé Sociaux, la Ligue des droits de l'Homme et l'association Aides –, ont adressé une demande au ministre de la Santé en vue de « prendre des mesures propres à éliminer la violation du règlement général sur la protection des données »[319] eu égard à l'hébergement des données de santé du HDH par un acteur potentiellement soumis à l'extraterritorialité du droit étasunien. En effet, les associations requérantes invoquaient une violation du RGPD résultant « des risques d'accès, par les autorités d'un État tiers, aux données de santé hébergées par cette société »[320] et avaient demandé au ministre la Santé d'annuler le contrat d'hébergement conclu avec Microsoft Ireland. N'ayant pas reçu de réponse explicite de la part du ministre, les requérants saisirent le juge administratif aux fins, d'une part, d'annuler pour excès de pouvoir cette décision implicite de refus, d'autre part, d'enjoindre « à la ministre d'adopter, dans les plus brefs délais, toute mesure de nature à éliminer le risque d'une telle violation »[321]. Parallèlement, les parties demanderesses sollicitaient le renvoi d'une « exception d'invalidité »[322] à la Cour de justice de l'Union européenne par le biais d'une question préjudicielle « relative à l'appréciation de la validité de la décision d'exécution (UE) 2023/1795 de la Commission européenne du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE – États-Unis »[323].

[318] CE, 13 novembre 2024, *Association INTERHOP et autres,* n°475297, C et CE, 13 novembre 2024, n°s 492895 e.a., C.
[319] CE, *Association INTERHOP et autres*, *op. cit.*, 1°).
[320] *Ibid.*, considérant 1er.
[321] *Ibid.*, 2°).
[322] Conclusions de la rapporteure publique Mme Esther DE MOUSTIER, Conseil d'État, séance du 10 octobre 2024, dans l'affaire *Association INTERHOP et autres*, n°475297, p. 1.
[323] CE, *Association INTERHOP et autres*, *op. cit.* 3°).

Dans la seconde affaire n° 492895, la CNIL a adopté le 21 décembre 2023, une délibération par laquelle elle autorise le groupement d'intérêt public PDS à mettre en œuvre un traitement de données personnelles pour constituer un entrepôt de données dans le domaine de la santé, dénommé « EMC2 », et dont l'hébergeur est la filiale irlandaise de la société Microsoft. Les requérants, Monsieur C. A. et Monsieur B. A., demandaient d'une part, l'annulation pour excès de pouvoir de « la délibération de la Commission nationale de l'informatique et des libertés n° 2023-146 du 21 décembre 2023 »[324], et d'autre part, requéraient au Conseil d'État d'imposer tant à la CNIL qu'au groupement d'intérêt public PDS la « communication de divers documents »[325]. De plus, l'un des requérants réclamait également d'enjoindre au HDH : « la suspension immédiate de flux de données résultant de l'hébergement de projets de recherche sur les serveurs de la société Microsoft »[326]. Le Conseil d'État rejette les demandes des associations requérantes et des requérants dans les deux affaires commentées, tant en raison des arguments de fond que de forme avancés par les demandeurs.

En questionnant la constitution d'une « gigantesque base de données »[327] administrée par le GIP, et hébergée par un opérateur dont le siège social est localisé hors du territoire de l'Union européenne, les requérants ouvrent le débat sur la souveraineté numérique dans l'hébergement de nos données de santé. En effet, ce qui est évoqué, est le risque d'accès par des autorités étrangères à nos données de santé conformément aux lois extraterritoriales en vigueur dans ces États. Dans ce contexte, le Conseil a agilement exercé un contrôle minimal fondé sur l'absence de lien entre le renvoi d'une question préjudicielle et la solution du litige dans la première affaire, et sur l'intérêt à agir des requérants dans la seconde (**I**). En revanche, il a adopté une lecture restrictive quant à la définition du risque d'un hébergement de données de santé chez une entité soumise à des lois étrangères, en manquant ainsi une occasion de préciser une doctrine européenne en matière de souveraineté numérique (**II**).

I. L'AGILITE JURIDIQUE DU CONSEIL D'ÉTAT POUR ECHAPPER AU CONTROLE DE LA DECISION D'HEBERGEMENT

Dans l'affaire n°475297 le Conseil d'État, saisi sur la compatibilité du droit étasunien aux exigences du droit de l'Union en matière de protection des données à caractère personnel, écarte le contrôle de la validité de la décision d'adéquation conclue entre les États-Unis et la Commission européenne concernant les transferts de données personnelles hors du territoire de l'Union, prise selon les dispositions de l'article 45 du RGPD. En effet, le juge administratif considère que « la circonstance que les États-Unis constituent un pays offrant un niveau de protection adéquat au sens du RGPD est sans incidence sur la légalité de la décision de refus implicite opposée à leur demande »[328]. Ainsi, par cet argument, le Conseil d'État s'épargne le contrôle délicat d'un acte contraignant pris par une autorité européenne et ayant une valeur supra legem, dont l'interprétation n'est pas nécessaire pour la solution du litige conformément aux exigences de l'article 267 du TFUE. Pour autant, le Conseil d'État suggère que ce refus de contrôle de la décision d'adéquation ne lui interdit pas de poursuivre son contrôle de la décision implicite de refus attaquée, et par là même, souligne que la décision de la Commission

[324] CE, 13 novembre 2024, n°s 492895 e.a., 1°, 1°).
[325] *Ibid.*, 1°, 2°) ; puis 2°, 2°) ; et 3°, 2°).
[326] *Ibid.*, 2°, 3°) ; et 3°, 3°).
[327] Selon Esther DE MOUSTIER : « une gigantesque base de données de santé, conformément à l'article L. 1462-1 du code de la santé publique », dans les conclusions de la rapporteure publique Mme Esther de Moustier, *op. cit.*, p. 1.
[328] CE, *Association INTERHOP et autres*, considérant 2.

ne doit laisser en rien présumer le sens dans lequel jugera le Conseil d'État. Au demeurant, il faut rappeler que la question de la compatibilité entre le droit étasunien et le droit de l'Union européenne en matière de privacy présente des enjeux sérieux concernant les relations transatlantiques[329]. Dès lors, il est compréhensible que la formation la moins solennelle du Conseil d'État choisisse de ne pas opérer de contrôle sur la légalité d'un acte à résonance éminemment extra-juridique. C'est pourquoi le juge administratif considère qu'il « n'y a pas lieu de saisir à titre préjudiciel la Cour de justice de l'Union européenne d'une question relative à la validité de la décision d'adéquation ou portant sur la compatibilité du droit des États-Unis avec les exigences du droit de l'Union sur la protection des données personnelles »[330]. Sur ce point, bien que le Conseil d'État, ne transmet pas à la CJUE l'examen de la validité de décision d'adéquation, la haute juridiction de l'Union aura néanmoins la responsabilité de résoudre cette question. En effet, en parallèle, une saisine du Tribunal de l'Union européenne a été réalisée au fond – après le rejet de sa demande en urgence fondée sur les articles 278 et 279 du TFUE[331] – par le député français Philippe Latombe, sur le fondement de l'article 263(4) du TFUE[332], pour contester la légalité du Data Privacy Framework[333].

Dans les affaires jointes n°s 492895 et autres, le Conseil d'État rejette également sur un argument de recevabilité tout examen au fond de la légalité, tant de l'hébergement par un sous-traitant ayant son siège social hors du territoire de l'Union des données de santé issues du SNDS, que leur appariement aux données issues de quatre centres hospitaliers pour la création de l'entrepôt « EMC2 », suite au contrat conclu entre le GIP PDS et l'Agence européenne du médicament. Certes, la recevabilité d'un recours en excès de pouvoir contre un acte d'une autorité administrative indépendante est admise depuis une dizaine d'années par une jurisprudence constante du Conseil[334]. Cependant, en l'espèce les requêtes contre la décision de la CNIL ne sont rejetées ni sur un moyen de légalité interne ni de légalité externe, mais sur un motif d'irrecevabilité ce qui conduit le juge administratif à ne pas se prononcer sur le fond des moyens avancés. Effectivement, le Conseil d'État estime que les requérants « ne justifient pas, ce faisant, d'un intérêt suffisamment direct et certain leur donnant qualité pour agir »[335]. Pour le Conseil, l'intérêt à agir des requérants n'est pas clairement établi, puisqu'il n'est pas certain qu'ils ne subissent les conséquences de l'exécution du contrat. En effet, le Conseil

[329] C. KOUMPLI, « Les transferts de données UE-États-Unis À la recherche du niveau élevé de protection européenne des données personnelles », *Revue du droit public*, Décembre(4), 2024, 105-113. Disponible sur : <https://droit.cairn.info/revue-revue-du-droit-public-2024-3-page-105 > [consulté le 29 mai 2025].

[330] *Ibid*., considérant 2.

[331] TUE, ordonnance, 12 octobre 2023, *Latombe c/ Commission*, aff. T-553/23 R.

[332] Recours introduit le 6 septembre 2023, *Latombe/Commission*, aff. T-553/23.

[333] Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE – États-Unis. *JOUE* n° L 231/118, du 20.9.2023.

[334] CE, Ass., 21 mars 2016, *Société Fairvesta International GMBH et autres* ; CE, Ass., 21 mars 2016, *Société NC Numericable* qui consacrent la recevabilité d'un recours contre certains actes des AAI sur le modèle du REP dès lors qu'ils « sont de nature à produire des effets notables, ou qui ont pour objet d'influer de manière significative sur les comportements des personnes auxquelles il s'adresse », dans CONSEIL D'ÉTAT, *Les grandes décisions depuis 1873*, 21 mars 2018, disponible sur: <https://conseil-etat.fr/decisions-de-justice/jurisprudence/les-grandes-decisions-depuis-1873/conseil-d-etat-21-mars-2016-societe-fairvesta-international-gmbh-et-autres-conseil-d-etat-assemblee-21-mars-2016-societe-nc-numericable> [consulté le 18 mai 2025].

[335] CE, 13 novembre 2024, n°s 492895 e.a., considérant 3.

d'État souligne que les requérants ne sont que potentiellement affiliés à « la population témoin dont les données, [...] seront appariées aux données de quatre centres hospitaliers pour la constitution de l'entrepôt de données de santé "EMC2" »[336]. Dès lors, pour le juge administratif plus rien ne justifie que les requêtes étudiées fassent l'objet ni d'une décision sur le fond, ni de conclusions par la rapporteure publique, notamment sur le point sensible de la validité et de l'opportunité d'un contrat entre le HDH et un organe de l'UE, l'Agence européenne du médicament. Or, il est dommageable que les requêtes aient été portées par des particuliers potentiellement impactés par le contrat de prestation de service relatif à la constitution de l'entrepôt de données de santé « EMC2 », car il s'agit ici d'une véritable occasion manquée de résoudre cette question par la voie contentieuse, dans un contexte géopolitique changeant. En effet, il existe un réel besoin d'opérer un renforcement de la doctrine de souveraineté numérique[337] en cours de construction par un rappel des critères techniques et juridiques exigés pour ce type d'hébergement. Finalement, seule l'affaire n°475297 a permis un contrôle sur le fond de la question du risque pour les données de santé issues du SNDS du fait de l'hébergement par un sous-traitant soumis légalement à l'extraterritorialité des lois étasuniennes qui présentent une gravité particulière et une occurrence incertaine sur la saisine de données de santé par les autorités américaines.

II. LA LECTURE RESTRICTIVE DU CONSEIL D'ÉTAT DANS L'APPROCHE DES RISQUES RELATIVE A LA DECISION L'HEBERGEMENT

Dans l'affaire n°475297, le Conseil d'État fonde en partie le rejet des prétentions posées au fond sur un argument de légalité externe à savoir l'insuffisance du « moyen tiré du défaut de motivation de la décision attaquée, dont aucune disposition légale ou réglementaire n'impose la motivation »[338]. Certes, un tel grief devait manquer inéluctablement de consistance puisque légalement rien n'oblige le ministre de la Santé à motiver son refus qu'il soit explicite ou implicite. Pour autant, le silence du ministre en la matière intrigue. En effet, d'aucuns pourraient alléguer qu'il s'agit d'une occultation des problématiques du choix du sous-traitant[339] – dont le cadre est posé à l'article 28 du RGPD – pour le traitement des données de santé considérées par essence comme sensibles[340]. Ce choix s'explique d'un point de vue politique, en partie, du fait que le GIP PDS est un projet pilote français dont l'objectif est de démontrer le rôle prépondérant de la France dans la création des espaces de données – particulièrement en matière de données de santé – en cohérence avec la réglementation de l'UE adoptée ces dernières années en matière de data spaces (DGA, DA, EHDS[341]). Dans ce prolongement, l'objet des présentes requêtes concernait le risque d'accès aux données de santé par une puissance étrangère. Or, le fait qu'un État tiers puisse accéder à ces données présente

[336] *Ibid*., considérant 3.

[337] B. BERTRAND et G. LE FLOCH (dir.), *La souveraineté numérique*, Bruylant, Bruxelles, 2024 ; voir également P. TÜRK, « Définition et enjeux de la souveraineté numérique », *Cahiers français*, 2020/2, n°415, 2020, p.18-28. Disponible sur : <https://shs.cairn.info/magazine-cahiers-francais-2020-2-page-18?lang=fr> [consulté le 29 mai 2025].

[338] CE, *Association INTERHOP et autres*, considérant 3.

[339] À ce sujet, voir entre autres : B. BEVIERE-BOYER, « La gestion des données de santé par le Heath Data Hub : le recours à la société Microsoft, entre risques et précautions », *Droit, Santé et Société*, 2021/3, n° 3, 2021. p.42-48. Disponible sur : <https://droit.cairn.info/article/DSSO_083_0042> [consulté le 29 mai 2025].

[340] Voir le considérant 10 du RGPD.

[341] Bien que le règlement EHDS soit entré en vigueur en 2025, sa négociation a débuté en mars 2022.

une gravité particulière et une occurrence aléatoire. En effet, cette gravité découle de la nature même de ces données de santé qui touchent à la vie privée et à la dignité humaine. Cependant, la probabilité que ce risque se produise est dans les faits plus importante car ces données sont hébergées chez un opérateur régi par des normes extra-européennes. En l'espèce, le Conseil d'État a jugé que le moyen tiré de ce qu'il existait des risques d'accès par les autorités d'un État tiers à des données sensibles « ne porte sur aucune disposition précise de ce règlement ni ne démontre dans quelle mesure la décision de refus du ministre a pu y porter atteinte »[342]. Ainsi, se fondant sur un défaut de base légale, le juge administratif pointe l'absence de lien de causalité, du moins de connexité entre « les risques d'accès à des données sensibles par les autorités d'un pays tiers »[343] et la décision de refus implicite du ministre. En refusant d'apprécier en opportunité cette articulation entre les risques d'accès et la conformité au RGPD[344,] le Conseil d'État laisse pendantes plusieurs problématiques. De deux choses l'une : refuser de voir dans les dispositions du RGPD une définition d'un tel risque, c'est pointer les carences du législateur européen, mais c'est aussi récuser – du moins incidemment – la prohibition d'un tel risque en présence d'une décision d'adéquation. En fait, pour le Conseil d'État, l'enjeu de ce point est assez secondaire, puisqu'il précise dans sa décision que le « contrat d'hébergement conclu entre le GIP et la société Microsoft Ireland Operations Ltd cité au point 1 n'a pas reçu d'exécution »[345]. Ici, il s'agit d'une appréciation fine et concrète du risque d'accès en raison du champ d'application ratione tempori du litige. Toutefois, notons que l'analyse du risque aurait pu se réaliser plus classiquement selon les deux critères de la gravité et de l'occurrence. Si la gravité d'un tel accès ne semble pas faire débat au regard des dispositions de l'article 9(1) du RGPD ; l'occurrence, quant à elle, pose plus de difficulté car sa détermination correspond à une analyse prospective de la politique des autorités américaines d'accéder à des données à haute valeur ajoutée tant d'un point de vue économique que géopolitique. Reste que l'incertitude juridique quant à la possibilité pour les autorités d'enjoindre à la filiale irlandaise de communiquer les données hébergées en Europe aurait le mérite d'être appréhendée in abstracto en un risque accru. D'autre part, les mesures techniques et organisationnelles de l'article 32 du RGPD combinées à l'obligation d'appliquer ces mesures par voie contractuelle, selon l'article 28 du règlement précité, s'apparentent également à un facteur d'accroissement du risque que les données du SNDS fassent l'objet d'un transfert vers le siège social de Microsoft au nom d'une injonction des autorités étasuniennes. En effet, au regard de la hiérarchie des normes, il est peu probable que l'obligation légale de Microsoft de se conformer à la législation extraterritoriale américaine pèse moins fort que l'engagement contractuel du sous-traitant de ne pas le faire.

Le dernier moyen des requérants écarté par le Conseil d'État concerne la qualité de tiers au contrat du ministre qui n'a pas la compétence « de modifier le contrat cité au point 1 »[346]. En effet, comme l'explique clairement la rapporteure publique, l'autorité ministérielle ne possède pas la capacité de s'immiscer dans un contrat auquel elle n'est pas partie, a fortiori pour « enjoindre au GIP de recourir à un autre cocontractant »[347]. Effectivement, depuis

[342] CE, *Association INTERHOP et autres*, considérant 4.
[343] *Ibid*., considérant 4.
[344] Voir les considérants 101 et 103 du RGPD. D'après nous, ces considérants combinés avec la lecture des articles 45 et 48 du RGPD permettent de déterminer un risque entre la décision d'adéquation et sa potentielle réalisation à travers l'injonction des autorités américaines via l'extraterritorialité de leur cadre normatif.
[345] CE, *Association INTERHOP et autres*, considérant 4.
[346] *Ibid*., considérant 5.
[347] Conclusions de la rapporteure publique Mme Esther DE MOUSTIER, *op. cit.*, p. 2.

une décision du 30 juin 2017 a été fermement établie la recevabilité de l'action d'un tiers au contrat[348] s'estimant lésé « de façon suffisamment directe et certaine par une décision refusant de faire droit à sa demande de mettre fin à l'exécution du contrat »[349], comme c'est le cas en l'espèce. Encore faut-il que les requérants prouvent d'une part, le caractère direct et certain du préjudice résultant de l'exécution du contrat, et d'autre part, le lien de causalité entre l'exécution du contrat et le préjudice allégué. De plus, la rapporteure publique rappelle que la recevabilité d'une action en responsabilité d'un tiers au contrat n'est possible que « devant le juge du contrat »[350] par un « recours de pleine juridiction »[351] pour obtenir la « fin [de] l'exécution du contrat »[352]. A contrario, comme les requérants l'ont fait dans le litige étudié, le juge de l'excès de pouvoir ne peut répondre ni sur la forme en raison de l'absence de recevabilité du moyen, ni sur le fond car le juge de l'excès de pouvoir n'a pas la compétence du juge du contrat qui apprécierait le moyen dans un contentieux de pleine juridiction. Néanmoins, en dépassant ces limites contentieuses, il faut s'interroger sur des techniques pré-contractuelles qui permettraient de limiter la possibilité de candidature d'opérateurs extra-européens par la définition ex ante lors de l'établissement des besoins et du cahier des charges déterminant les conditions de candidature. En effet, le contrat d'hébergement soumis à une procédure de marché public devrait respecter des conditions strictes telles que la certification SecNumCloud en plus de la certification HDS pour limiter légalement des sous-traitants à la zone géographique de l'UE, car malheureusement ex post, un tiers au contrat malgré sa qualité ministérielle ne peut juridiquement avoir un impact sur les conditions d'exécution du contrat litigieux.

Ainsi, pour l'heure, il apparaît que l'ambition menée au niveau européen de constituer des espaces de données suffisamment puissants prenne le pas sur la nécessité de développer des architectures numériques souveraines, bien qu'une réorientation en ce sens semble se profiler. Comme le rappelle Esther de Moustier dans une autre affaire : « il serait préférable, pour les données présentant une sensibilité particulière telles que les données de santé, de retenir une solution pleinement souveraine, échappant aux législations de pays tiers et minimisant ainsi tout risque d'ingérence extérieure. Pour autant, la quête d'une solution technique présentant un risque zéro apparaît, du moins pour l'heure, largement illusoire »[353].

Conseil d'État, 10ème chambre, 13 novembre 2024, *Association INTERHOP et autres*, n° 475297, ECLI:FR:CECHS:2024:475297.20241113 et Conseil d'État, 10ème chambre, 13 novembre 2024, n° 492895, ECLI:FR:CECHS:2024:492895.20241113

[348] CE, Section, 30 juin 2017, *Syndicat mixte de production de l'activité transmanche*, n° 398445.
[349] Conclusions de la rapporteure publique Mme Esther DE MOUSTIER, *op. cit.*, p. 2.
[350] *Ibid.*
[351] *Ibid.*
[352] *Ibid.*
[353] Conclusions de la rapporteure publique Mme Esther DE MOUSTIER, Conseil d'État, séance du 2 octobre 2024, dans les affaires jointes *Association Internet Society France*, n°491644, et *Société Clevercloud et autres*, n°492368, p. 8.

Le Conseil d'État valide l'hébergement des données de santé par Microsoft dans le projet DARWIN.EU

Le Conseil d'État, dans cette affaire est saisi en référé d'une demande de suspension de l'exécution de deux délibérations de la CNIL en date du 13 février 2025 publiées en mars 2025 (2024-014 et 2024 013) ayant autorisé l'EMA à mettre en œuvre, pendant une durée limitée à trois ans, des traitements automatisés de données à caractère personnel ayant pour finalité, dans le cadre du projet DARWIN.EU, des études portant sur l'estimation d'incidence et de prévalence des pathologies (délibération n° 2025-014) et de l'utilisation des médicaments (délibération n° 2025-013) dans la population générale en France.

S'agissant plus précisément de la délibération 2024-014, les requérants invoquent le fait, pour justifier l'urgence à suspendre l'exécution de la délibération contestée, que l'autorisation donnée par la CNIL, en ce qu'elle admet la légalité de l'hébergement de données sensibles par un sous-traitant, Microsoft Ireland, dont la société mère est soumise au droit des Etats-Unis, « préjudicie de manière grave et immédiate aux intérêts qu'ils entendent défendre, en raison principalement du risque qui en résulte d'accès à ces données, qui concernent dix millions de personnes, par des autorités des États-Unis, dans un contexte d'instabilité juridique qui s'est accentué dans ce pays depuis 2024 ».

Ce moyen n'est pas retenu par les juges en référé car « s'il ne peut être totalement exclu que les données du traitement autorisé, alors même qu'il est prévu qu'elles soient conservées dans des centres situés en France, fassent l'objet de demandes d'accès par les autorités des États-Unis, par l'intermédiaire de la société mère de l'hébergeur, et que celui-ci ne puisse s'y opposer, le risque d'accès aux données de santé hébergées en France demeure hypothétique en l'état de l'instruction ». A l'appui de cette affirmation les juges relèvent que la société Microsoft est certifiée « HDS » et à ce titre respecte un référentiel de sécurité, les données sont pseudonymisées à plusieurs reprises et non directement identifiantes, et enfin, la décision souligne l'intérêt public à ne pas retarder la réalisation des études menées dans le cadre du projet DARWIN.EU. Pour les juges, dans le cadre d'une analyse « bénéfice/risques, il serait regrettable que le projet de recherche DARWIN.EU soit retardé et il n'y aurait pas d'atteinte suffisamment grave et immédiate aux intérêts des requérants ce qui justifie le rejet de la demande.

Le Conseil d'État ne manque pas de souligner par ailleurs « qu'il ne résulte pas de l'instruction que des solutions pouvant offrir à la PDS les mêmes fonctionnalités et une meilleure sécurité globale que celle commercialisée par *Microsoft « soient d'ores et déjà disponibles* ». Il faut donc comprendre en filigrane que cette solution technique d'hébergement présente un caractère temporaire faute d'avoir aujourd'hui la capacité technique d'héberger sur le territoire national un volume de données aussi important et c'est donc sans véritable surprise que la délibération de la CNIL est validée.

Compte tenu de la quantité importantes de données à stocker il a été fait appel à Microsoft mais, il faut le souligner, seules des données techniques sont transférées aux USA.

Pour les juges, dans le cadre d'une analyse « bénéfice/risques, il serait regrettable que le projet de recherche DARWIN.EU soit retardé et il n'y aurait pas d'atteinte suffisamment grave et immédiate aux intérêts des requérants ce qui justifie le rejet de la demande.

On notera aussi la formule selon laquelle « bien que tout risque d'atteinte aux données hébergées ne soit pas totalement écarté », la double

pseudonymisation mise en œuvre permet de protéger l'identité des patients.

Conseil d'État, Juge des référés, 25 avril 2025, n° 503163,
ECLI:FR:CEORD:2025:503163.20250425

Modalités d'accès au dossier médical partagé d'un patient par des professionnels « hors santé » participant à sa prise en charge : une affirmation non équivoque de constitutionnalité

par Joud GHARZEDDINE

Étudiante en Master 2 Juriste européen, Université Toulouse Capitole

Par sa décision n° 2024-1101 rendue le 12 septembre 2024, le Conseil constitutionnel déclare conformes à la Constitution les modalités d'accès au dossier partagé du patient par les professionnels participant à sa prise en charge.

En l'espèce, le Conseil constitutionnel avait été saisi par le Conseil d'État d'une question prioritaire de constitutionnalité portant sur la conformité à la Constitution du paragraphe III de l'article L. 1111-17 du code de la santé publique[354]. Selon le Conseil national de l'Ordre des médecins – requérant devant le Conseil d'État, cette disposition serait contraire au droit au respect de la vie privée du patient en ce qu'elle permet à tout professionnel participant à sa prise en charge– n'excluant ainsi pas les professionnels qui ne relèvent pas de la catégorie de santé et qui, conséquemment, ne sont pas soumis aux mêmes règles déontologiques – d'accéder à son dossier médical partagé.

La réponse apportée par le Conseil constitutionnel est aussi pragmatique que la question est délicate. Le Conseil commerce par rappeler que les dispositions contestées de l'article L. 1111-17 ont été édictées afin d'améliorer la *« coordination des soins de la personne prise en charge »*, permettant au législateur de poursuivre l'objectif de valeur constitutionnelle de protection de la santé. Le droit au respect de la vie privée est certes un droit appelant à une vigilance particulière dès lors qu'il s'agit du domaine médical, toutefois et tel que le souligne le Conseil, cela n'est pas de nature à le substituer à son contrôle classique de conciliation. Le Conseil note ensuite que les dispositions contestées limitent l'accès au dossier aux seuls professionnels participant directement à la prise en charge du patient, dans le respect des articles L. 1110-4[355] et L. 1110-12 du code de la santé publique[356]. De plus, l'accès au dossier est conditionné au consentement préalable du patient, qui peut *à tout moment* clôturer son dossier médical partagé, rendre certaines informations inaccessibles voire même restreindre la liste des professionnels y ayant accès. Cependant, une fois recueilli, ce consentement vaut pour tous les professionnels de l'équipe de soins. Le Conseil constitutionnel écarte ainsi l'argument déontologique mis en avant par

[354] Aux termes de cet article, *« Tout professionnel participant à la prise en charge d'une personne en application des articles L. 1110-4 et L. 1110-12 peut accéder, sous réserve du consentement de la personne préalablement informée, au dossier médical partagé de celle-ci et l'alimenter. L'alimentation ultérieure de son dossier médical partagé par ce même professionnel est soumise à une simple information de la personne prise en charge ».*

[355] Conformément à son paragraphe II, *« un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social. »*

[356] L'article L. 1110-12 du code de la santé publique définie l'équipe de soins comme *« un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes ».*

le Conseil national de l'Ordre des médecins, estimant que l'ensemble de l'équipe de soins reste soumis au secret médical et encourt, en cas de non-respect, les sanctions prévues aux articles L. 1110-4 paragraphe V du code de la santé publique[357] et 226-13 du code pénal[358]. C'est à la vue de l'ensemble de ces éléments que le Conseil conclut à la conformité des dispositions contestées à la Constitution.

Conseil Constitutionnel, 12 septembre 2024, Décision n° 2024-1101 QPC, *JORF* n° 0218 du 13 septembre 2024
Conseil d'État, 10ème et 9ème chambres réunies, 10 juin 2024, n° 490409, ECLI:FR:CECHR:2024:490409.20240610.

[357] Cet article dispose que *« le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende. ».*

[358] Aux termes de cet article, *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. »*

Bulletin de
l'EDiHL
European Digital Health Law

LISTE DES CONTRIBUTEURS

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

Sarah BISTER
Avocate au Barreau de Paris et
Docteure en droit public

Claire BORIES
Docteure en droit public, École de droit de Toulouse, Université Toulouse Capitole

Noémie DUBRUEL
Doctorante en droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier,
UMR 1295 Inserm équipe BIOETHICS

Valentine DURAND
Doctorante en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole

Winnie DONGBOU WAMBA
Doctorant en Droit public, IRDEIC, École de droit de Toulouse, Université Toulouse Capitole et Juriste en protection des données de santé My Data-TRUST

Lisa FERIOL
Doctorante CIFRE, Ekitia et Équipe BIOETHICS, CERPOP UMR1295 Inserm et Université Toulouse Paul Sabatier

Joud GHARZEDDINE
Étudiante en Master 2 Juriste européen, Université Toulouse Capitole

Luis HALEGA
Étudiant en Master 2 Droit de la santé et de la protection sociale, Université Toulouse Capitole

Romane MASSIMI
Étudiante en Master 2 Juriste européen

Maximilien MAUGEAIS
Étudiant en Master 2 Droit du numérique, Université Paris Panthéon-Sorbonne

Kévin MINGOT
Étudiant en Master 2 Droit de la santé, Université Toulouse Capitole

Pierre-Emmanuel PARENT DE CURZON
Étudiant en Master 2 Juriste européen, Université Toulouse Capitole

Bulletin de l'EDiHL

European Digital Health Law



N° 2

2ème année – Bulletin annuel
Juin 2024 – Juin 2025

Cofinancé par l'Union européenne

Nathalie DE GROVE-VALDEYRON
Claire BORIES
Directrices scientifiques

Claire BORIES
Coordinatrice

Bulletin de l'EDiHL

European Digital Health Law

ACTUALITÉ DU DROIT EUROPÉEN DU NUMÉRIQUE EN SANTÉ

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

À LA UNE

DÉPLOIEMENT DE L'IA DANS LES SOINS DE SANTÉ

Initiative européenne sur les jumeaux humains virtuels

par Noémie DUBRUEL

RÈGLEMENTATION DES DISPOSITIFS MÉDICAUX

L'encadrement de la mise à disposition des applications qualifiées de dispositifs médicaux sur les plateformes en ligne. Commentaire du guide MDCG 2025-4

par Sarah BISTER

DIGITAL HEALTH AND ONLINE PROTECTION OF MINORS

Online Health Taskforce, *Final Report : Online health and rights for Ireland's children and young people*, Department of Health, September 2025

par Thomas BOUDON

TÉLÉMÉDECINE

La construction prétorienne de la notion de « télémédecine » dans le cadre des soins de santé transfrontaliers

CJUE, 11 septembre 2025, *Österreichische Zahnärztekamme*, aff. C-115/24

par Salaheddine ZAHID

N° 3

3ème année – Bulletin annuel
Juin 2025 – Juin 2026

Cofinancé par l'Union européenne

Financé par l'Union européenne.

Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables

Funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them



ÉDITORIAL

Nathalie DE GROVE-VALDEYRON
Professeure de droit public
Chaire Jean Monnet (2017-2023) et (2023 - 2026)
Université Toulouse Capitole – IRDEIC

Ce troisième bulletin, qui sera le dernier de la Chaire EDIHL (European Digital Health Law, 2023-2026) se situe dans le prolongement des deux précédents. Il reprend les éléments marquants de l'actualité tant législative que contentieuse, dans le domaine du numérique en santé, tout en se caractérisant par une plus grande place donnée à la mise en œuvre, par les Etats membres, des règlements récemment adoptés, et tout particulièrement, du Règlement sur l'Espace européen des données de santé (ci-après EEDS). Comme cela a déjà été précisé dans les éditions précédentes, si le règlement est bien en vigueur, il implique cependant d'une part, que les États satisfassent à un certain nombre d'obligations préalables pour pouvoir le mettre en œuvre de manière effective, et d'autre part, que les actes d'exécution attendus de la part de la Commission soient aussi adoptés pour disposer d'éléments techniques indispensables.

On peut souligner ici le rôle important joué par l'action conjointe TEHDAS 2 afin de répondre aux questions que les différentes parties prenantes, les acteurs du numérique et, au premier chef, les citoyens se posent sur les conséquences du règlement tant dans le cadre de l'utilisation primaire que de l'utilisation secondaire des données de santé électroniques.

Le lecteur trouvera en outre dans ce bulletin, en français, l'essentiel du contenu des « Guidelines » de TEHDAS soumises encore à consultation publique. Non moins essentielles, les « Guidelines » de l'EMA (Agence européenne des médicaments) adoptées dans le domaine des dispositifs médicaux connectés (DMC) (ou numériques, DMN) apportent des précisions indispensables aux développeurs de tels dispositifs. S'agissant toujours de ces dispositifs médicaux numériques, une incursion dans le droit français (principes applicables par la CNEDIMTS) et dans le droit suédois permet d'avoir une idée des différences de mode de prise en charge de ces DM, en fonction des particularités étatiques, la question du remboursement restant, conformément à l'art. 168 du TFUE, de l'unique compétence des États membres.

On relèvera aussi deux études de première main sur la mise en œuvre de l'EEDS en Italie et en Irlande, des textes ayant été récemment adoptés dans ces deux États. Des textes importants adoptés en Espagne ou en Belgique sont également rapidement évoqués, la dimension du bulletin ne permettant pas de faire état des avancées réalisées au sein de chacun des États membres. Le bulletin comporte enfin, dans le cadre de sa partie contentieuse, les commentaires de quelques arrêts marquants adoptés par le Conseil d'État (France) ou par la Cour de justice.

Ce bulletin n'aurait pu voir le jour sans la participation de fidèles doctorants (Noémie, Lisa, Valentine, Winnie), dont certains sont devenus docteurs depuis le début de la chaire. De plus anciens doctorants encore, devenus avocats (Sarah) ou occupant des fonctions au sein du ministère de la santé (Claire) ont souhaité continuer à s'investir pour le bulletin, malgré leurs obligations professionnelles. Qu'ils soient chaleureusement remerciés.

Mes remerciements vont aussi aux étudiants qui ont découvert cette nouvelle discipline qu'est le droit européen du numérique en santé, grâce au *DU EDIHL* (Thomas, Franck) mais aussi au cours de *droit européen du numérique en santé* que j'ai pu créer grâce à la chaire J Monnet, à l'École de droit de Toulouse (UTC) (Chaimae, Laure, Philippine, Thomas pour cette année 2025-2026). Merci aussi aux étudiants du Master 2 juriste européen et droit européen international et comparé (Salaheddine, Joud, Maddalena) et du Master 2 Santé (Alizée, Lukas, Amina, Marie, Clarance, Mélanie, Maïlys). Enfin mes remerciements les plus chaleureux vont à Claire BORIES, qui s'est chargée, cette année encore, malgré ses obligations professionnelles, de toute la réalisation formelle du bulletin et de la coordination scientifique. Bonne lecture !

Bulletin de l'EDiHL
European Digital Health Law

SOMMAIRE

N°3 /
3ème année – Bulletin annuel
Juin 2025-Juin 2026

VEILLE LÉGISLATIVE

Droit de l'Union européenne

DÉPLOIEMENT DE L'INTELLIGENCE ARTIFICIELLE DANS LES SOINS DE SANTÉ 10

Étude européenne sur le déploiement de l'IA dans les soins de santé 10
DG Santé, *Study on the deployment for AI in healthcare. Final report*, January 2024-2025, 241p.

INITIATIVE EUROPÉENNE EN MATIÈRE D'IMAGERIE SUR LE CANCER

Aperçu général sur le plan européen de lutte contre le cancer 12

Initiative européenne en matière d'imagerie sur le cancer : action phare du plan européen pour vaincre le cancer
par Joud GHARZEDDINE 12

INITIATIVE EUROPÉENNE « +1 MILLION GENOMES » (1+MG°)

Émergence d'une infrastructure européenne fédérée au service de la génomique et de la médecine personnalisée
Le *Genomic Data Infrastructure (GDI)* dans le cadre de l'initiative européenne « 1+ million Genomes » (1+GM)
par Salaheddine ZAHID 16

INITIATIVE EUROPÉENNE SUR LES JUMEAUX HUMAINS VIRTUELS (VHT)

Commission européenne, European Virtual Human Twins (VHT) Initiative
par Noémie DUBRUEL 20

Les jumeaux humains virtuels
par Alizée FERNANDEZ 23

STRATÉGIE POUR L'UNION DES DONNÉES 28

Décrypter la stratégie européenne pour les données 28

La stratégie pour une union des données : vers une mobilisation stratégique des données au service de l'intelligence artificielle dans l'Union européenne
Communication de la Commission du 19 novembre 2025, "Data Union Strategy Unlocking data for AI", *COM(2025)* 835 final
par Salaheddine ZAHID 28

FOCUS — LE « DIGITAL OMNIBUS » 33

La crise identitaire des données synthétiques en Europe face au diagnostic jurisprudentiel de la CJUE sur la définition de l'anonymisation
Compte rendu de la présentation à l'occasion de la rencontre Québec et Toulouse sur l'Espace Européen des Données de Santé
par Winnie DONGBOU WAMBA 36

TEHDaS 2 40

23.06.2025
Workshop on the ethical dimensions of the European Health Data Space
par Lisa FÉRIOL 40

27.05.2025
M7.1 Guideline on how to use data in a secure processing environment
par Franck AZNAR 43

05.09.2025
M7.2 Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data
par Franck AZNAR 45

Commentaire des propositions TEHDaS2 clarifiant les modalités d'examen des finalités de réutilisation, de notification des constatations significatives et portant sur les infrastructures techniques de traitement des données

16.09.2025
M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data

17.09.2025
M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025
M7.4 Draft technical, functional and security specifications of Secure Processing Environments

07.09.2025
M8.2 Draft Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data

par Winnie DONGBOU WAMBA 48

AUTRES PUBLICATIONS TEHDAS 2 53

17. 09.2025
M4.1.1 Draft guideline on fees related to the EHDS regulation

Second section: 4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

07.09.2025
M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse

06.05.2025
D6.2 Guideline for data users on good application and access practice

17.09.2025
D6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access

17.09.2025
D6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)

17.09.2025
M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025
M7.4 Draft technical, functional and security specifications of Secure Processing Environments

RÈGLEMENTATION DES DISPOSITIFS MÉDICAUX 54

La Commission européenne propose une simplification du cadre règlementaire applicable aux dispositifs médicaux

DOCUMENTS DE RÉFÉRENCE 54
Fiche d'information de la Commission européenne
Proposition de règlement *COM(2025)* 1023 final
Questions & Answers de la Commission européenne

LES GUIDES MDCG

Aperçu général du MDCG et de ses guides 55

L'encadrement de la mise à disposition des applications qualifiées de dispositifs médicaux sur les plateformes en ligne. Commentaire du guide MDCG 2025-4

MDCG 2025-4 - *Guidance on the safe making available of medical device software (MDSW) apps on online platforms*, June 2025
par Sarah BISTER 55

L'articulation opérationnelle entre le règlement sur les dispositifs médicaux et la législation sur l'intelligence artificielle. Commentaire du Guide MDCG 2025-6
MDCG 2025-6 FAQ on Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), June 2025
par Sarah BISTER 60

Lignes directrices relatives à la qualification et à la classification des logiciels dans le cadre du règlement (UE) 2017/745 et du règlement (UE) 2017/746. Analyse opérationnelle de la révision MDCG 2019-11 rev. 1
MDCG 2019-11 rev.1 - Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746
par Sarah BISTER 76

ÉVALUATION POUR LE REMBOURSEMENT DES DISPOSITIFS MÉDICAUX NUMÉRIQUES (DMN) 88

L'évaluation clinique commune des dispositifs médicaux à l'épreuve de la pratique
Règlement d'exécution (UE) 2025/2086 du 17 octobre 2025 établissant, conformément au règlement (UE) 2021/2282 concernant l'évaluation des technologies de la santé, les règles de procédure applicables à l'interaction au cours des évaluations cliniques communes de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro au niveau de l'Union, à l'échange d'informations concernant l'élaboration et la mise à jour de ces évaluations et à la participation à ces dernières, ainsi que des modèles pour ces évaluations cliniques communes, *JOUE* n° L 2025/2086 du 20/10/2025
par Sarah BISTER 88

COMPLÉMENT UTILE 98
HTA CG, Annual Work Programme 2025, 28 November 2025

ERS – TÉLÉMÉDECINE POUR LA VENTILATION MÉCANIQUE À DOMICILE 99

EUROPEAN RESPIRATORY SOCIETY 99

Marieke L. DUIVERMAN et *al.*, « European Respiratory Society Clinical Practice Guideline on Telemedicine in Home Mechanical Ventilation », *European Respiratory Journal*, 2025 99

Droit français

ÉVALUATION ET REMBOURSEMENT DES DMN PAR LA CNEDiMTS 100

GUIDE

Principe d'évaluation de la CNEDiMTS

Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS,* 1er juillet 2025

par Marie DESMEULES 100

Principe d'évaluation de la CNEDiMTS

Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM)

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM),* 1er juillet 2025

par Lukas MARA 104

Principe d'évaluation de la CNEDiMTS

Volume 3 : la prise en charge transitoire (PECT)

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 3 :la prise en charge transitoire (PECT),* 1er juillet 2025

par Amina MOUSTOIFA 105

Principe d'évaluation de la CNEDiMTS

Volume 4 : la prise en charge anticipée des dispositifs médicaux numériques (PECAN)

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 4 :la prise en charge anticipée des dispositifs médicaux numérique*, 1er juillet 2025

par Mélanie de SOUSA BARBEIRO 109

BILAN MÉDICAMENTEUX – RÉFÉRENTIEL HAS 113

RÉFÉRENTIEL :

Harmonisation du bilan médicamenteux. **Recueil des besoins métiers en matière de bilan médicamenteux**

HAS, *Harmonisation du bilan médicamenteux. Recueil des besoins métiers en matière de bilan médicamenteux*, 24 juillet 2024

par Clarance JEAN-PIERRE 113

IA GÉNÉRATIVE EN SANTÉ 114

GUIDE

Premières clefs d'usage de l'IA générative en santé, **dans les secteurs sanitaire, social et médico-social**

A.V.E.C : Apprendre – **V**érifier – **E**stimer – **C**ommuniquer

HAS, *Première clefs d'usage de l'IA générative en santé, dans les secteurs sanitaire, social et médico-social. A.V.E.C : Avance – Vérifier – Estimer – Communiquer*, 23 octobre 2025

par Maylïs CAPELL 114

TRANSFORMATION NUMÉRIQUE DES ÉTABLISSEMENT DE SANTÉ 119

Instruction n° DNS/2025/180 du 29 décembre 2025 relative au lancement de la deuxième phase du programme HOP'EN 2 pour soutenir la transformation numérique des établissements de santé, *BO* du 12/01/2026 119

Arrêté du 27 janvier 2026 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - HospiConnect, *JORF* n° 0024 du 29/01/2026 119

PRISE EN CHARGE DES ACTES DE TÉLÉSURVEILLANCE MÉDICALE 120

TÉLÉSURVEILLANCE DU DIABÈTE GESTATIONNEL 120

Renouvellement de la prise en charge du DMN MYDIABBY jusqu'en 2028

Arrêté du 27 mars 2026 portant renouvellement d'inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° L 0077 du 31 mars 2026

TÉLÉSURVEILLANCE DES PORTEURS DE MONITEURS CARDIAQUES IMPLANTÉS 120

Inscription du dispositif CARELINK (Medtronic)

Arrêté du 24 juillet 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025

Arrêté du 24 juillet 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025

Inscription du dispositif HOME MONITORING SERVICE CENTER (Biotronik)

Arrêté du 23 juin 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0149 du 28 juin 2025

Arrêté du 23 juin 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0147 du 26 juin 2026

Inscription du dispositif LATITUDE CLARITY (Boston Scientific)
Arrêté du 3 mars 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026

Arrêté du 3 mars 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026

Inscription du dispositif IMPLICITY IM009 (Implicity)
Arrêté du 20 mai 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0119 du 22 mai 2026

Arrêté du 20 mai 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n°0119 du 22 mai 2026

MON ESPACE SANTÉ 121

Guide de la consultation, « Comment consulter les documents de mon espace partagé ? »
ANS, *Guide professionnel de santé – Consultation Mon espace santé/DMP*, septembre 2025
par Lukas MARA 121

Actualisation des critères de référencement des services et outils numériques dans Mon espace santé 123
Arrêté du 19 juin 2025 modifiant l'arrêté du 20 novembre 2023 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé, JORF n° 0147 du 26 juin 2025

e-CARTE VITALE 124

Approbation du référentiel d'utilisation de l'application carte Vitale comme moyen d'identification à distance 124
Arrêté du 5 février 2026 approuvant le référentiel fixant les critères applicables en vue de la délivrance de l'autorisation d'utilisation de la carte Vitale sous forme d'application mobile comme moyen d'identification à distance des utilisateurs, *JORF* n° 0034 du 10/02/2026

L'APPLICATION CARTE VITALE COMME MOYEN D'AUTHENTIFICATION À DISTANCE 124

SANTEXPO 2026 125

Le numérique en santé : synthèse des principaux enseignements de Santexpo 2026
GLOSSAIRE DES ABRÉVIATIONS 126
AVANT-PROPOS 127
BIBLIOGRAPHIE 138
par Thomas BOUDON 125

Droit belge

TÉLÉMATIQUE ET DOSSIERS MÉDICAUX PARTAGÉS 140

Soutien financier à l'utilisation de la télématique et des dossiers médicaux électroniques par les médecins 140
Arrêté royal modifiant l'arrêté royal du 30 juin 2017 fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux médecins pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux, *M.B* du 25/07/2025

Extension du soutien financier aux sage-femmes pour l'utilisation de la télématique 140
Arrêté royal fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux sage-femmes pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux en 2025, *M.B* du 30/10/2025

Droit espagnol

COOPÉRATION EN MATIÈRE DE SANTÉ NUMÉRIQUE 141

Resolución de 1 de diciembre de 2025, de la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, por la que se publica el Convenio con la Sociedad Española de Informática de la Salud, para impulsar la transformación digital del Sistema Nacional de Salud, « BOE » núm. 294, de 08/12/2025 141

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (SEIS). 141

MISE EN ŒUVRE DE L'EHDS EN ESPAGNE 142

Consultation publique sur l'avant-projet de loi relatif à la santé numérique 142
Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria

Droit irlandais

SANTÉ NUMÉRIQUE ET PROTECTION DES MINEURS // DIGITAL HEALTH AND ONLINE PROTECTION OF MINORS 143

Department of Health (An Roinn Sláinte), *Online Health Taskforce. Final Report : Online health and rights for Ireland's children and young people*, September 2025
par Thomas BOUDON 143

INFRASTRUCTURES NUMÉRIQUES DE SANTÉ // DIGITAL HEALTH INFRASTRUCTURES 151

Health Service Executive (HSE), *Digital for Care Capital Plan 2026*, December 2025
et
Department of Health (An Roinn Sláinte), *National Development Plan Review 2025 – Sectoral Investment Plan : Department of Health 2026–2030*, July 2025
par Thomas BOUDON. 151

EEDS – MISE EN ŒUVRE EN DROIT INTERNE // EHDS – DOMESTIC IMPLEMENTATION 154

***Health Information Act 2026*, No. 10 of 2026, signed into law by the President of Ireland on 30 April 2026**
par Thomas BOUDON 154

INTELLIGENCE ARTICIELLE EN SANTÉ // ARTIFICIAL INTELLIGENCE IN HEALHCARE 161

Department of Health (An Roinn Sláinte) & Health Service Executive (HSE), *AI for Care – The Artificial Intelligence (AI) Strategy for Healthcare in Ireland 2026–2030*, March 2026
par Thomas BOUDON 161

Droit italien

STRATÉGIE ITALIENNE DE SANTÉ NUMÉRIQUE POUR 2026 168

Ministère italien de la Santé, *Direttiva generale per l'attività amministrativa e la gestione (ai sensi degli articoli 4 e 14 del decreto legislativo 30 marzo 2001, n. 165), Anno 2026*
par Maddalena DE CARLO 168

Droit suédois

REMBOURSEMENT DES DISPOSITIFS MÉDICAUX NUMÉRIQUES 174

Reimbursement of Digital Medical Devices in Sweden
par Sarah DE HEER 174

VEILLE CONTENTIEUSE

Droit de l'Union européenne

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL 180

La notion de données personnelles au regard de la pseudonymisation
CJUE, 4 septembre 2025, *CRE / CRU*, aff. C-413/23 P, ECLI:C:2025:645
par Lili-Marie FERRANDO 180

TÉLÉMÉDECINE ET SOINS TRANSFRONTALIERS 185

La construction prétorienne de la notion de « télémédecine » dans le cadre des soins de santé transfrontaliers
A propos de l'arrêt de la Cour de justice de l'Union européenne du 11 septembre 2025, *UJ c. Österreichische Zahnärztekamme*, aff. C-115/24
CJUE, 11 septembre 2025, *Österreichische Zahnärztekamme*, aff. C-115/24, ECLI:EU:C:2025:694
par Salaheddine ZAHID 185

Droit français

ACCÈS AU DOSSIER MÉDICAL PARTAGÉ (DMP) 190

Accès au dossier médical partagé : *« pas sans le consentement initial du patient »* nous dit le Conseil d'État
CE, 10ème et 9ème chambres réunies, 15 octobre 2025, n° 490409, ECLI:FR:CECHR:2025:490409.2025101
par Joud GHARZEDDINE 190

CONSULTATION DU DOSSIER PATIENT INFORMATISÉ (DPI) 193

Consultation irrégulière de 441 dossiers médicaux : quand le Conseil d'État rappelle l'importance du consentement des patients pour la recherche
CE, 5ème chambre, 04 juillet 2025, n° 491701, ECLI:FR:CECHS:2025:491701.20250704
par Joud GHARZEDDINE 193

GOUVERNANCE DES DONNÉES DE SANTÉ 194

Commentaire sous l'arrêt du Conseil d'État, *Association Les Licornes célestes et autres c. CNIL*, 20 mars 2026 (n°s 503159 et 504171)
CE, Section du contentieux, 10ème chambre, 26 mars 2026, n°s 503159-504171, ECLI:FR:CECHS:2026:503159.20260320
par Chaimae HBA 194

Droit de l'Union européenne



Étude européenne sur le déploiement de l'IA dans les soins de santé

La Commission européenne (DG SANTE) publie en 2025 une étude consacrée au déploiement de l'intelligence artificielle (IA) dans les systèmes de santé européens. Réalisée à partir d'une revue de littérature, d'enquêtes, d'ateliers et d'études de cas, cette étude analyse à la fois les potentialités offertes par l'IA et les principaux obstacles à son intégration dans la pratique clinique.

Le rapport souligne que les systèmes de santé européens sont confrontés à plusieurs **défis structurels** : vieillissement de la population, augmentation des maladies chroniques, pénurie de professionnels de santé, hausse des dépenses de santé et surcharge administrative. Dans ce contexte, l'IA est présentée comme un levier susceptible d'améliorer l'efficacité opérationnelle des établissements de santé, de réduire les charges administratives et d'améliorer les parcours de diagnostic et de traitement.

Les usages considérés comme les plus prometteurs concernent notamment l'optimisation des flux hospitaliers et de l'allocation des ressources, l'automatisation des tâches administratives et de la documentation clinique, les outils d'aide au diagnostic, la médecine prédictive et personnalisée, ainsi que la télésurveillance et le triage des patients. L'étude cite plusieurs exemples concrets de déploiement dans les établissements de santé, notamment des outils utilisés dans les services d'urgence afin d'améliorer le triage des patients et de réduire les temps d'attente, des solutions déployées en radiologie et en oncologie pour améliorer les performances diagnostiques, ainsi que des outils conversationnels et des modèles de langage destinés à automatiser une partie de la documentation clinique et des tâches administratives.

Toutefois, malgré le potentiel identifié et la disponibilité croissante d'outils d'IA sur le marché, le rapport constate que leur déploiement dans la pratique clinique demeure encore lent. Plusieurs freins sont identifiés : difficultés liées à l'interopérabilité et à la gouvernance des données, insuffisance des infrastructures numériques, complexité du cadre réglementaire, enjeux de cybersécurité et de protection des données, ainsi que manque de confiance et de formation des professionnels et des patients. Le rapport souligne par exemple que certains outils d'IA utilisés dans les services d'urgence ou pour le triage des patients nécessitent une adaptation importante aux organisations locales et aux besoins médicaux

spécifiques. Il insiste également sur les difficultés rencontrées par les établissements de santé pour intégrer ces outils dans des systèmes d'information parfois peu interopérables et insuffisamment adaptés au traitement des données de santé à grande échelle.

Le rapport insiste enfin sur le fait que l'Union européenne dispose d'un cadre particulièrement favorable pour accompagner le développement d'une IA en santé qui soit sûre, efficace, éthique et respectueuse des droits fondamentaux des patients. Il met notamment en avant le rôle du cadre réglementaire européen — AI Act[1], règlement sur l'Espace européen des données de santé (EHDS)[2], RGPD[3] et règlements applicables aux dispositifs médicaux[4] — comme levier structurant pour encadrer et accompagner ce déploiement.

Dans cette perspective, l'étude formule plusieurs **pistes d'action** afin de favoriser une intégration durable de l'IA dans les systèmes de santé européens : développement de standards communs d'interopérabilité, soutien à des centres d'excellence et à des mécanismes de financement adaptés, renforcement des outils d'évaluation et de suivi du déploiement de l'IA en santé. Le rapport propose également un véritable cadre de suivi (« *monitoring framework* ») reposant sur des indicateurs et des mécanismes d'évaluation destinés à mesurer, dans le temps, le niveau de déploiement des outils d'IA, leurs effets sur l'organisation des soins et les difficultés rencontrées lors de leur mise en œuvre.

DG Santé, *Study on the deployment for AI in healthcare. Final report*, January 2024-2025, 241p.

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union et modifiant les règlements n° (CE) 300/2008, n° (UE) 167/2013 n° (UE) 168/2013, n° (UE) 2018/858, n° (UE) 2018/1139 et n° (UE) 2019/2144 et les directives n° (UE) 2014/90, (UE) 2016/797 et n° (UE) 2020/1828 (règlement sur l'intelligence artificielle – « AI Act »), *JOUE* n° L 2024/1689 du 12/07/2024.

[2] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/284, *JOUE* n° L 2025/327 du 05/03/2025.

[3] 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 (règlement général sur la protection des données – « RGPD »), *JOUE* n° L 119/1 du 04/05/2016.

[4] V. notamment, règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, *JOUE* n° L 117/I du 05/05/2017 et 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 (CE) 98/79 ainsi que la décision (UE) 2010/227 de la Commission, *JOUE* n° L 117/I du 05/05/2017.

Aperçu général sur le plan européen pour vaincre le cancer

Présenté par la Commission européenne en 2021, le Plan européen pour vaincre le cancer constitue l'une des principales stratégies européennes en matière de santé publique. Il vise à renforcer l'action de l'Union européenne tout au long du parcours de soins en cancérologie, depuis la prévention et le dépistage jusqu'au diagnostic, au traitement et à la qualité de vie des patients.
Parmi les initiatives structurantes prévues par ce plan figure notamment l'**initiative européenne en matière d'imagerie du cancer,** présentée comme l'une des actions phares du volet numérique et innovation.

La Cour des comptes européenne a par ailleurs publié en février en 2026 un rapport spécial consacré à la mise en œuvre du Plan européen pour vaincre le cancer, soulignant les avancées engagées mais également plusieurs défis persistants en matière de coordination, de financement et de déploiement opérationnel des actions prévues.



INITIATIVE EUROPÉENNE EN MATIÈRE D'IMAGERIE SUR LE CANCER

Initiative européenne en matière d'imagerie sur le cancer : action phare du plan européen pour vaincre le cancer

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Introduction

« Construire une Union européenne de la santé : renforcer la résilience de l'UE face aux menaces transfrontières pour la santé ». Tel était le titre de la communication de la Commission européenne du 11 novembre 2020 qui faisait état, dans le contexte de la lutte contre la pandémie de la Covid-19, de la nécessité de coordonner les actions nationales afin de garantir leur efficacité[5]. Ce constat ne se limite toutefois pas à ce contexte spécifique. Il pourrait même être légitimement soutenu qu'il n'émerge aucunement du fait de ce contexte. En effet, dès 2019, un combat est placé au centre des préoccupations de la Commission : la lutte contre le cancer[6]. Cette lutte silencieuse[7], portée tant par la Commission[8] que par sa présidente[9], se traduit par un engagement politique fort, baptisé le **plan européen pour vaincre le cancer**[10].

[5] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 11 novembre 2020, *COM(2020)* 724 final (consulté le 22/03/2026).
[6] En atteste le discours prononcé à la séance plénière du Parlement européen par la présidente de la Commission européenne, le 27 novembre 2019 (consulté le 24/03/2026).
[7] Communiqué de presse IP/21/342 de la Commission européenne sur le Plan européen pour vaincre le cancer : une nouvelle approche européenne de la prévention, du traitement et des soins, Bruxelles, le 3 février 2021 (consulté le 24/03/2024).
[8] En 2020, un cancer a été diagnostiqué chez 2,7 millions de citoyens européens et 1,3 ont perdu la vie. En l'absence de mesures concrètes dans ce domaine, les cas de cancer devraient augmenter de 24% d'ici à 2035, ce qui en ferait la cause principale de décès dans l'Union européenne. Ces chiffres, présentés par la Commission et repris dans le communique de presse *précité*, sont corroborés par ceux du Centre international de recherche sur le cancer de l'Organisation mondiale de santé qui prévoient une augmentation de 19,2% d'ici à 2035 en se basant sur le nombre de décès en Europe de cancer en 2022 (consulté le 31/03/2026).
[9] Dans le discours prononcé à la séance plénière du Parlement européen en 2019, *précité*, la présidente s'exprime en ces termes : *« Quand j'étais jeune fille, à Bruxelles, ma petite sœur est décédée d'un cancer à l'âge de 11 ans. Je me souviens du sentiment d'impuissance totale de mes parents – mais aussi du personnel médical qui lui a prodigué tant de soins. Chacun d'entre nous a une histoire semblable à raconter – ou connaît quelqu'un qui a vécu la même expérience. »*.
[10] L'ensemble des documents relatifs à ce plan sont disponibles sur la page web du site de la Commission qui lui est dédiée (consulté le 31/03/2026).

Ce plan se décline en plusieurs actions parmi lesquelles figure l'**initiative européenne en matière d'imagerie sur le cancer**. Cette dernière, lancée officiellement en décembre 2022, se décline elle-aussi en deux axes principaux. Le premier axe vise à mettre fin à l'éparpillement des données d'imagerie du cancer, ce qui limite leur réutilisation à des fins de recherche et d'innovation. La lutte contre cet éparpillement est ainsi placée au cœur du projet **EU**ropean Federation for **CA**ncer **Im**ages, dit aussi « EUCAIM » (I). Le second axe, dans le prolongement du premier, repose sur la centralisation des données au sein d'une infrastructure sécurisée. Cette centralisation faciliterait leur utilisation secondaire, nécessaire à la validation d'algorithmes d'intelligence artificielle (ci-après « IA) qui améliorent la prévention, le diagnostic et le traitement du cancer (II).

I. LA CENTRALISATION DES DONNÉES D'IMAGERIE DU CANCER, AU CŒUR DU PROJET EUCAIM

Le projet « EUCAIM » est la pierre angulaire du plan européen pour vaincre le cancer. Ce projet, lancé en janvier 2023 et financé dans le cadre du programme **DIGITAL**[11], met en œuvre l'initiative européenne en matière d'imagerie sur le cancer en déployant la plateforme **Cancer Image Europe**.

Il s'agit d'une infrastructure numérique, sécurisée et fédérée qui relie les initiatives européennes et nationales dans ce domaine ainsi que les différents réseaux et référentiels de recherche abritant de telles données. L'initiative s'appuie ainsi tout particulièrement sur les réalisations du réseau **AI for Health Imaging** (« AI4HI »), qui regroupe cinq grands projets financés par l'Union européenne sur le big data et l'IA dans le domaine susvisé[12]. Deux projets additionnels, financés dans le cadre du programme **EU4health**[13], étendent cette initiative autour du dépistage et de la détection précoce du cancer : **Unified Network for International Cancer Advancement**[14] et **Breast Image Platform for Advanced AI-Based Breast Cancer Screening**[15].

Face à ces nombreuses initiatives – européennes comme nationales – déjà entreprises dans ce domaine, une question se pose : *au vu de leur importance, quel intérêt présente réellement le déploiement de cette nouvelle infrastructure ?*

La réponse est à la fois claire et complexe, telle que le révèle l'explication même de cette initiative qui se situe au carrefour de plusieurs plans, programmes et stratégies. Le premier avantage résulte du fait qu'elle se bâtit autour d'une infrastructure *« unique »*. Cette caractéristique favorise le partage des données d'imagerie et la collaboration entre prestataires de soins de santé, chercheurs et innovateurs de plusieurs pays. En effet, si les nombreuses initiatives en la matière ont donné naissance à des référentiels d'imagerie, ceux-ci sont souvent spécifiques à un projet, limités dans le temps et *de facto* restreints dans la capacité à être réutilisés[16].

[11] Selon le site dédié à ce programme, DIGITAL – plus connu sous le nom de *programme pour une Europe numérique* – est un programme de financement de l'Union européenne qui vise à apporter la technologie numérique aux entreprises, aux citoyens et aux administrations publiques (consulté le 30/03/2026).

[12] Il s'agissait des projets suivants : Chaimeleon, EuCanImage, ProCancer-I, Incisive et Primage. Une explication détaillée de chacun de ces projets est disponible en ligne (consulté le 30/03/2026).

[13] Pour plus d'informations concernant ce programme, se référer à la page web de la Commission européenne qui lui est dédiée.

[14] https://www.unica-project.eu/.

[15] https://cancerimage.eu/breastscan/.

[16] Carina SOLER PONS,Ana DE MARCO GARCIA, Ricard MARTINEZ et *al.*, « How the First Medical Imaging Cancer Atlas EUCAIM Was Populated : The Experience of a Reference Hospital [Version 3; Peer Review: 2 Approved, 1 Approved with

Le second avantage résulte, quant à lui, du fait que l'infrastructure a été conçue dans le respect des règlementations européennes relatives aux données personnelles, à savoir le règlement général sur la protection des données (RGPD)[17], le règlement européen sur l'intelligence artificielle (AI Act)[18] et plus récemment le règlement relatif à l'espace européen des données de santé (EHDS)[19]. Elle constitue donc un cadre sécurisé dans lequel le traitement licite des données personnelles est assuré. Cela favorise l'utilisation secondaire de ces dernières, élément indispensable à la validation de toute innovation fondée sur l'IA.

II. UN CADRE INSTITUTIONNEL SECURISE, FAVORABLE A L'INNOVATION PAR UN ACCÈS MASSIF AUX DONNÉES

« Si nous souhaitions créer des technologies novatrices dans le domaine du cancer, il faut permettre l'accès à une masse critique de données »[20] affirmait Marco Marsella lors de l'évènement de lancement de l'initiative en matière d'imagerie sur le cancer en 2023. La plateforme **Cancer Image Europe** assure aisément cet accès en ce qu'elle vise à rassembler, d'ici la fin de 2026, *« plus de 100 000 cas et 60 millions d'images »*. Ces données sont de haute qualité et respectent des normes communes concernant leur anonymisation, leur standardisation, leur annotation et leur curation[21]. De plus, l'utilisabilité de l'infrastructure suit les principes FAIR[22], ce qui implique que les données soient *« traçables, accessibles, interopérables et réutilisables »*[23].

Cet accès massif à des données standardisées permet *« la réalisation d'études de validation de l'IA à grande échelle et multicentriques »*. Il aide à produire des preuves quant à *« l'utilité clinique des solutions d'IA »*, de nature à accélérer leur déploiement dans des environnements cliniques réels. En effet, s'il n'est nullement contesté aujourd'hui que les outils numériques intégrant l'IA améliorent significativement l'exactitude des diagnostics et permettent une détection précoce, l'obstacle[24] qui perdure est celui de renforcer la confiance dans l'IA. L'EUCAIM relève cet obstacle, expliquant le rôle central qui lui est octroyé dans la réalisation des objectifs de la stratégie **Appliquer l'IA**[25].

Reservations] », *Open Res Europe 2025*, vol. 5, n° 310 (consulté le 22/03/2026).

[17] Règlement (UE) 2016/679 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.

[18] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements n° (CE) 300/2008, n° (UE) 167/2013, n° (UE) 168/2013, n° (UE) 2018/858, n° (UE) 2018/1139 et n° (UE) 2019/2144 et les directives n° (UE) 2014/90, (UE) 2016/797 et n° (UE) 2020/1828 (règlement sur l'intelligence artificielle).

[19] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° (UE) 2011/24 et le règlement n° (UE) 2024/2847.

[20] Traduction libre de la prise de parole de M. Marco MARSELLA, à l'époque chef de l'unité « eHealth, Well-Being, Ageing », lors de l'évènement de lancement de l'initiative en matière d'imagerie sur le cancer en janvier 2023 (consulté le 22/03/2026).

[21] Carina SOLER PONS et *al.*, *précité*.

[22] Luis MARTI-BONMATI, Ignacio BLANQUER, Manolis TSIKNAKIS et *al.*, « Empowering cancer research in Europe : the EUCAIM cancer imaging infrastructure », *Insights Imaging*, vol. 16, n° 47, 2025 (consulté le 22/03/2026).

[23] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

[24] Pour une liste plus détaillée des Défis liés à l'intégration de l'IA dans les soins de santé, voir : https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_fr.

[25] Il s'agit de la stratégie sectorielle globale de l'Union européenne en matière d'intelligence artificielle. Pour plus d'informations, se référer à la page web du site de la Commission qui y est dédiée.

Conclusion

L'étude de l'initiative européenne en matière d'imagerie sur le cancer nous amène à un constat : l'Union européenne bâtit, initiative par initiative, stratégie par stratégie et plan par plan, un écosystème favorable à l'innovation et à la recherche fondée sur l'IA. Elle vise à se placer en tête du combat contre le cancer, sans pour autant négliger la protection accrue que réserve sa législation aux données de santé. Il en résulte une Union qui, *« Unie dans la diversité »,* devient une Union *« Unie dans l'Unique »*[26]

[26] Il s'agit du thème de la Journée Mondiale contre le Cancer 2025-2027.

INITIATIVE EUROPÉENNE « +1 MILLION GENOMES » (1+MG°)

L'initiative européenne « 1+ Million Genomes » (1+MG) *constitue l'une des principales actions européennes en matière de données génomiques et de médecine personnalisée. Lancée en 2018, elle vise à favoriser le partage sécurisé de données génomiques et cliniques à l'échelle européenne afin de soutenir la recherche et l'innovation. Son objectif est de permettre la mise à disposition de plus d'un million de génomes pour améliorer la prévention, le diagnostic et la prise en charge de nombreuses pathologies, notamment les cancers et les maladies rares.*

Émergence d'une infrastructure européenne fédérée au service de la génomique et de la médecine personnalisée

Le Genomic Data Infrastructure (GDI), dans le cadre de l'initiative européenne « 1+ Million Genomes » (1+MG)

par Salaheddine ZAHID

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Le développement de la médecine personnalisée constitue aujourd'hui l'un des axes les plus structurants de l'évolution contemporaine des systèmes de santé. Les progrès réalisés dans les technologies de séquençage ont transformé les capacités d'analyse du génome humain, permettant la production massive de données génétiques exploitables à des fins diagnostiques, thérapeutiques et préventives. La génomique occupe désormais une place centrale dans des domaines tels que les maladies rares, l'oncologie de précision, la pharmacogénomique ou encore la médecine prédictive[27].

Cette évolution scientifique s'accompagne d'un défi majeur, à savoir que la valeur clinique et scientifique des données génomiques dépend de leur capacité à être comparées et exploitées à grande échelle.

Or, les données génomiques européennes demeurent fragmentées. Elles sont produites et conservées au sein d'infrastructures nationales, de centres hospitaliers, de biobanques ou de programmes de recherche qui se reposent sur des standards techniques, des terminologies et des cadres juridiques hétérogènes[28].

Face à la dispersion des bases nationales et aux contraintes légales, l'Union européenne a lancé en 2018 l'initiative *1+ Million Genomes* (1+MG)[29]. Vingt-six pays européens[30] ont signé une déclaration visant à permettre un accès sécurisé et transfrontalier aux données génomiques européennes afin de soutenir la recherche médicale, les politiques de

[27] Voir en ce sens, l'initiative européenne « 1+ Million Genomes » ; et la note d'orientation « Genomics in Healthcare. Key issues for implementation ».

[28] Voir en ce sens, la fiche technique « D8.2 Integration of genomics and phénotypic data » publiée le 3 février 2026 ; et la feuille de route B1MG 2023-2027.

[29] Déclaration de coopération, « Towards acess to at least 1 million sequenced genomes in the European Union by 2022 », Bruxelles, 10 avril 2018.

[30] Plus le Royaume-Uni et la Norvège.

santé publique et le développement de la médecine personnalisée. La déclaration identifie trois objectifs principaux : la mise en place d'une infrastructure technique permettant un accès fédéré sécurisé aux données génomiques ; le développement d'un cadre éthique et juridique adapté ; ainsi que l'intégration progressive de la génomique dans les systèmes européens de santé.

Pour concrétiser cette vision, le projet *Genomic Data Infrastructure* (GDI) a été conçu comme l'instrument technique majeur de la phase d'extension du *1+ MG*. Il ne centralise pas les données, au contraire, il définit une architecture fédérée (**I**) où chaque pays conserve ses propres référentiels[31]. Le GDI met en place les interfaces et standards techniques nécessaires[32] pour permettre des requêtes inter-systèmes[33]. Les ensembles de données demeurent donc sous le contrôle des infrastructures numériques nationales (**II**), tandis que le GDI organise les mécanismes d'interrogation, de découverte et de coordination des accès. Cette architecture repose sur des standards ouverts développés notamment par la *Global Alliance for Genomics and Health*, afin de garantir l'interopérabilité entre les systèmes nationaux[34].

I. UNE ARCHITECTURE EUROPÉENNE FEDÉRÉE AU SERVICE DE LA GÉNOMIQUE

Sur le plan opérationnel, le GDI repose sur plusieurs fonctions essentielles : découverte des données, traitement des requêtes, gestion des accès, stockage sécurisé et réception des résultats[35]. Les travaux préparatoires du projet *Beyond One Million Genomes* (B1MG) ont notamment permis de tester plusieurs services interopérables fondés sur les standards de la GA4GH destinés à interroger des bases distribuées notamment afin de « *[o]ffers the possibility to query for the annotations on the variants found, including expert or clinician conclusions — when available — on the pathogenicity of a specific mutation in an individual or its contribution to a particular phenotype* »[36].

[31] Cette approche s'inscrit dans une évolution des pratiques scientifiques en génomique. Les premiers systèmes de partage des données reposaient essentiellement sur des modèles centralisés impliquant le transfert des données vers des dépôts communs. Comme le souligne un article publié le 4 mars 2019 sur le site Nature Biotechnology, *Federated discovery and sharing of genomic data using Beacons*, par plusieurs contributeur.ices, « *many former systems for genomic data sharing have followed a centralized model* […]. *This model requires data generators to transfer whole copies of datasets over the internet, which will become inefficient and expensive as the rate of genomic data acquisition increases. An alternative, federated model for data sharing*[1] *requires organizations to host data independently and to interoperate via an agreed-upon technical language. This model removes the inefficiencies of large data transfers and gives host organizations more control over data privacy, security and representation".*

[32] Pour les aspects techniques, des fiches d'avancements et comptes rendus du projet sont publiées régulièrement sur la page web.

[33] Les documents techniques du projet précisent explicitement que « *data does not need to leave the country of origin* » (GDI « D8.2 Integration of genomics and phénotypic data » précité).

[34] Voir en ce sens « Technical GA4GH Technical Standards Documentation. Policy and processes for developing and communicating maturity of GA4GH Technical Specifications » , 17 September 2025.

[35] Voir en ce sens la documentation B1MG Technical Infrastructure .

[36] Des infrastructures telles que de type *Beacon* dont les bénéfices sont exposés sur le site . Concrètement, un clinicien ou un chercheur peut adresser une requête portant sur un variant donné et recevoir une réponse indiquant si ce variant est présent dans une ou plusieurs bases de données européennes, sans que les données sous-jacentes ne soient transmises. Cette logique est importante dans le domaine des maladies rares, où l'identification de variantes similaires observés dans d'autres pays peut accélérer le

Le GDI repose également sur des mécanismes de gouvernance des accès particulièrement structurés. Les demandes d'accès aux données sont examinées par des *Data Access Committees*, chargés d'évaluer les conditions scientifiques, éthiques et juridiques d'utilisation des données[37]. Les travaux du projet mentionnent également l'utilisation d'outils tels que le *Resource Entitlement Management System (REMS)*, destiné à gérer les autorisations d'accès et les droits des utilisateurs[38].

Le projet doit également composer avec les exigences du Règlement général sur la protection des données de 2016[39], les données génomiques constituant des données sensibles au sens de l'article 9 dudit règlement. L'architecture fédérée permet précisément de limiter les transferts transfrontaliers de données tout en intégrant les principes de « *Data Protection by Design and Default* » prévus à l'article 25 du RGPD[40]. Les mécanismes d'accès distribués permettent ainsi de concilier exploitation scientifique des données et maintien d'un haut niveau de protection des personnes.

Le GDI intègre également une dimension stratégique de confiance et d'acceptabilité sociale. Les documents du projet soulignent l'importance d'une communication destinée à informer les citoyens sur les garanties de sécurité, de gouvernance et d'utilisation responsable des données[41]. Cette question apparaît essentielle dans un contexte où la confiance conditionne directement l'acceptabilité du partage des données génomiques. À cet égard, les professionnels de santé occupent un rôle central dans l'explication des

---

diagnostic et améliorer la caractérisation des pathologies. En oncologie, l'accès à des cohortes européennes permet d'affiner l'interprétation des variants tumoraux et de soutenir le développement de traitements personnalisés (voir en ce sens l'initiative européenne en matière d'imagerie sur le cancer).

[37] Voir en ce sens « Beyond 1 Million Genomes (B1MG) D2.4 Report on data access and governance framework », 5 otobre 2023. Sur les *Data Access Committees*, voir le site internet de la European Genome-Phenome Archive, *What is a DAC ?*.

[38] *Secure cross-border data access roadmap*, version du 23 novembre 2021.

[39] 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 (CE) 95/46 (règlement général sur la protection des données).

[40] L'article 25 du RGPD dispose que : « *1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. 2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.* » ; voir également REGINA Becker et autres « B1MG / 1+MG: IT infrastructure requirements based on a data protection by design and default approach », 4 août 2022.

[41] Deliverable D1.8 Wider Communication Strategy - final evaluation and review, 27 février 2026.

mécanismes de protection et dans l'accompagnement des patients.

Les bénéfices attendus sont alors considérables. L'agrégation fonctionnelle de données issues de plusieurs pays permettrait de constituer des cohortes élargies particulièrement utiles pour les maladies rares et les maladies complexes. Le développement de l'IA appliquée à la santé faciliterait l'accès à des jeux de données plus diversifiés et représentatifs. À long terme, les analyses de ces vastes bases de données pourraient contribuer à renforcer les politiques de santé publique, notamment en matière de prévention, de surveillance épidémiologique ou d'identification précoce des facteurs de risque.

II. LES LIMITES ET DÉFIS DE L'EFFECTIVITE DU *GENOMIC DATA INFRASTRUCTURE*

Toutefois, malgré ces ambitions, le projet demeure confronté à plusieurs limites importantes. Les capacités nationales de séquençage et de structuration des données restent asymétriques. Les données publiées sur les tableaux de bord de l'initiative montrent des écarts entre États membres[42]. Ces disparités reflètent des différences majeures de capacités techniques, financières et institutionnelles en ce qu'elles limitent mécaniquement l'effectivité du GDI et la disponibilité homogène des données génomiques à l'échelle européenne[43].

L'interopérabilité constitue également un défi majeur. Malgré le recours à des standards ouverts, les infrastructures nationales utilisent encore des formats de données, des terminologies cliniques et des référentiels différents[44]. Les documents techniques du projet identifient ainsi des phénomènes de « *geographical, technical, incompatibility, legal and regulatory divergence, semantic barriers* »[45]. Des efforts importants d'harmonisation demeurent donc nécessaires pour assurer une exploitation cohérente des données génomiques à l'échelle européenne.

Enfin, la question de la confiance reste centrale. Toute faille de sécurité ou utilisation abusive des données génomiques pourrait fragiliser la légitimité du projet. Le succès du GDI dépendra donc autant de la robustesse de son architecture technique que de sa capacité à maintenir un haut niveau de protection des données et de transparence vis-à-vis des citoyens.

Dès lors, le GDI apparaît comme l'un des fondements potentiels d'un futur espace européen intégré de médecine personnalisée, dans l'exploitation des données génomiques tout en respectant les enjeux juridiques et éthiques qui structurent la santé numérique européenne.

[42] Renvoi au *1+MG Dashboard Data*. L'Italie se distinguant en ce qu'elle possède 27 datasets contrairement au Danemark qui en a une. Les données génomiques de la France n'étant pas disponibles.

[43] Le projet prévoit qu'au moins quinze pays disposent d'une infrastructure opérationnelle en 2026 (B1MG feuille de route 2023-2027), mais plusieurs États restent loin de cet objectif.

[44] GDI D8.2 précité.

[45] *Ibid.*



INITIATIVE EUROPÉENNE SUR LES JUMEAUX HUMAINS VIRTUELS (VHT)

L'initiative européenne sur les « jumeaux humains virtuels » (« Virtual Human Twins » – VHT) *s'inscrit dans la stratégie européenne de développement de l'IA appliquée à la santé. Elle vise à favoriser l'émergence de représentations numériques du corps humain destinées à mieux comprendre, simuler et anticiper l'évolution des pathologies, dans une logique de médecine personnalisée.*

Commission européenne, European Virtual Humain Twins (VHT) Initiative

par Noémie DUBRUEL

Docteure en Droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Le recours à différents outils numériques, dont l'intelligence artificielle, dans le domaine de la santé permet la création de nombreuses méthodes qui présentent un intérêt considérable pour l'amélioration de la santé, de la recherche et de l'innovation. Parmi celles-ci figure le jumeau humain virtuel (*Virtual Human Twin, VHT*). Ce dernier est défini par la Commission européenne comme une « représentation numérique intégrée à plusieurs niveaux, dans le temps et selon plusieurs disciplines d'un corps, d'un organe ou d'une cellule, permettant la caractérisation complète de l'état physiologique et pathologique dans son hétérogénéité »[46].

S'appuyant sur plusieurs technologies de modélisation et de simulations informatiques, d'intégration de données et de modèles de calcul, cette méthode apparaît particulièrement pertinente pour accélérer l'émergence d'une médecine plus prédictive, préventive et personnalisée. Les VHT présentent alors des opportunités de ciblage des préventions et des parcours cliniques et sont un véritable soutien pour les professionnels de santé et les chercheurs. En effet, ils peuvent particulièrement être sollicités pour la mise en œuvre d'essais cliniques, la formation des professionnels de santé ou bien encore la planification des interventions chirurgicales, par exemple.

Forte des opportunités offertes par ces usages numériques innovants, la Commission européenne a fait le choix d'investir dans leur déploiement, à travers la mise en œuvre d'une initiative spécifique, lancée en décembre 2023 et intitulée « *The European Virtual Human Twins Initiative* »[47]. Le premier objectif poursuivit vise à pallier l'évidente fragmentation de l'écosystème européen dans ce domaine. En effet, si un grand nombre d'innovations émergent en Europe, dans un contexte où le « jumeau numérique » emporte de plus en plus d'intérêt, les méthodes, usages et même terminologies demeurent très disparates, freinant considérablement la

[46] Site officiel de l'initiative : https://www.virtualhumantwins.eu/, (consulté le 30/04/2026).

[47] Commission européenne, "European Virtual Human Twins", Infographics, décembre 2023, p.01.

reconnaissance de cette innovation. Plus encore, la Commission européenne poursuit un objectif fort par le souhait de « renforcer les capacités avancées de supercalcul et l'intelligence artificielle afin de faciliter la recherche collaborative et le développement technologique en matière de VHT ». Afin de répondre à ces attentes, la Commission européenne a d'abord fait le choix de la publication d'un manifeste, officiellement rendu public le 21 décembre 2023, illustrant parfaitement la nécessité de rassembler les différentes forces vives européennes et diverses parties prenantes autour d'une volonté européenne affirmée. Le manifeste, qui a obtenu une centaine de signatures[48], favorise des coopérations et collaborations interdisciplinaires et établit plusieurs pistes d'actions : atteindre un niveau d'excellence européen pour la recherche et l'innovation, identifier des cas d'usage à fort impact clinique et scientifique, valoriser des données et modèles de VHT européens, accompagner et clarifier le paysage réglementaire en la matière, générer des preuves numériques, contribuer à la bonne compréhension des usages des méthodes de VHT et enfin garantir le recours à une technologie au bénéfice du plus grand nombre, permettant un « accès équitable et universel à des traitements sûrs et de qualité »[49].

En complément, diverses actions de recherche et de déploiement alimentent cette initiative. En premier lieu, le projet européen « VHT » (EDITH) permet l'élaboration d'une action de coordination et de soutien financée au titre du programme DIGITAL[50]. Ce projet se veut mettre en évidence les leviers et points bloquants pour le déploiement des VHT en Europe, dans les domaines de la santé et de la recherche, au bénéfice des patients, des professionnels de santé, des régulateurs et de l'industrie. En ce sens, un chantier essentiel réside dans la cartographie et la structuration d'un écosystème collaboratif et inclusif à l'échelle européenne, fondé sur un consensus entre les parties prenantes. De même, le projet insiste sur l'importance de produire une feuille de route permettant de passer des modèles existants (souvent limités à un organe ou à un système) à un VHT multi-échelle, multi-organes, intégré et fondé sur les données et les connaissances.

Par ailleurs, l'initiative repose sur des financements complémentaires générés au titre du programme « Horizon Europe » ainsi que de l'initiative en matière de santé innovante[51] pour de meilleurs suivis et visualisations des accidents vasculaires cérébraux via l'usage de modèles de calcul prédictifs et de données intégrées.

Enfin, le programme pour une Europe numérique (DIGITAL) est source de soutien pour l'initiative VHT en ce qu'il permet le financement d'une plateforme numérique de pointe pour l'intégration et la validation de modèles de jumeaux humains virtuels. Initié le 26 juin 2025, le processus de développement d'une plateforme met en évidence la forte volonté de la Commission européenne de déployer les générations et les usages des VHT en se positionnant comme moteur en la matière. Annoncée dans le « programme de travail pour une Europe numérique 2023-2024 », la création de cette plateforme s'inscrit largement dans la volonté européenne de mettre en œuvre une stratégie d'intelligence artificielle[52]. Cette récente avancée met également en exergue le souhait primordial de la Commission européenne de placer sur le

[48] Commission européenne, "European Virtual Human Twins (VHT) Initiative" (consulté le 30/04/2026).

[49] Commission européenne, "Virtual Human Twins Manifesto", Manifesto, décembre 2023, p.03.

[50] Commission européenne, "EDHITH. Building the European Virtual Human Twin", livrable 3.2 "VHT roadmap", décembre 2024, 362p.

[51] Site officiel de l'initiative en matière de santé innovante : https://www.ihi.europa.eu/, (consulté le 30/04/2026).

[52] European Commission, "ANNEX to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025- 2027", Digital Europe Programme, *C(2025)* 1839 final, Brussels, 28 march 2025, p.16 et p.79.

devant de la scène les différents acteurs des modèles VHT (chercheurs, innovateurs et cliniciens) afin, non seulement, de les solliciter dès les prémices de la mise en œuvre de cette plateforme, mais également de leur offrir un maximum d'outils et de ressources pour déployer, connecter, articuler et valider les modèles et méthodes VHT. Le choix d'intégrer les utilisateurs de la plateforme dès sa conception participe à l'acceptation de cette dernière. Ainsi, les utilisateurs futurs peuvent exprimer leurs besoins, souhaits ou inquiétudes concernant la création de cet espace de partage. Les objectifs poursuivis par cette plateforme sont multiples : fournir aux divers acteurs des secteurs publics et privés un espace commun d'intégration voire de génération des modèles ; assurer un espace d'accès à des technologies de pointe, à des modèles de calcul, à des données synthétiques, voire directement à des modèles VHT[53]. Assurément, l'initiative insiste sur l'importance que de fortes garanties de protection des droits de propriété intellectuelle et de cybersécurité soit assurées lors de l'usage de la plateforme.

Enfin, la Commission européenne annonce souhaiter passer une étape importante afin de combler le fossé entre la génération, la mise sur le marché et l'adoption des VHT dans les établissements de santé et organismes de recherche[54]. Pour cela, l'initiative soutient la création d'un incubateur[55], dit « VHT Uptake » correspondant à « un centre de partage des connaissances, de mise en réseau, de coopération et de collaboration »[56].

À travers cette initiative, la Commission européenne affirme sa volonté de positionner l'Europe comme un réel acteur moteur dans la création et l'usage d'innovations numériques qui semblent révolutionner les manières de considérer la santé et de faire de la recherche. Pour autant, ce tournant numérique ne peut se faire sans garantir une réelle acceptabilité de ces nouveaux usages et, de fait, une prise en compte concrète et précoce de l'ensemble des acteurs, concernés par les préoccupations tant technologiques et scientifiques qu'éthiques et réglementaires. Si cette initiative présente un réel intérêt pour le déploiement des méthodes VHT en Europe, il s'agit de vérifier si la création d'un tel écosystème participatif peut perdurer et rester à la pointe d'une technologie qui évolue si rapidement.

[53] En ce sens, la Commission européenne prévoit que la plateforme puisse offrir certaines spécificités d'accès en *open source*, sans que ces dernières ne soient définies à ce jour.

[54] European Commission, "ANNEX to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025- 2027", *Op. Cit.,* p.79.

[55] *Ibid*., pp.79-80.

[56] Commission européenne, « Plate-forme pour les modèles VHT (Advanced Virtual Human Twin) », (consulté le 30/04/2026).

Les jumeaux humains virtuels

par Alizée FERNANDEZ

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Si la médecine s'est longtemps attachée à soigner un corps tangible, fait de chair et d'os, elle est aujourd'hui confrontée à une nouvelle réalité : celle de gouverner son double de données. La simulation numérique tend ainsi à devenir un outil central de la décision clinique, ouvrant, par ricochet, un champ inédit pour le droit.

Après vingt ans de transition numérique centrée sur la gestion administrative et la dématérialisation des dossiers médicaux, l'innovation en santé prend désormais un tournant majeur avec la modélisation du vivant. Initialement conçue pour l'ingénierie aéronautique et automobile afin de simuler le comportement de systèmes complexes et prévenir leurs défaillances, la technologie du jumeau numérique a récemment été adaptée au domaine médical. Ce passage de la machine à l'organisme humain transforme profondément la nature et la portée de cette technologie.

En santé, le Virtual Human Twin (VHT), ou jumeau humain virtuel, est une représentation mathématique et dynamique d'un patient ou d'un organe. Ce n'est pas une image figée, mais un modèle évolutif, constamment alimenté par des données médicales, biologiques, comportementales et environnementales. L'objectif n'est pas de reproduire intégralement un individu, ce qui est à la fois irréaliste d'un point de vue technique aujourd'hui et éthiquement délicat, mais de créer une représentation suffisamment fidèle pour tester des hypothèses de soins sans exposer directement le patient à un risque.

L'enjeu est considérable. Le jumeau numérique porte la promesse d'une médecine plus personnalisée, plus prédictive et plus précise, capable d'anticiper l'évolution d'une pathologie ou la réponse d'un patient à un traitement donné. Toutefois, cette promesse s'accompagne de tensions profondes. Le corps humain ne se réduit pas à un système mécanique : il est traversé par une histoire, une subjectivité et des choix. L'essor des VHT soulève ainsi des interrogations majeures relatives à la protection des données de santé, à la responsabilité en cas d'erreur algorithmique et au risque de réduire la personne à une simple agrégation de variables numériques.

Conscients de ces enjeux, les pouvoirs publics européens ont structuré le développement des jumeaux humains virtuels autour d'une architecture hybride, au confluent de la stratégie industrielle et de la régulation des données. Dès lors, comment l'Union européenne (UE) parvient-elle à pallier ses limites de compétence par des mécanismes de coordination stratégique, tout en instaurant via l'Espace européen des données de santé (EHDS), un cadre normatif indispensable à l'interopérabilité des données nécessaires au déploiement des jumeaux virtuels ?

L'architecture de ce dispositif repose sur le fondement de l'initiative entre soft law et stratégie de coordination (I), laquelle se déploie à travers l'Espace européen des données de santé comme levier d'interopérabilité et d'exploitation systémique des données de santé (II).

I. LE FONDEMENT DE L'INITIATIVE : ENTRE SOFT LAW ET STRATÉGIE DE COORDINATION

L'initiative VHT privilégie une approche pragmatique au sein de l'UE, où la contrainte législative s'efface au profit d'une convergence stratégique des acteurs. Lancé le 21 décembre 2023, le Manifeste pour les jumeaux humains virtuels constitue

la pierre angulaire de cette approche[57]. En tant qu'instrument de droit souple, cette déclaration d'intention sur le développement collaboratif des VHT et leur adoption accrue dans l'ensemble de l'UE, ne crée pas d'obligations juridiques contraignantes au sens de l'article 288 du Traité sur le fonctionnement de l'UE (TFUE). Toutefois, sa portée ne doit pas être sous-estimée car il remplit une fonction de pré-normalisation. En recueillant l'adhésion volontaire des chercheurs, des professionnels de santé, des innovateurs de l'industrie, des décideurs politiques et des autorités des États membres, il installe un consensus sur des standards éthiques et techniques communs. Cette coopération permet à la Commission européenne de structurer un secteur technologique émergent avant même que le législateur ne vienne codifier ces pratiques garantissant ainsi une unité d'action sans passer par le temps long de la navette législative.

Cette stratégie de coordination apparaît d'autant plus pertinente que l'action de l'Union en matière de santé est encadrée par un cadre constitutionnel strict. En vertu de l'article 168 du TFUE, la santé publique relève principalement d'une compétence d'appui (dite aussi « de coordination » ou de complément). Conformément à l'article 168§7, l'Union doit respecter la responsabilité des États membres dans la définition de leurs politiques de santé ainsi que dans l'organisation et la fourniture des soins et de plus, toute harmonisation législative directe est exclue dans le cadre de cet article. L'Union dispose par ailleurs d'une compétence partagée avec les États membres pour les enjeux communs de sécurité en matière de santé, conformément à l'article 168§4 du TFUE, qui autorise le Parlement européen et le Conseil à adopter des mesures fixant des normes élevées de qualité et de sécurité des organes et substances d'origine humaine, du sang et des dérivés du sang (art. 168 §4 a)), des mesures dans les domaines vétérinaire et phytosanitaire ayant directement pour objectif la protection de la santé publique (art. 168 §4 b)), ainsi que des mesures fixant des normes élevées de qualité et de sécurité des médicaments et des dispositifs à usage médical (art. 168 §4 c)).

Les jumeaux humains virtuels n'entrant pas dans ces catégories, la Commission européenne a choisi de les appréhender comme un objet de haute technologie, assimilable à un logiciel ou à une infrastructure de données, plutôt que comme un acte médical stricto sensu.

Ainsi on pourrait considérer qu'au sens de l'article 3§1 de l'IA Act[58], un VHT constituerait un système d'IA dès lors qu'il déduit, à partir des données médicales qu'il reçoit, la manière de générer des sorties telles que des prédictions ou des recommandations susceptibles d'influencer une décision clinique. Cette qualification acquise, le règlement appelle une classification par niveau de risque. Or, l'annexe III du règlement, qui liste limitativement les systèmes d'IA à haut risque, ne prévoit aucune catégorie dédiée aux outils de simulation médicale. Le rattachement le plus plausible serait celui du point 5 d), qui vise les systèmes d'IA utilisés pour le tri des patients dans les services d'urgence, ce qui pourrait couvrir un VHT à visée pronostique en soins intensifs, mais reste insuffisant pour couvrir l'ensemble des usages cliniques des jumeaux numériques. Par ailleurs, lorsque le VHT est intégré comme composant de sécurité d'un dispositif médical au sens du règlement (UE) 2017/745, qui figure à l'annexe I, point 11 de l'IA Act, et que ce dispositif est soumis à une évaluation de conformité par un tiers, l'article 6§1 entraîne sa

[57] « Lancement de l'initiative européenne sur les jumeaux humains virtuels », *Digital Strategy*, 21 déc. 2023.

[58] Règlement (UE) 2024/1689/UE du 13 juin 2024 sur l'intelligence artificielle du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* n° L 2024/1689 du 12/07/2024.

qualification automatique de système à haut risque, indépendamment de tout rattachement à l'annexe III[59]. Si l'IA Act peut donc offrir des pistes de qualification en fonction de la finalité d'usage du VHT, force est de constater qu'à ce jour aucune qualification juridique n'a été officiellement retenue, ce qui n'empêche pas des initiatives telles que celle mentionnée.

En effet, en intervenant sur les infrastructures technologiques qui conditionnent l'exercice des soins, l'UE respecte les limites de l'article 168 du TFUE, tout en exerçant une influence indirecte sur les pratiques médicales nationales. Cette approche est renforcée par le recours aux instruments de la politique industrielle, qui permettent à l'UE, conformément à l'art 173 du TFUE, de soutenir la compétitivité de son industrie. Ainsi, dans le cadre du programme politique de la « Décennie numérique 2030 », la Commission mobilise l'European Digital Infrastructure Consortia (EDIC), mis à la disposition des Etats membres afin de faciliter la mise en oeuvre de projets multinationaux de grande ampleur[3]. En rattachant l'initiative VHT à ce dispositif, le développement des jumeaux humains virtuels s'inscrit dans une dynamique de souveraineté technologique et de concurrence mondiale[60].

Toutefois, la coordination institutionnelle et la politique industrielle ne suffisent pas à garantir le déploiement effectif des jumeaux humains virtuels. Leur viabilité dépend avant tout de la circulation et de l'interopérabilité des données de santé, ce qui rend indispensable leur articulation avec le cadre normatif de l'EHDS (**II**).

II. L'ESPACE EUROPÉEN DES DONNÉES DE SANTE COMME LEVIER D'INTEROPERABILITE : VERS UNE EXPLOITATION SYSTEMIQUE DES DONNÉES DE SANTE

Bien que des prototypes de jumeaux numériques d'organes isolés existent déjà, à l'instar du projet « Living Heart » pour la cardiologie ou du projet « NeuroTwin » pour les pathologies cérébrales, créer un jumeau du corps humain entier est encore impossible aujourd'hui. Les freins au déploiement des jumeaux numériques résultent de la complexité du fonctionnement du corps humain dans son entièreté mais aussi du manque d'accès à des données de santé massives et hétérogènes. Actuellement cantonnés à des projets de recherches spécifiques, ces modèles pourront profiter des opportunités offertes par la création de l'Espace européen des données de santé.

Entré en vigueur le 26 mars 2025, le Règlement (UE) 2025/327 établissant l'EHDS instaure un cadre juridique et infrastructurel propre au secteur sanitaire. S'il garantit d'abord aux patients un accès transfrontalier à leurs dossiers médicaux électroniques via l'utilisation primaire des données de santé, il opère surtout un changement de paradigme pour le développement des jumeaux numériques grâce à son régime d'utilisation secondaire. Ce mécanisme autorise la réutilisation sécurisée des informations à des fins de recherche et d'innovation, dépassant la seule finalité de soins. En effet, un modèle de simulation cardiaque ou neurologique n'a de valeur prédictive que s'il est alimenté par des milliers de trajectoires de patients réels, ce que le cadre contractuel préexistant rendait impossible à l'échelle européenne. Sur le plan juridique, cette articulation

[59] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030, *JOUE* n° L 323 du 19/12/2022.

[60] « Virtual Human Twins », Digital Strategy.

garantit que le traitement des données pour l'entraînement des modèles de simulation ne soit plus perçu comme une violation du principe de limitation des finalités posé par le règlement général sur la protection des données (RGPD), mais comme un prolongement légitime et sécurisé de leur exploitation initiale, à condition de respecter strictement les conditions prévues par le règlement, comme nous le verrons ci-après.

L'apport majeur de l'EHDS réside dans le passage d'une gestion contractuelle et individuelle des données à une gouvernance publique régulée. Si le consentement individuel demeure un principe directeur tant pour l'utilisation primaire que secondaire des données, le règlement laisse pour cette dernière une marge de manœuvre aux États membres qui peuvent, à certaines conditions permettre la réutilisation des données nonobstant le refus du patient. En s'appuyant sur une base légale harmonisée fondée sur l'intérêt public et la recherche scientifique, l'EHDS facilite l'accès aux données de santé électroniques, par la mise en place d'organismes responsables de l'accès aux données de santé, les ORAD, désignés par les États membres et chargés d'instruire les demandes de réutilisation dans le respect des garanties prévues par le règlement. Ce système centralisé autour des ORAD permettra de remplacer la fragmentation des accords locaux par une procédure qui offre aux innovateurs un cadre prévisible et unifié, condition indispensable au développement des projets technologiques à dimension européenne.

L'article 53 du règlement EHDS énumère les finalités légitimes de ce type d'accès aux données de santé. Celles-ci incluent notamment l'amélioration des soins, la surveillance de la sécurité des médicaments, l'élaboration de politiques sanitaires, les statistiques officielles ou encore l'intelligence artificielle de santé[5]. Un chercheur ou un industriel souhaitant réutiliser ces données ne pourra pas s'adresser directement à un hôpital ou à un fournisseur de données. Il devra présenter une demande complète aux ORAD, justifiant la finalité, la proportionnalité et les garanties mises en œuvre. À cet égard, l'article 68 du règlement prévoit des critères stricts : l'anonymisation des données est privilégiée, la pseudonymisation n'étant admise qu'à titre subsidiaire et dûment justifiée, auxquelles s'ajoutent des exigences de documentation transparente, de limitation d'accès et de sécurité renforcée. Cette « harmonisation » des procédures d'accès, toujours en cours de d'élaboration dans le cadre des travaux de l'action conjointe TehdAs, devrait garantir aux projets des jumeaux humains virtuels une alimentation en données continue et sécurisée.

Au-delà de l'accès aux données, le succès du VHT repose sur la capacité à croiser des données massives et hétérogènes. Dans cette optique, l'EEDS et le projet *European Digital Innovation Hub* (EDITH), dédié au développement de l'innovation numérique[61], forment un binôme indissociable. Tandis que l'EEDS impose une interopérabilité juridique indispensable à l'usage secondaire des données de santé, le projet EDITH en assure la traduction technique par une feuille de route stratégique visant à intégrer des informations hétérogènes. Ce projet structure un écosystème collaboratif via un répertoire fédéré sur le cloud, mutualisant modèles et algorithmes pour lever les barrières technologiques à l'échelle européenne. L'aboutissement de cette démarche est une plateforme de simulation conçue comme un guichet unique ou *one-stopshop*, permettant aux utilisateurs non seulement de valider des modèles d'organes spécifiques, mais aussi de les combiner pour aboutir à une vision holistique et intégrée du corps humain. En somme, si l'EEDS apparaît être un excellent levier

[61] Règlement (UE) 2025/327 du Parlement européen et du Conseil relatif à l'Espace européen des données de santé, *JOUE* n° L 2025/327 du 5/03/2025.

pour ouvrir l'accès aux données, il participe également à instaurer un cadre de confiance nécessaire pour que les VHT passent du stade de prototypes de recherche à celui d'outils cliniques quotidiennement exploitables.

Ainsi, en imposant que les données soient traitées au sein de l'UE, l'EHDS assure un cadre protecteur de l'intégrité des informations de santé face aux géants numériques de la *Big Tech.* En outre, à travers des prototypes appliqués à des domaines critiques tels que l'oncologie cérébrale, les maladies cardiovasculaires ou les soins intensifs, le projet EDITH se prépare à un déploiement clinique à grande échelle où l'interopérabilité imposée par l'EHDS devient la condition sine qua non de la libre circulation et de la reconnaissance mutuelle des jumeaux numériques au sein de l'Union européenne.

Toutefois, ce déploiement ne saurait occulter les défis de régulation que suscite l'intégration des VHT dans le parcours de soin. En ce qu'il constitue le prolongement numérique d'un patient réel, le jumeau humain virtuel fait émerger une notion d'intégrité numérique, qui exige de concilier la complétude des données, la condition de sa fiabilité avec les principes de minimisation et de finalité du RGPD, tout en préservant l'autonomie décisionnelle du patient face à la force prédictive de l'algorithme. Cela se traduit concrètement dans la relation de soin, désormais structurée autour d'un quatuor inédit entre patient, médecin, jumeau numérique et concepteur, appelant un passage du consentement figé vers un consentement dynamique et modulaire. Par ailleurs, la nature hybride de ces systèmes, qui sont à la fois logiciel dispositif médical au sens du Règlement (UE) 2017/745 et système à haut risque au sens de l'AI Act, impose un régime de responsabilité adapté, associant obligation de sécurité de résultat, traçabilité infalsifiable par *smart contracts* et socialisation des risques via des fonds d'indemnisation sectoriels et des polices d'assurance dédiées, afin que le jumeau humain virtuel demeure un outil d'aide à la décision et non un substitut à la responsabilité humaine[62].

Si l'encadrement juridique et éthique s'efforce aujourd'hui de protéger les droits des patients et de sécuriser cette innovation, un défi ultime demeure pourtant en dehors du champ strictement normatif : celui de son impact environnemental. En effet, l'initiative des VHT repose sur des infrastructures matérielles énergivores dont l'empreinte carbone interroge la finalité même du soin. Dès lors, quel sens aurait l'amélioration de la santé d'un patient si elle participe, par son coût écologique, à la dégradation de la santé mondiale

[62] https://www.village-justice.com/articles/les-jumeaux-numeriques-digital-twins-defis-juridiques-implications,49211.html.

Décrypter la stratégie européenne pour les données



L'essor de l'intelligence artificielle repose largement sur la disponibilité de jeux de données de qualité, tout en renouvelant les interrogations relatives à la protection des droits fondamentaux et à la maîtrise des flux informationnels. Présentée par la Commission européenne en novembre 2025, la stratégie pour l'Union des données vise à favoriser l'accès et le partage des données au sein de l'Union tout en renforçant la souveraineté numérique européenne.
Les contributions réunies dans cette rubrique éclairent plusieurs enjeux au cœur de cette ambition. Elles abordent tant la stratégie institutionnelle portée par l'Union européenne que les débats juridiques relatifs à l'anonymisation, aux données synthétiques et au risque de réidentification, qui conditionnent la confiance dans les mécanismes de partage et de réutilisation des données.

La stratégie pour une union des données : vers une mobilisation stratégique des données au service de l'intelligence artificielle dans l'Union européenne

par Salaheddine ZADINE

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Introduction

A l'heure où l'intelligence artificielle « *métamorphose* » les équilibres économiques, industriels et géopolitiques mondiaux, l'accès à « *de volumes massifs de données de grande qualité* » apparaît comme une condition essentielle pour la stimulation de l'innovation[63] au sein de l'Union européenne.

Par la communication de la Commission du 19 novembre 2025[64], cette dernière entend faire évoluer la Stratégie européenne pour les données de 2020[65], qui n'a posé que « *de simples bases* », aux fins de « *libérer le potentiel des données* » au sein « *d'un marché unique des données sûr et interopérable* »[66], permettant ainsi à l'Union de « *jouer un rôle de premier plan dans le développement et l'adoption de l'IA* »[67]. La Commission constate que, malgré l'existence d'un cadre juridique « *visant à instaurer la confiance, à promouvoir le partage des données et à clarifier les règles tout au long de la chaîne*

[63] Mise à point de modèles d'IA solides, optimisation des soins de santé ou du système énergétique et soutenir la primauté industrielle.
[64] *COM(2025)* 835 final précitée
[65] La Commission européenne a publié le 19 février 2020 une communication intitulée « Une stratégie européenne pour les données » (*COM(2020)* 66 final), qui fait partie d'un paquet plus vaste de documents stratégiques comprenant également une communication intitulée « Façonner l'avenir numérique de l'Europe » (COM (2020) 67 final) et un livre blanc intitulé « Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance » (*COM(2020)* 65 final).
[66] Voir en ce sens, Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (dit « *Data Act* »). Pour ce qui concerne l'investissement de l'UE dans des espaces européens communs de données, v. notamment Commission européenne, document de travail des services de la Commission sur les espaces européens communs des données, *SWD(2024)* 21 final, 24 janvier 2024. La Commission aurait investi, entre 2021 et 2024, un montant de 336 millions d'euros dans 14 espaces européens communs de données stratégiques.
[67] Voir en ce sens, Communication de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée « Plan d'action pour un continent de l'IA », *COM(2025)* 165 final ; et, Communication de la Commission européenne au Parlement européen et au Conseil portant sur la « Stratégie pour l'application de l'IA », *COM (2025)* 723 final, 8 octobre 2025.

de valeur de données »[68], l'Union demeure confrontée à une pénurie de données[69] mobilisables pour le développement de l'IA[70].

A cet égard, la Commission structure sa stratégie autour de trois piliers complémentaires : élargir l'accès à des données de qualité pour l'IA et l'innovation (**I**), rationaliser les règles applicables aux données (**II**) et renforcer la position de l'Union européenne dans les flux internationaux de données (**III**).

I. UN ACCÈS PLUS LARGE A DES DONNÉES DE QUALITÉ POUR L'IA ET L'INNOVATION

Le premier pilier de la stratégie repose sur l'idée que la compétitivité de l'Union européenne en matière d'IA dépend directement de l'accès à des données de grande qualité ainsi qu'à des infrastructures permettant leur partage sécurisé à grande échelle. A cette fin, la Commission européenne entend notamment renforcer les espaces européens communs de données (**i**), développer des « *laboratoires de données* » destinés à faciliter l'utilisation sécurisée des données pour l'IA (**ii**), soutenir les infrastructures européennes d'informatique en nuage et d'IA (**iii**), mobiliser des ressources stratégiques publiques, scientifiques et culturelles (**iv**), ainsi que des mesures horizontales relative aux données synthétiques, à la mise en commun des données et aux normes (**v**).

i. Le développement des espaces européens communs de données

Les espaces européens communs de données constituent l'un des principaux instruments de la stratégie pour une Union des données. Ils doivent permettre de passer d' « *initiatives fragmentées* » à un « *écosystème de donnée continu, interopérable*[71] *et durable* », qui reposerait sur des infrastructures en nuage et sur des règles communes de gouvernance définissant les conditions d'accès, d'utilisation et de partage des données[72].

Les espaces européens de données sont directement intégrés à la stratégie européenne pour l'application de l'IA[73], puisqu'ils doivent fournir les ressources

[68] Voir en ce sens, 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 (dit « *Data Governance Act* ») ; Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public ; et le Règlement sur les données 2023/2854 précité.

[69] Les données en question sont qualifiées par la Commission comme un « *atout stratégique* » précieux. Pourtant, beaucoup de données restent encore peu exploitées ou enfermées dans des silos, notamment à cause de règles complexes et fragmentées. Afin de simplifier ce cadre, la Commission propose, dans le cadre du « *train de mesures omnibus sur le numérique* », de fusionner plusieurs instruments juridiques afin de créer un cadre européen des données cohérent et prévisible. La stratégie prévoit également plusieurs mesures d'accompagnement – telles que des clauses contractuelles types, des standards applicables aux services clous et des services d'assistance – destinées notamment à aider les PME à respecter plus facilement leurs obligations et à favoriser le partage des données dans les relations B2B et B2G.

[70] L'ambition de cette stratégie apparaît notamment à travers certains projets européens déjà en cours, tels que l'espace européen des données d'imagerie sur le cancer, qui devrait regrouper plus de 60 millions d'images anonymisées et annotées d'ici à 2027, afin de soutenir le développement de systèmes d'IA dans le domaine médical.

[71] Afin de garantir l'interopérabilité entre les différents espaces européens de données, la stratégie prévoir le développement de la plateforme *Simpl*, présentée comme un intergiciel sécurisé et à code source ouvert destiné à faciliter la circulation des données. Simpl devrait fournir « *plusieurs composants compatibles, d'utilisation gratuite, conformes à une norme commune en matière de qualité et de partage des données* ».

[72] Ces espaces doivent être progressivement reliés aux infrastructures européennes d'IA grâce aux « *laboratoires de données* » et aux « *fabriques d'IA* » (voir *infra*). Ces derniers fourniront notamment des outils de mise en commun, de curation, de pseudonymisation et d'anonymisation afin de rendre les données directement utilisables pour l'entraînement des systèmes d'IA.

[73] *COM(2025)* 723 final, *op. cit.*

sectorielles[74] nécessaires au développement de modèles d'IA spécialisés et d'« *avant-garde* »[75].

Les futurs financements européens donneront ainsi la priorité aux secteurs d'intérêt public (notamment la santé, la mobilité, l'énergie, les administrations publiques et l'environnement). A titre d'exemple concret de cette approche, la communication évoque le développement de « *centres de dépistage fondés sur l'IA dans le domaine des soins de santé* », destinés à valider des outils de diagnostic grâce à l'exploitation des données issues de l'Espace européen des données de santé[76]. Cette initiative s'inscrit plus largement dans les actions menées au titre du plan européen pour vaincre le cancer[77] ainsi que du plan de l'Union européenne pour la santé cardiovasculaire[78].

A partir de 2026, le déploiement des espaces de données dans les secteurs prioritaires sera soutenu par des investissements européens d'environ 100 millions d'euros afin de permettre une utilisation « *fiable et à grande échelle* » des données pour les applications d'IA.

En ce qui concerne le domaine de la santé, l'EEDS occupe alors une place centrale dans ce dispositif puisqu'il doit constituer une « *passerelle essentielle* » entre les écosystèmes de données de santé et le développement de l'IA. A ce titre, la stratégie prévoit notamment le développement d'applications de diagnostic fondées sur l'IA et de médecine grâce à l'utilisation d'ensembles de données « *anonymisées et synthétiques dans des environnements de traitement fiables* ».

ii. « Les laboratoires de données »

Les laboratoires de données sont définis en tant qu'« *installations spécialisées* » permettant, de manière similaire à des conteneurs de données - tout en favorisant l'interopérabilité et la cohérence dans l'ensemble de l'écosystème d'IA de l'Union - de faciliter leur utilisation pour l'entraînement des systèmes d'IA. Pour arriver à ces fins, ces laboratoires doivent fournir des services pratiques, notamment, de mise en commun, de curation, d'étiquetage et de pseudonymisation des données[79].

Les laboratoires de données sont ainsi conçus comme des « *catalyseurs* » de l'expérimentation et du déploiement de l'IA à partir de données de grande qualité. Ces catalyseurs constituent ainsi une réponse à

[74] Pour un exemple concret de l'application concrète de cette approche : des centres de dépistage fondés sur l'IA dans le domaine des soins de santé, qui valident les outils de diagnostic en utilisant l'espace européen des données de santé, dans le cadre d'actions menées dans le cadre du plan européen pour vaincre le cancer, de la stratégie pour les sciences du vivant et du plan de l'UE pour la santé cardiovasculaire.

[75] La communication mentionne ainsi plusieurs initiatives fondées sur l'exploitation de données sectorielles mises à disposition par ces espaces européens communs, telles que « Foundational Models for Industry », « AI-powered Pharma Discovery » ou « Autonomous Drive Ambition Cities ».

[76] Voir en ce sens le Règlement (UE) 2025/32 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/2847(dit « Règlement EEDS »).

[77] Voir « Commission staff working document. Review of Europe's Beating Cancer Plan », SWD (2025) 39 final, Bruxelles, 4 février 2025.

[78] Voir Communication de la Commission européenne sur un plan de l'Union européenne pour la santé cardiovasculaire : plan pour un cœur en bonne santé, *COM(2025)* 1024 final, du 16 décembre 2025.

[79] D'autres services sont prévus tels que, bien évidemment, la facilitation de l'accès aux données ; des conseils d'orientations réglementaires et des formations ; la production de données synthétiques sans divulgation d'informations sensibles ou confidentielles ; ainsi que des outils techniques et infrastructures simples et fiables permettant le traitement su site des données sensibles. La stratégie vise ainsi à permettre, en particulier, aux start-ups et aux entreprises en expansion de partager et d'utiliser des données « *en toute sécurité* », de favoriser l'entraînement coopératif de modèles d'IA et de soutenir le développement de modèles sectoriels fondés sur différents mécanismes de gouvernance et de licences.

une « *défaillance majeure du marché* », tenant à la « *disponibilité limitée* » de données diverses ainsi qu'à la réticence des acteurs privés à partager leurs données pour l'entraînement des systèmes d'IA.

En ce sens, les laboratoires fonctionneront à partir de « *canaux d'accès* » et des « *cadres de gouvernance* » déjà existants, sans nécessiter d'une centralisation massive des données impliquant leur transfert[80].

La participation aux laboratoires doit demeurer volontaire et les détenteurs de données conserveront le contrôle des conditions (consentement explicite) d'utilisation de leurs données. La stratégie insiste également sur le recours à des techniques « *préservant la confidentialité* »[81] afin de garantir le respect du RGPD[82] et renforcer la confiance « *tout en augmentant l'utilisation des données pour l'IA* ».

Plus largement, les laboratoires de données s'inscrivent dans l'évolution des infrastructures européennes de calcul développées autour d'EuroHPC[83]. La stratégie prévoit désormais le déploiement de « *fabriques d'IA* », puis à terme de « *gigafabriques d'IA* », destinées à relier capacités de calcul, accès aux données et expérimentation en matière d'IA. Les premiers laboratoires de données doivent être opérationnels dans ce cadre afin de mettre les développeurs d'IA en relation avec les espaces européens communs de données[84].

iii. Acte législatif sur le développement de l'informatique en nuage et de l'IA

Le développement d'une véritable Union européenne des données suppose l'existence d'infrastructures souveraines de calcul, de centres de données et de services d'informatiques en nuage capables de soutenir le développement de l'IA à grande échelle.

Face à l'augmentation continue des volumes de données et à la dépendance de l'Union à l'égard structures situées hors de son territoire, la Commission européenne annonce la présentation, au premier trimestre 2026, d'un acte législatif sur le développement de l'informatique aux nuages et de l'IA destiné à soutenir l'ensemble de la chaîne de valeur européenne du cloud et de l'IA. Ce dernier devra favoriser le développement de capacités durables de centre de données afin de garantir « *la sécurité et la souveraineté des futurs services européens d'informatique en nuage et d'IA* ». La stratégie précise également que cette initiative couvrira l'ensemble des infrastructures nécessaires de développement de l'IA, « *des processeurs de pointe jusqu'au matériel, logiciel et technologie de refroidissement durable* ».

---

[80] Ainsi, les espaces européens communs de données demeurent les infrastructures de confiance au sein desquelles les données sont gouvernées et mises à disposition, tandis que les laboratoires de données en assurent l'exploitation opérationnelle pour le développement de l'IA « *en toute sécurité et en apportant une valeur ajoutée* ».

[81] Telles que l'apprentissage fédéré, le chiffrement homomorphe et le calcul multipartite sécurisé. De plus, les données pourront être traitées localement ou à travers différents nœuds sans être fusionnées dans un répertoire unique, ce qui permet aux détenteurs initiaux de conserver le contrôle sur leurs données.

[82] 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 n° 95/46/CE (règlement général sur la protection des données).

[83] Entreprise commune pour le calcul à haute performance européen (EuroHPC), créée en 2020 à Luxembourg (Luxembourg). Son rôle est celui de développer un écosystème de supercalcul de classe mondiale en mettant en commun les ressources de l'Union européenne, des pays européens et de partenaires privés destiné à la recherche scientifique.

[84] Les laboratoires doivent également travailler en coordination avec les pôles européens d'innovation numérique (EDIH) qui font office de points de contact orientés vers les utilisateurs et aident à mettre les besoins en données en correspondance avec des applications concrètes.

iv. Ressources en données stratégiques : secteur public et données scientifiques

La stratégie fait de l'accès à des données « *de qualité, structurées et fiables* » une condition essentielle du développement de l'IA et de la souveraineté numériques européenne. A cette fin, la Commission entend renforcer l'exploitation des ensembles de données du secteur public, notamment les « *ensembles de données de forte valeur* » prévus par la Directive sur les données ouvertes[85], qui doivent être accessibles gratuitement, dans des formats lisibles par machine et via des d'interfaces de programmation d'applications (API)[86].

La Commission insiste également sur le potentiel stratégique des données scientifiques, illustré par l'exemple d'AlphaFold, dont les capacités de prédiction des structures protéiques ont profondément accéléré « *l'innovation* ». Des bases de données scientifiques bien structurées sont ainsi présentées comme des leviers permettant de réduire les « *coûts de recherche et développement et d'accélerer l'innovation dans des domaines tels que les produits pharmaceutiques, l'énergie, les matériaux ou les biotechnologies* ».

La stratégie prévoit dès lors le développement de nouvelles infrastructures numériques de recherche ainsi que le renforcement du « *nuage européen pour la science ouverte* » (EOSC), présenté comme un espace européen de partage et de réutilisation de données de recherche « FAIR »[87].

Ces ressources doivent soutenir les activités scientifiques fondées sur l'IA dans le cadre de RAISE[88]. En parallèle, le futur acte législatif sur l'Espace européen de la recherche « EER »[89] doit renforcer les conditions juridiques de partage, d'accès et de réutilisation des résultats, publications et données issues de la recherche financée par des fonds publics.

v. Mesures horizontales : données synthétiques, mise en commun des données et normes

La stratégie prévoit également plusieurs mesures transversales destinées à soutenir l'économie européenne des données. Premièrement, la Commission identifie notamment les données synthétiques comme un levier essentiel pour entraîner des systèmes d'IA dans des domaines où les « *données sont rares ou sensibles* », notamment en santé. Il s'agira alors de créer une « *usine de données synthétiques* » et d'élaborer des orientations et de normes relatives à leur utilisation fiable[90].

Deuxièmement, la stratégie entend sécuriser juridiquement la mise en commun des données, notamment dans des secteurs tels que la santé, où les entreprises ne disposent pas individuellement de volumes suffisants pour entraîner des modèles d'IA[91].

Enfin, la stratégie insiste sur la nécessité de renforcer la qualité et la standardisation des données afin d'éviter une fragmentation des pratiques de partage et de réutilisation

[85] Directive n° 2019/1024 précitée.
[86] La liste de ces données devrait être étendue dès 2026 aux données juridiques, judiciaires et administratives.
[87] De haute qualité, faciles à trouver, accessibles, interopérables et réutilisables.
[88] Communication de la Commission européenne au Parlement européen et au Conseil portant sur Une stratégie européenne pour l'intelligence artificielle dans le domaine de la science: poser les jalons du centre de ressources de la science pour et par l'IA en Europe (RAISE) *COM(2025)*724 final, du 8 octobre 2025.
[89] Proposition de Recommandation du Conseil sur le programme stratégique 2025-2027 de l'Espace européen de la recherche, Bruxelles, 28 février 2025, COM (2025) 62 final.
[90] Horizon Europe doit également financer des travaux de recherche sur les techniques de production de données synthétiques.
[91] Des lignes directrices sur les futures orientations sur les bonnes pratiques d'échange et de mutualisation des données par la Commission sont attendues afin de réduire l'insécurité juridique liée notamment au droit de la concurrence de l'Union.

efficace. La Commission prévoit, à ce titre, une future « *norme européenne relative à la qualité des données* »[92].

II. RATIONALISER LES REGLES EN MATIERE DE DONNEES

Le deuxième pilier de la stratégie vise à simplifier le cadre européen des données afin de « *moderniser et consolider l'acquis horizontal de l'UE en matière de données* ». La Commission européenne annonce notamment « *un train de mesures omnibus sur le numérique* »[93] destiné à *supprimer les règles obsolètes*, à *rationaliser les règles en matière de partage de données*[94], à *consolider le partage des données du secteur public* ainsi qu'à *moderniser les règles applicables aux cookies* et à la *protection des données*.

La stratégie prévoit également des adaptations ciblées du RGPD afin de clarifier certaines notions essentielles pour le développement de l'IA[95], ainsi que plusieurs ajustements du Règlement sur les données permettant « *d'éviter les « fuites » de données vers des pays tiers, d'introduire des régimes adaptés pour les services en nuage sur mesure et de supprimer les dispositions relatives aux contrats intelligents* », afin de *réduire les contraintes pesant sur les entreprises en expansion*[96].

FOCUS — LE « DIGITAL OMNIBUS »

Présentée par la Commission européenne le 19 novembre 2025, la proposition de règlement « Digital Omnibus » s'inscrit dans la stratégie pour l'Union des données. Elle vise à simplifier et rationaliser plusieurs textes européens relatifs au numérique, notamment en matière de partage des données, de protection des données personnelles et d'intelligence artificielle. Son objectif est de réduire les charges administratives tout en favorisant l'innovation et la compétitivité européennes.

III. PRESERVER LA SOUVERAINETE DE L'EUROPE EN MATIERE DE DONNEES GRACE A UNE APPROCHE STRATEGIQUE DE LA POLITIQUE INTERNATIONALE EN MATIERE DE DONNEES

Le troisième pilier de la stratégie repose sur l'idée que la souveraineté européenne en matière de données suppose non plus seulement la protection des données sensibles de l'Union, mais également la capacité de l'Union européenne à contrôler les conditions dans lesquelles les données circulent au niveau international.

La communication critique explicitement la situation actuelle dans laquelle des acteurs étrangers bénéficient d'un accès abusif au marché européen des

[92] Couvrant notamment les aspects d'exhaustivité, de cohérence, de clarté sémantique et de gouvernance, ainsi que des travaux de normalisation relatifs à l'annotation, à l'étiquetage et à la capture des données utilisées pour le développement des systèmes d'IA.

[93] Proposition de Règlement du Parlement et du Conseil modifiant les règlements n°s 2016/679/UE, 2018/1724/UE, 2018/1725/UE et 2023/2854/UE ainsi que les directives n°s 2002/58/CE, 2022/2555/UE et 2022/2557/UE en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements 2018/1807/UE, 2019/1150/UE et 2022/868/UE ainsi que la directive 2019/1024/UE (règlement omnibus numérique), *COM(2025)* 837 final, du19 novembre 2025.

[94] La Commission annonce vouloir identifier les chevauchements et interactions peu claires entre les différents régimes relatifs aux données pour *aider les entreprises à se conformer au Règlement sur les données*.

[95] Il s'agira, pour l'essentiel, de la notion de données à caractère personnel, les conditions d'anonymisation et de pseudonymisation, l'intérêt légitime comme base juridique de l'entraînement des systèmes d'IA ou encore les règles relatives à la prise de décision automatisée. La Commission entend réduire l'insécurité juridique encadrant la réutilisation des données tout en maintenant les garanties de respect de la vie privée.

[96] Le concept de « conformité en un clic » permettra ainsi d'automatiser certaines obligations réglementaires grâce à des certificats numériques de conformité et au futur « portefeuille européen d'identité numérique pour les entreprises ».

données tandis que les entreprises européennes demeurent confrontées à des exigences de localisation, à des restrictions d'accès ou à des règles discriminatoires dans certains Etats tiers. A cet égard, « *[l]a Commission agira donc de manière plus ferme pour défendre les intérêts et l'autonomie réglementaire de l'UE, en adoptant des mesures proportionnées lorsque la politique d'ouverture donne lieu à des abus ou lorsque les vulnérabilités sont instrumentalisées* ».

La stratégie identifie également plusieurs risques liés aux cyberattaques, aux fuites de technologie[97], à la surveillance et les dépendances coercitives pour la souveraineté européenne des données critiques[98].

Dans cette logique, la Commission annonce vouloir faire des « *conditions équitables pour l'accès aux données et les transferts transfrontières* » un « *pilier du commerce numérique* ». Elle prévoit également l'adoption de mesures destinées à renforcer la protection des « *données sensibles à caractère non personnel* » de l'Union, en complément des garanties offertes par le RGPD[99].

En parallèle, la Commission relève la nécessité de renforcer les liens entre les écosystèmes européens de données et ceux des « *partenaires partageant les mêmes valeurs* »[100]. Elle prévoit notamment de développer « *des services et des infrastructures de soutien tels que les espaces européens communs des données* », afin d'assurer un partage transfrontière ininterrompu [des données] ; de fournir « *des clauses contractuelles* standard », pour sécuriser les échanges internationaux de données ; et « *d'intégrer les engagements en matière de partage transfrontière des données dans des accords commerciaux internationaux* »[101].

Enfin, la communication affirme la volonté de l'Union de renforcer son influence dans la gouvernance mondiale des données en promouvant ses standards au sein du G7, du G20, de l'OCDE et des Nations Unies, tout en développant des coopérations spécifiques avec les pays candidats et partenaires proches de l'Union autour de plateformes partagée de données publiques et d'accords de confiance relatifs aux flux de données sensibles.

Conclusion

Pour conclure, la stratégie du 19 novembre 2025 pour une *Union des données* marque une nouvelle étape de la politique numérique européenne. Au-delà

[97] Au premier trimestre 2026, sera prévue la publication de lignes directrices destinées à évaluer le traitement réservé aux données européennes dans les Etats tiers ainsi qu'une « boîte outils de lutte contre la fuite de données ». Cette dernière fait l'objet d'une action phare de la stratégie (Création d'une boîte à outils pour lutter contre la localisation injustifiée, l'exclusion, la faiblesse des garanties et les fuites de données (T2 2026).

[98] A cet égard, la Commission envisage de mobiliser plusieurs instruments européens déjà existants, notamment le Règlement (UE) 654/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant l'exercice des droits de l'Union pour l'application et le respect des règles du commerce international, le Règlement (UE) 2023/2675 du Parlement européen et du Conseil du 22 novembre 2023 relatif à la protection de l'Union et de ses États membres contre la coercition économique exercée par des pays tiers (Instrument anticoercition).

[99] Ce qui fait de l'adoption de mesures visant à protéger les données sensibles à caractère non personnel (T3 2026), une action phare de la stratégie.

[100] D'ici 2026, conformément à la stratégie numérique internationale (Communication conjointe de la Commission européenne et du Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil sur « Une stratégie numérique internationale pour l'Union européenne », *JOIN(2025)* 140 final, du 5 juin 2025), la Commission et le Service européen pour l'action extérieure entendent renforcer les partenariats numériques de l'Union avec des Etats partageant les mêmes objectifs, notamment à travers le développement des accords sur le commerce numérique et l'intégration de chapitres numériques dans les accords commerciaux internationaux.

[101] L'objectif étant celui de promouvoir le cadre européen de données fiables dans les « *dialogues internationaux et dans le réseau de partenariat numérique* ».

de la seule régulation des données, la Commission cherche désormais à construire une véritable infrastructure européenne de l'IA fondée sur la circulation, l'(la) (ré)utilisation et la sécurisation des données de grande qualité et à grande échelle.

Un constat peut être fait, les données ne sont plus seulement envisagées comme des objets de protection juridique, mais comme des ressources stratégiques conditionnant la souveraineté numérique, la compétitivité industrielle et la capacité d'innovation de l'Union.

Communication de la Commission européenne du 19 novembre 2025 sur la « Stratégie pour une union des données – Faciliter l'accès aux données pour l'intelligence artificielle », *COM(2025) 835 final*.

La crise identitaire des données synthétiques en Europe face au diagnostic jurisprudentiel de la CJUE sur la définition de l'anonymisation

Compte rendu de la présentation à l'occasion de la rencontre Québec/Toulouse sur l'Espace Européen des Données de Santé

par Winnie DONGBOU WAMBA

Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

La journée – ou soirée selon le fuseau horaire concerné – du 29 avril fut marquée par une rencontre entre l'Université Toulouse Capitole et l'Université de Laval autour des enjeux de l'Espace Européen des Données de Santé[102]. A cette occasion, nous avions le plaisir de discuter de la qualification juridique des données synthétiques en matière de protection des données personnelles en Europe. Une question qui, à première vue technique, revêt des implications légales fondamentales pour les acteurs de la recherche en santé, notamment dans le cadre du déploiement de l'Espace Européen des Données de Santé (EEDS)[103].

I. DÉFINITION ET UTILITÉ SCIENTIFIQUES DES DONNÉES SYNTHÉTIQUES

Les données synthétiques peuvent être définies comme des données de patients générées soit par calcul, algorithmes et processus automatisés, soit par agrégation de données de patients collectées antérieurement, soit par une combinaison des deux approches[104]. Elles sont ainsi le produit d'un traitement algorithmique qui vise à reproduire les caractéristiques statistiques de données réelles sans en être une copie directe.

L'état de l'art en recherche clinique identifie plusieurs cas d'usage majeurs pour les données synthétiques dont la facilitation du partage de données entre acteurs internationaux, notamment pour les transferts de données de l'Europe vers les États-Unis ; l'augmentation des données pour la recherche sur les maladies rares, où les données de vie réelle sont insuffisantes ; l'entraînement de modèles d'apprentissage automatique en santé et la simulation de cohortes de patients afin d'explorer différentes hypothèses avant toute mise en application sur des patients réels. Tous ces usages convergent vers une interaction importante entre les patients, ou plutôt leurs données de santé et des modèles d'IA. Une interaction que les données synthétiques elles-mêmes promettent de limiter si elles peuvent être qualifiées de données anonymes.

II. LA CRISE IDENTITAIRE DES DONNÉES SYNTHÉTIQUES : DEUX THÈSES EN TENSION

Le cœur de la problématique réside dans la qualification juridique des données synthétiques au regard du droit européen de la protection des données (RGPD). Deux thèses structurent le débat. Il s'agit de la

[102] Un enregistrement de la rencontre sera d'ailleurs disponible sur la chaîne Youtube de la chaire DOSA https://www.youtube.com/@ChaireDOSA

[103] DDONGBOU WAMBA W., « Tentative d'une qualification juridique de la donnée synthétique au regard du règlement sur l'espace européen des données de santé », Le droit en mouvement : les évolutions du droit d'hier à aujourd'hui, Colloque jeunes chercheuses et chercheurs de la Faculté de droit de l'Université de Sherbrooke, 2025.

[104] Voy. le glossaire SILICA disponible ici : https://silica-asso.fr/glossaire-silica/ et FRAYSSE J.-L. et ALLASSONNIERE S., *Données de santé artificielles: analyse et pistes de réflexion* [en ligne], [s. n.], 2024, [consulté le 27 février 2025].

thèse de la dépersonnalisation complète[105] réfutée par la doctrine au profit de la thèse de la personnalité résiduelle[106].

Selon la thèse de la dépersonnalisation complète, les données synthétiques, étant par nature artificielles et non directement issues d'individus identifiables, seraient par définition des données à caractère non personnel. Elles échapperaient ainsi au champ d'application du RGPD et pourraient circuler librement, sans les contraintes réglementaires applicables aux données de santé. La thèse de la personnalité résiduelle, aujourd'hui dominante, reconnaît que les données synthétiques peuvent conserver un risque résiduel de réidentification. Deux arguments viennent étayer cette position :

- l'impossibilité d'atteindre un risque zéro de réidentification en raison de certains attributs présents dans les données synthétiques (notamment lorsqu'elles sont générées à partir de données réelles) ;
- la vulnérabilité des modèles génératifs face à des attaques spécifiques permettant de reconstituer des informations sur les individus ayant servi à l'entraînement du modèle.

Si un risque résiduel de réidentification subsiste, se pose alors la question de l'articulation entre anonymisation relative et anonymisation absolue : l'anonymisation parfaite est-elle un standard atteignable, ou le droit doit-il s'accommoder d'une approche probabiliste et contextuelle ? Comme nous le verrons ci-dessous, une conclusion déjà implicite dans le Règlement sur l'EEDS a été confirmée par la Cour de justice de l'UE (CJUE)[107].

III. DONNÉES SYNTHÉTIQUES ET EEDS : UNE QUALIFICATION INDIRECTE ET PRUDENTE

Le Règlement relatif à l'Espace Européen des Données de Santé ne mentionne pas explicitement les données synthétiques. On y trouve en revanche une première reconnaissance fonctionnelle dans les projets de lignes directrices de l'action TEHDAS2 :

- comme alternative pour la description des jeux de données sensibles disponibles (draft guidance M5.1)[108] ;
- comme alternative pour l'extraction autorisée des résultats de recherche depuis les environnements sécurisés

[105] NIŠEVIĆ M., MILOJEVIC D. et SPAJIĆ D., « Synthetic data in medicine: Legal and ethical considerations for patient profiling », *Computational and Structural Biotechnology Journal*, 28, 2025 ; VALLEVIK V., BEFRING A., ELVATUN S. *et al.*, « Processing of synthetic data in AI development for healthcare and the definition of personal data in EU law » [en ligne], *ArXiv*, abs/2508.08353, 2025.

[106] BEDUSCHI A., « Synthetic data protection: Towards a paradigm change in data regulation? » [en ligne], *Big Data & Society*, 11, 2024 ; NIŠEVIĆ M., MILOJEVIC D. et SPAJIĆ D., *op. cit.* ; PALACIOS M., BOUDEWIJN A., SACCANI S. *et al.*, « Empirical Evaluation of Structured Synthetic Data Privacy Metrics: Novel experimental framework » [en ligne], *ArXiv*, abs/2512.16284, 2025 ; GANEV G. et DE CRISTOFARO E., « Rethinking Anonymity Claims in Synthetic Data Generation: A Model-Centric Privacy Attack Perspective », *ArXiv*, abs/2601.22434, 2026.

[107] Analyses des décisions Patrick Breyer contre Bundesrepublik Deutschland, C-582/14, 2016, ECLI:EU:C:2016:779. ; IAB Europe v. Gegevensbeschermingsautoriteit, C-604/22, 2022, ECLI:EU:C:2024:214. Et Contrôleur Européen de la Protection des Données (CEPD) contre Conseil de Résolution Unique (CRU), C-413/23 P, 2025, ECLI:EU:C:2025:645. Bien que cette dernière décision concerne principalement la question de savoir si des données pseudonymisées seraient anonymes dans le chef du destinataire desdites données, la Cour cite les décisions précédentes en rappelant que « la perspective pertinente pour apprécier le caractère identifiable de la personne concernée dépend essentiellement des circonstances caractérisant le traitement des données dans chaque cas particulier » : Voir le résumé de l'affaire.

[108] Draft guideline for data holders on data description.

de traitement des données (draft guidance M7.2)[109].

Au sujet de l'anonymisation, L'EEDS semble se ranger du côté de l'approche relative et contextuelle. A juste titre, le considérant 92 du Règlement reconnaît explicitement que certaines catégories de données de santé restent particulièrement sensibles même après anonymisation, et qu'un risque résiduel de réidentification ne peut pas toujours être raisonnablement atténué. La question non résolue sur l'atténuation raisonnable du risque résiduel de réidentification est renvoyée au RGPD qui a fait l'objet d'une interprétation intéressante sur la question par la CJUE.

IV. LE DIAGNOSTIC DE LA CJUE : UNE JURISPRUDENCE CONSTANTE SUR L'ANONYMISATION CONTEXTUELLE

La jurisprudence de la Cour de justice de l'Union européenne offre un cadre interprétatif essentiel pour trancher la question de la qualification de l'anonymité des données et partant, celle des données synthétiques. À travers plusieurs décisions de référence[110] la Cour décide que l'anonymisation ne peut être considérée comme une qualité intrinsèque d'une information, mais comme le résultat d'une évaluation contextuelle de l'identifiabilité, variable selon les acteurs, les moyens de réidentification et le moment du traitement.

La transposition de cette position jurisprudentielle aux données synthétiques conduit à quatre implications concrètes :

- L'analyse doit tenir compte des catégories de données utilisées pour la génération des données synthétiques – certaines données sources étant plus sensibles et plus propices à la réidentification.
- L'évaluation de l'anonymité s'apprécie dans le chef du destinataire des données : c'est sa capacité concrète à réidentifier qui est déterminante, et non une propriété abstraite des données.
- La question des moyens raisonnables et légaux à disposition du destinataire pour procéder à une réidentification est centrale dans l'évaluation.
- L'évaluation doit être périodique : l'évolution de l'état de l'art technologique (modèles d'attaque, puissance de calcul, bases de données tierces disponibles) peut augmenter le risque de réidentification dans le temps.

CONCLUSION : AU-DELÀ DE LA CATÉGORISATION, LA DÉMONSTRATION DU RISQUE

Le rattachement des données synthétiques à une catégorie préexistante de données – personnelles ou non personnelles – importe finalement moins que la capacité à démontrer que le risque de réidentification est suffisamment réduit pour justifier l'application d'un régime allégé de protection des données.

Cette approche fonctionnelle, cohérente avec la jurisprudence de la CJUE, invite les Organismes Responsables de l'Accès aux Données, les détenteurs et les utilisateurs des données dans le cadre de l'EEDS à ne pas chercher à trancher définitivement la question de la nature des données synthétiques, mais plutôt à mettre en place des mécanismes robustes d'évaluation et de documentation du risque résiduel de réidentification, au regard du contexte précis de chaque traitement et de chaque destinataire.

[109] Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data, consulté le 17/05/2026.

[110] Voy. *supra*, note de bas de page 6.

En somme, la « crise identitaire » des données synthétiques ne se résoudra pas par une définition législative figée, mais par une méthodologie juridique et technique de l'évaluation continue du risque, dans l'esprit même de l'approche contextuelle consacrée par la Cour de justice.

Second Joint Action Towards the European Health Data Space – TEHDaS 2

23.06.2025

Workshop on the ethical dimensions of the European Health Data Space

par Lisa FÉRIOL

Doctorante CIFRE, Ekitia et Équipe BIOETHICS,
CERPOP UMR1295 Inserm et Université Toulouse Capitole

Introduction

L'action conjointe TEHDaS 2 (*Toward European Health Data Space*) [111] a organisé en ligne le 23 juin 2025 un atelier pour réfléchir collectivement à ce que devrait, de manière concrète, recouvrir les obligations en matière d'éthique introduites lors des discussions sur le texte du Règlement sur l'Espace européen des données de santé (Reg. EEDS)[112]. L'atelier a réuni 174 participants. Quatre experts[113] ont été invités afin de discuter ces enjeux autour d'une table ronde. Trois sessions en petits groupes se sont également tenues. Ce commentaire visera à résumer les principaux apports de cet atelier dont le contenu a été colligé au sein d'un document par TEHDaS2[114].

Rappelons pour commencer que l'article 67 du Reg. EEDS sur les *Demandes d'accès aux données de santé* en son paragraphe 2 point j) impose que les demandes d'accès aux données comportent des éléments éthiques précis concernant l'utilisation secondaire des données de santé lorsque ces derniers sont requis « au titre du droit national ». Ces dispositions permettent de valoriser le processus d'évaluation éthique de manière structurée et transparente dans ce nouveau système visant à faciliter l'utilisation secondaire des données de santé. Elles permettent également de réfléchir aux coopérations à mettre en œuvre au niveau européen sur ces procédures qui restent de la compétence nationale.

Les questions soulevées au cours de l'atelier portaient principalement sur l'interprétation et l'application des exigences prévues par le règlement par les parties prenantes concernées (comme les futurs organismes d'accès aux données de santé, les comités d'éthique existants, les chercheurs, les patients, les citoyens et professionnels). L'adéquation des

[111] L'action commune TEHDaS2 (deuxième phase de l'action conjointe TEHDaS qui a débutée en mai 2024) vise à soutenir la mise en œuvre de l'EEDS en promouvant des pratiques harmonisées pour l'utilisation secondaire des données de santé grâce à l'élaboration de lignes directrices et des spécifications techniques destinées aux détenteurs de données de santé, aux utilisateurs et aux organismes chargés de l'accès aux données de santé. V. Site internet de TEHDaS : https://tehdas.eu/ [consulté le 10-04-26].

[112] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive (UE) 2011/24 et le règlement (UE) 2024/2847, *JOUE* n° L 2025/327.

[113] Rosa JUUTI DE FINDATA, Magdalena EITENBERGER de l'Université de Vienne, Mikkel LINDSKOV Sachs du National Center for Ethics au Danemark, et Ole JOHAN BAKKE, Président du Standing Committee of European Doctors ont chacun donné une présentation.

[114] Site internet de TEHDaS, Workshop report "Workshop on the ethical dimensions of the European Health Data Space", 19.09.2025 [consulté le 10-04-26].

procédures nationales existantes avec les requis du règlement par ailleurs été questionnée, soulevant la potentielle nécessité de réfléchir à de nouveaux outils, rôles et collaborations afin d'assurer la bonne mise en œuvre du règlement. Les participants ont discuté comment de larges principes comme l'intérêt public, le bénéfice pour la société et l'intérêt légitime pouvaient être traduits de manière opérationnelle et cohérente pour les Etats membres impliquant des contextes culturels différents.

L'objectif principal était de s'accorder sur une conception commune de la gouvernance éthique dans le cadre de l'EEDS. Pour ce faire, différentes thématiques se sont dégagées lors de ces discussions. Parmi elles nous pouvons mentionner la reconnaissance mutuelle des avis éthiques émis par les différents comités d'éthique, le rôle des organismes d'accès aux données de santé en matière de gouvernance éthique, et la nécessité de veiller à ce que l'éthique reste un processus vivant et participatif, et ne soit pas perçue dans la construction de l'Espace européen des données de santé comme une simple étape ponctuelle de mise en conformité.

Rappel du caractère national de l'évaluation éthique

Owe LANGFELDT, chargé de mission au sein de l'Unité Santé numérique de la Direction générale de la santé et de la sécurité alimentaire de la Commission européenne a, en début de workshop, contextualisé les défis que représente l'évaluation éthique au sein de l'EEDS. Son introduction a rappelé que, malgré le fait que le système de l'EEDS soulève des enjeux sociétaux et éthiques importants comprenant la préservation de l'autonomie des individus ou encore les finalités pour lesquelles les données peuvent être réutilisées, les évaluations éthiques restent une compétence nationale. Il n'existe pas de procédure d'évaluation éthique harmonisée au sein de l'UE. Ceci expliquant le fait que le règlement renvoie au droit national applicable en la matière au sein de l'article 67 du Reg. EEDS. Owe LANGFELDT a à ce sujet rappelé que le projet pilote de l'EEDS[115] s'est interrogé sur la faisabilité d'un modèle éthique commun, mais que les positions nationales divergentes n'ont pas permis sa réalisation.

Implications éthiques de l'EEDS

A la suite des quatre présentations données par les experts, un débat sur les implications éthiques de l'EEDS a permis de faire émerger 5 thèmes essentiels :

- **La nécessaire mise en place de pratiques cohérentes en matière d'autorisations d'accès aux données dans un paysage aujourd'hui encore très fragmenté.**

Les participants ont souligné le risque que certains Etats membres s'obstinent à appliquer leurs propres règles sans coopération au niveau européen pour arriver à une approche cohérente. L'approche commune à défendre a été discutée au regard de l'articulation avec les ambitions du marché européen. Les apports d'un point de vue sanitaires et sociétaux devant également être réellement pris en compte dans l'évaluation des demandes d'accès.

- **Les risques liés à la coopération en matière de données de santé, notamment au regard des préoccupations liées à la confidentialité conduisant certains secteurs médicaux à refuser de participer à de tels systèmes coopératifs.**

La confiance a été ici considérée comme essentielle pour améliorer la collaboration des acteurs. De

[115] D'octobre 2022 à décembre 2024, le projet pilote HealthData@EU a élaboré une version pilote de l'infrastructure d'utilisation secondaire des données de santé prévue par l'Espace européen des données de santé. Ce projet pilote a été piloté par la Plateforme des données de santé (ou Health Data Hub) et a réuni 12 pays européens. V. https://health-data-hub.fr/page/healthdataeu-pilot.

plus, le lien entre utilisation primaire et utilisation secondaire des données doit être davantage mis en évidence dans la construction de l'EEDS, ce dernier permettant une meilleure qualité des données et donc une meilleure utilisation secondaire. Des efforts restent également à faire en matière de sensibilisation du public afin de ne pas exacerber les inégalités liées à son accès.

- **Les défis techniques liés à la qualité des données, aux métadonnées et à l'accès transfrontalier.**

Il a été souligné ici que les métadonnées sont essentielles à l'utilisation secondaire des données de santé selon les principes FAIR (*Findable, Accessible, Interoperable, Reusable*)[116]. De plus, il a été convenu que toutes les demandes de données ou d'accès à des données, qu'elles soient nationales ou internationales doivent être traitées de manière égale selon les principes communs prévus par le Reg. EEDS. Ceci a été rappelé en réponse à l'inquiétude formulée de voir certaines régions de l'UE dotées de systèmes de gouvernance de l'utilisation secondaire des données de santé plus réticentes à partager les données de santé détenues demandées par certaines régions présentant des systèmes moins développés.

- **La définition de la structure et du rôle des Organismes d'accès aux données de santé (ORAD).**

Il a été défendu que les ORAD[117] s'insèrent dans le paysage existant en s'appuyant notamment sur les infrastructures existantes, tout en soulignant le défi de coordination des différents acteurs. Si le modèle décentralisé apparaît comme étant le plus adapté, certaines inquiétudes à sa mise en place ont été soulignées : cela ne doit pas conduire à un paysage illisible. Une approche stratégique et coordonnée au niveau européen de la mise en œuvre de l'EEDS en matière d'évaluation éthique est plébiscitée afin d'éviter une mise en œuvre fragmentée du règlement.

- **L'élargissement par le Reg. EEDS du champ des détenteurs de données, des catégories de données et des cas d'utilisation de ces dernières.**

Les cas d'utilisation des données de santé visés ici étaient notamment ceux de l'exploitation des données d'assurance ou l'entrainement des systèmes d'intelligence artificielle. Cet élargissement des cas d'usage des données impliquant une grande quantité de données mais aussi de multiples acteurs, a souligné le défi lié à la capacité des ORAD à avoir la ressource humaine adaptée pour traiter de questions éthiques complexes.

Conclusions et résultats

Le rapport résumant le workshop souligne dans ses conclusions qu'un alignement entre les Etats membres est nécessaire afin de garantir la fiabilité et le respect de l'éthique au sein de l'EEDS. Pour ce faire, quatre messages clés peuvent être retenus :

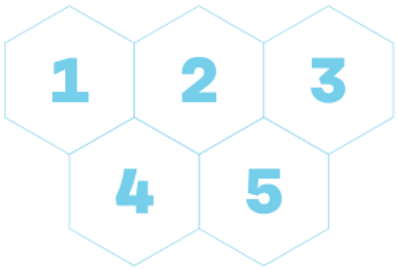
- Trouver un équilibre entre l'harmonisation et le respect des compétences nationales en parvenant à un alignement des pratiques entre les Etats membres.
- Faire de la solidarité en matière de données un principe clé en guidant les décisions relatives à la gouvernance des données de santé par la question fondamentale de la garantie du bénéfice sociétal et de réponse aux objectifs de santé publique.
- Assurer la confiance des personnes et des professionnels en garantissant la confidentialité et la sécurité des données de manière visible dans la mise en œuvre de l'EEDS.

[116] Décrits en 2016, les principes FAIR sont des principes favorisent l'accès et la réutilisation des données de la recherche.

[117] La structuration, les missions et les obligations des organismes responsables de l'accès aux données de santé sont décrites aux articles 55, 57 et 58 du Reg. EEDS.

- Renforcer les capacités et l'expertise des organes de gouvernance pour naviguer dans le paysage éthique et technique complexe que l'EEDS implique.

Le rapport mentionne enfin que les résultats de l'atelier seront analysés plus en détail dans le cadre de la tâche 4.2 du Work Package 4 de TEHDaS2 afin de servir de référence pour la planification de la mise en œuvre du Reg. EEDS.



27.05.2025

D7.1 Guideline on how to use data in a secure processing environment

par Franck AZNAR

Diplomé en biotechnologies, biologie moléculaire et cellulaire ; titulaire du DU EDiHL

La ligne directrice définitive 7.1[118] du groupe de travail TEHDAS 2[119], intitulée « comment utiliser les données dans un environnement de traitement sécurisé ? » publiée fin 2025 à l'occasion de la consultation publique vise à accompagner les utilisateurs de données de santé de la phase de planification préalable à leur demande d'accès aux données de santé jusqu'à la clôture du projet une fois leur analyse effectuée.

L'environnement de traitement sécurisé

Un environnement de traitement sécurisé (ci-après, ETS) est défini comme un espace de travail numérique hautement contrôlé, physique ou virtuel, garantissant un haut niveau de sécurité et de confidentialité, à travers lequel seuls les participants autorisés par l'organisme responsable de l'accès aux données (ci-après, ORAD) peuvent analyser des données de santé personnelles, et ce dans la limite des finalités définies dans l'autorisation de traitement qui leur est délivrée.

Ce nouveau mécanisme de traitement de données de santé de l'espace européen des données de santé (EEDS) coexiste avec les dispositifs traditionnels d'accès et de traitement de données pour la recherche et l'innovation, il ne les remplace pas (voir la ligne directrice D6.2 pour plus d'informations). À ce titre, la combinaison ou l'analyse conjointe de données obtenues via l'EEDS avec des informations issues d'un autre cadre n'est autorisée qu'à la condition d'être explicitement déclarée dans la demande d'accès aux données et validée par l'ORAD dans l'autorisation de traitement des données de santé, conformément à l'article 68§1, point b) du règlement sur l'EEDS.

Au plus tard le 26 mars 2027, les exigences techniques et organisationnelles, ainsi que les exigences en matière de sécurité de l'information, de confidentialité, de protection des données et d'interopérabilité applicables aux ETS seront adoptées par la Commission européenne à travers l'adoption d'actes d'exécution (voir Art.73§5 EEDS), définissant par

[118] Ligne directrice définitive 7.1, disponible ici.

[119] Instituée par la Commission européenne, « Toward European Health Data Space 2 » (TEHDAS 2) est la deuxième action conjointe ayant comme objectif de définir des lignes directrices relatives à la mise en œuvre du règlement « Espace européen des données de santé » (EEDS).

ailleurs les outils et fonctionnalités préinstallés pour les utilisateurs dans les différents ETS.

Préparer et anticiper son projet dans l'ETS

Préalablement aux spécifications actuellement non-adoptées, la ligne directrice 7.1 avance quelques conseils pratiques concernant les modalités et spécificités relatives à l'ETS à prendre en considération pour l'utilisateur de données de santé afin de mener à bien son traitement de données, lui permettant ainsi d'informer l'ORAD de ses besoins dès sa demande d'accès aux données de santé (p.15-16).

Dans la suite de cette ligne directrice sont détaillées les règles à respecter concernant le dialogue entre l'utilisateur des données et le fournisseur de l'ETS (p.17) et les mesures relatives à l'identification des individus autorisés au traitement lors de leur accès à l'ETS, suivant la politique du « Zero Trust » (p.18).

De plus le groupe de travail propose une description de l'infrastructure interne et des règles générales relatives à l'utilisation des ETS, avec notamment la possibilité pour les utilisateurs de données d'installer des logiciels spécifiques, en plus de ceux préinstallés, afin de mener à bien leur traitement. Il y est également fait mention des règles de responsabilités légales, comportementales et administratives qui incombent aux utilisateurs de l'ETS (p.18 à 20).

Le chapitre 11 du document quant à lui détermine les différents responsables du traitement des données, au sens de l'article 4§7 du règlement général sur la protection des données (RGPD), en fonction des activités réalisées lors des différents stades de l'accès et du traitement des données de santé dans le cadre de l'EEDS. Sont également précisées les responsabilités spécifiques qui leur incombent, et notamment celles qui pèsent sur les utilisateurs de données de santé en tant que responsables du traitement des données lorsqu'ils interviennent dans l'ETS, conformément à l'article 74§1 du règlement EEDS (p. 20 à 22).

Dans l'avant dernière partie du document sont mentionnées les actions interdites lors de l'utilisation d'un ETS et les conséquences qui en découlent, ainsi que l'obligation de notification des brèches de sécurité à l'autorité compétente, conformément au RGPD (p. 22-23).

Sont définies *in fine* les conditions relatives à l'exportation des résultats de l'ETS. Il est possible d'archiver les données dans un environnement de traitement avec des capacités limitées, notamment à des fins de reproductibilité et de vérification des résultats par les pairs. Il est rappelé qu'une autorisation de traitement de données, conformément à l'article 68 de l'EEDS, ne peut excéder 10 années consécutives, extensible une seule fois pour une période de 10 années supplémentaires. Une fois l'autorisation expirée, l'ORAD dispose alors de 6 mois pour supprimer l'intégralité des données de santé stockées sur l'ETS. Les résultats doivent être publiés dans les 18 mois suivant la fin du traitement (p.23).

05.09.2025

M7.2 Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data

par Franck AZNAR

Diplomé en biotechnologies, biologie moléculaire et cellulaire ; titulaire du DU EDiHL

Lors de cette même consultation publique, le groupe de travail 7.2[120] a publié sa ligne directrice préliminaire M7.2 concernant la minimisation des données, la pseudonymisation, l'anonymisation et les données synthétiques.

Minimisation des données

Dans la première partie du document (p. 8 à 24), le groupe de travail se penche sur la question de la minimisation des données, principe fondamental énoncé à l'article 5§1, c) du règlement général sur la protection des données (RGPD) comme suit « les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Le groupe de travail met ainsi en avant le respect de ce principe tout au long de l'intégralité du cycle de vie des données, définissant en ce sens plusieurs recommandations et bonnes pratiques à destination des différents acteurs impliqués. Parmi ces recommandations, on retiendra notamment la réduction du volume des différents jeux de données en fonction des finalités de traitement, et ce en limitant nécessairement la granularité et les variables disponibles, avec une attention particulière portée aux identifiants indirects (âge, nationalité, appartenance ethnique, lieu de travail, niveau de revenus, etc..).

Le document précise la recommandation sus-mentionnée par le biais de cinq dimensions : « Qui ? ; Quoi ? ; Quand ? ; Où ? ; Comment ? » (voir **schéma relatif à la minimisation des données – page suivante**), permettant d'apprécier le spectre des critères essentiels afin d'établir une minimisation efficiente des données (p.13 à 19).

La pseudonymisation comme pierre angulaire

Dans la seconde partie du document la pseudonymisation des données est abordée, telle que définie à l'article 4§5 du RGPD. La pseudonymisation est une transformation, dans laquelle les identifiants personnels directs sont remplacés par de nouveaux identifiants appelés pseudonymes. Elle permet une utilisation secondaire des données de santé électroniques dans un environnement de traitement sécurisé, sous condition prévue par l'article 68§1, c) du règlement relatif à l'Espace européen des données de santé (EEDS).

Le groupe de travail liste dans ce chapitre les avantages de la pseudonymisation par rapport à l'anonymisation, à savoir un degré de qualité et de fidélité des données plus élevé, la possibilité de lier différents jeux de données entre eux et l'aspect réversible de la pseudonymisation.

Concernant la possibilité de lier différents jeux de données appartenant à différents détenteurs de données, c'est par l'intermédiaire de l'organisme responsable de l'accès aux données (ORAD) ou d'un détenteur de données de confiance que sera délivrée, suite à une évaluation des risques, une autorisation de traitement de données permettant ou non la liaison des jeux de données, utilisant les identifiants directs en amont de la pseudonymisation (p.26) – (Pour davantage d'informations sur la liaison des différents jeux de données voir le document M7.5[121] du TEHDAS 2).

Les auteurs énoncent ensuite différents scénarios impliquant tous les acteurs

[120] Ligne directrice préliminaire 7.2, disponible ici.

[121] Ligne directrice préliminaire 7.5, disponible ici.

lors des différentes phases de l'utilisation secondaire des données de santé (voir schéma récapitulatif des cas d'usage généraux) et émettent des recommandations générales, notamment en termes de métadonnées (voir ligne directrice D5.1[122], de mesures techniques, organisationnelles et de gestion des risques associées à la pseudonymisation (p.28 à 33). Une pseudonymisation réversible est nécessaire dans le cas d'une constatation significative relative à la santé d'une personne physique (voir article 58§3 EEDS) ou pour l'application du droit d' « opt-out » (voir article 71 EEDS).

Aller plus loin dans la protection des données

Le groupe de travail a été amené à discuter en détail, dans ce dernier chapitre dédié à l'anonymisation et à la génération de données synthétiques, de différentes techniques qui permettent une protection complémentaire à la minimisation des données et aux données pseudonymisées. Il y est précisé que ces techniques d'anonymisation et de génération de données synthétiques seront souvent rendues nécessaires afin, entre autres, de garantir un niveau de protection des données élevé empêchant les risques de ré-identification notamment dans le cadre d'entraînement de modèles d'IA d'apprentissage automatique, ou lors de l'exportation de données des environnements de traitement sécurisés, ou encore afin de permettre aux demandeurs de données de santé de tester divers algorithmes informatiques, préalablement à la demande de traitement des données, sur des échantillons de jeux de données publiquement disponibles (voir ligne directrice D5.1 section 8.2.4).

Le document présente différents cas d'utilisation des données de santé et en ce sens différentes méthodologies et outils utiles au développement d'une architecture « la plus robuste qui soit » en matière d'anonymat, de génération de données synthétiques, et d'évaluation des risques associés (p.37 à 40).

Les règles générales relatives à l'établissement d'une documentation obligatoire lors de l'utilisation de techniques d'anonymisation des jeux de données et de génération de données synthétiques sont également définies (p.40-41).

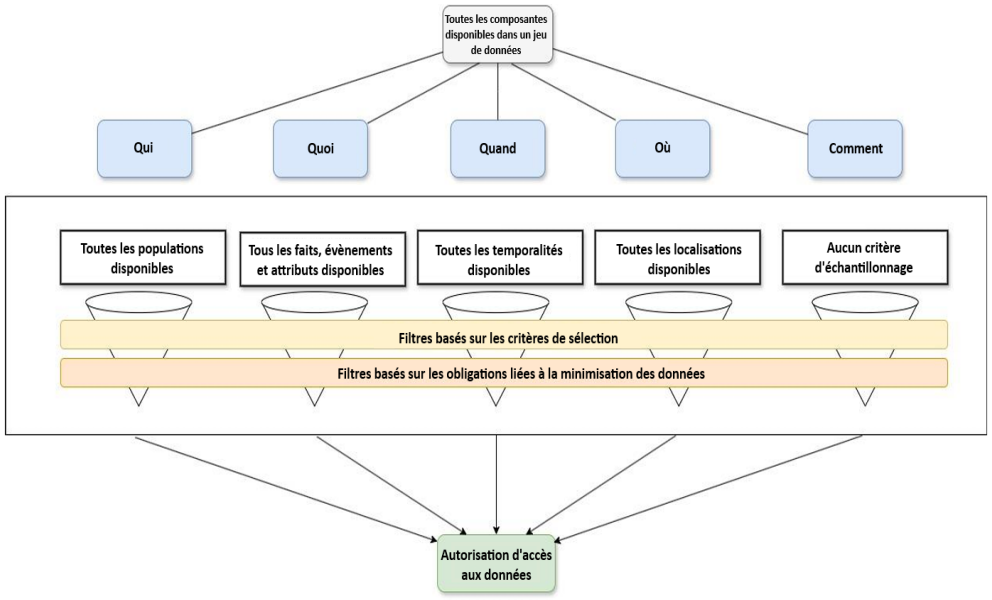


Schéma relatif à la minimisation des données définissant les différentes dimensions liées à la minimisation des données dans le cadre de l'EEDS

[122] Ligne directrice définitive 5.1, disponible ici.

Enfin, dans la dernière partie du document, sont présentées différentes techniques existantes d'anonymisation et de génération de données synthétiques (p.41-45), ainsi que différents outils supposés nécessaires afin d'aider les différents acteurs impliqués à vérifier, et évaluer automatiquement (ou semi-automatiquement) la viabilité des mesures de protection des données ayant été mises en œuvre sur un jeu de données (p.45 à 47).

Un arrêt attendu :

La Cour dans son arrêt *CEPD contre CRU*, C-413/23 P, du 4 septembre 2025[123] a été amenée à se prononcer sur plusieurs questions relatives aux données à caractère personnel. Après avoir réaffirmé, conformément à une jurisprudence constante, les critères caractérisant les données à caractère personnel, à savoir le fait que les données à caractère personnel se rapportent à une personne physique en raison de « leur contenu, de leur finalité ou de leur effet » *(voir arrêt Nowak, C-434/16[124])* et le fait qu'elles se rapportent à une personne physique « identifiée ou identifiable » *(voir arrêt Breyer, C-582/14[125]),* la Cour consacre le caractère relatif (ou contextuel) de l'effet de la pseudonymisation sur l'identifiabilité des données à caractère personnel.

On notera avec intérêt la formulation retenue selon laquelle « l'existence d'informations supplémentaires permettant d'identifier la personne concernée n'implique pas à elle seule, que des données pseudonymisées doivent être considérées comme constituant en toute hypothèse et pour toute personne, des données à caractère personnel ».

En conséquence, laissant ouverte la question du caractère contextuellement identifiable des données pseudonymisées, la Cour nous amène à nous attendre, vraisemblablement, à l'apparition future d'une vaste jurisprudence en la matière, évoluant et se précisant, au gré des nouvelles réglementations et des nouvelles technologies.

Il n'est pas interdit de penser, sous réserve d'une confirmation par la CJUE de cette interprétation, si elle en est saisie, que les utilisateurs de données de santé autorisés par l'ORAD, auraient la possibilité de télécharger, conformément à l'article 73§2 tiret 2 du règlement EEDS des données de santé électroniques pseudonymisées ne comportant aucun élément à caractère personnel au sens de l'interprétation retenue dans l'arrêt CRU. En attendant, la version définitive du projet de lignes directrices M7.2 apportera sans doute des éléments éclairants et déterminants. Une telle possibilité aurait été inenvisageable si la Cour s'était prononcée en faveur du caractère dit « absolu » de la pseudonymisation.

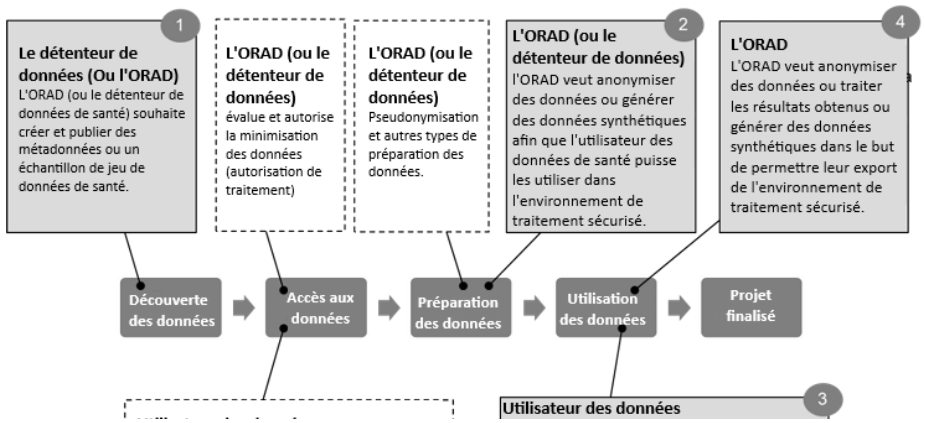


Schéma récapitulatif des cas d'usage généraux dans lesquels interviendraient minimisation, pseudonymisation, anonymisation des données et génération de données synthétiques en fonction des différentes phases de l'utilisation secondaire des données de santé et des différents acteurs impliqués

[123] Arrêt CRU contre CEPD, C-413/23 P, disponible ici.

[124] Arrêt Nowak, C-434/16, disponible ici.

[125] Arrêt Breyer, C-582/14, disponible ici.

Commentaire des propositions TEHDaS2 clarifiant les modalités d'examen des finalités de réutilisation, de notification des constatations significatives et portant sur les infrastructures techniques de traitement des données

par Winnie DONGBOU WAMBA

Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

16.09.2025
M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data

17.09.2025
M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025
M7.4 Draft technical, functional and security specifications of Secure Processing Environments

07.09.2025
M8.2 Draft Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data

Dans le cadre d'une consultation publique ouverte du 30 septembre au 30 novembre 2025, TEHDAS2[126] a soumis à contributions un ensemble de onze projets de lignes directrices[127], dont quatre retiennent particulièrement notre attention en raison de l'importance des dispositions du Règlement EEDS qu'ils proposent de concrétiser. Il s'agit du projet de ligne directrice M5.2 sur les catégories minimales et les limitations à la réutilisation des données de santé[128], la ligne directrice M8.2 sur l'obligation de notification aux personnes physiques des constatations importantes liées à leur santé, issues de l'utilisation secondaire[129], ainsi que les projets de spécifications techniques M7.3 et M7.4 portant respectivement sur l'infrastructure informatique commune[130] et sur les environnements de traitement sécurisés[131].

Ces projets de lignes directrices et de spécifications techniques abordent des questions essentielles à l'opérationnalisation effective de l'EEDS : la frontière entre finalités autorisées et usages prohibés, y compris l'harmonisation de l'évaluation des demandes d'accès (I), la primauté de l'intérêt

[126] L'action conjointe TEHDAS2 (Towards a European Health Data Space-2) a pour objectif d'accompagner la Commission Européenne dans la conception de lignes directrices visant à opérationnaliser l'utilisation secondaire des données de santé.
[127] Tous les 11 projets de lignes directrices sont disponibles ici https://tehdas.eu/public-consultations/#public-consultation.
[128] TEHDAS2, M5.2 Draft Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data, 16 September 2025.
[129] TEHDAS2, M8.2 Draft Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data, 7 September 2025.
[130] TEHDAS2, M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure, 17 September 2025.
[131] TEHDAS2, M7.4 Draft technical, functional and security specifications of Secure Processing Environments, 12 September 2025.

du participant à la recherche à travers la notification des constatations significatives (II), et à la configuration technique et organisationnelle de l'infrastructure indispensable aux échanges entre autorités compétentes (III), à l'accès, au partage et la sécurité des données de santé (IV).

I. LA BARRIERE POREUSE ENTRE FINALITES AUTORISEES ET USAGES PROHIBES

La ligne directrice M5.2 vise essentiellement à guider les Organismes d'accès aux données de santé (ORAD, en anglais *Health Data Access Bodies* – HDAB) dans l'interprétation des articles 53 et 54 du Règlement EEDS, qui définissent respectivement les finalités autorisées et les usages prohibés de l'utilisation secondaire des données de santé électroniques. Elle énumère six finalités licites au titre de l'article 53(1) dont les finalités d'intérêt public et de recherche scientifique, qui nous intéresseront particulièrement en raison de leur frontière floue avec certains usages prohibés.

A. Les clarifications conceptuelles attendues sur les finalités d'intérêt public et de recherche scientifique

Le projet de ligne directrice propose une lecture restrictive de l'intérêt public en soulignant que la finalité doit relever des domaines de la santé publique ou de la santé au travail tels que définis par le Règlement (UE) 1338/2008 et par les standards de l'Organisation mondiale de la santé[132]. Le document insiste sur le fait que l'intérêt public au sens de l'EEDS doit s'entendre comme un concept fonctionnel, étroitement lié à des compétences d'autorité publique[133]. Cette précision est utile, car elle évite l'instrumentalisation du concept par des acteurs qui invoqueraient un intérêt public diffus pour accéder à des données sensibles.

Concernant la clarification de la finalité de recherche scientifique, le projet de ligne directrice procède en deux temps. il observe d'abord que ce concept n'est pas entièrement défini dans les actes du droit dérivé de l'Union, et qu'il convient de la rapprocher de la définition extensive donnée au considérant 159 du RGPD, laquelle englobe le développement et la démonstration technologiques, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé[134]. Il introduit ensuite une distinction subtile entre « recherche scientifique » stricto sensu et « activités d'innovation »[135], reconnaissant que ces dernières couvrent un spectre allant de la recherche translationnelle à des activités de développement de produits. Les risques d'une lecture trop extensive de la « recherche scientifique », ne sont pas explicitement adressés, mais le projet de ligne directrice propose néanmoins des garde-fous opérationnels en exigeant des ORAD qu'ils vérifient la cohérence entre les qualifications du demandeur et l'objectif déclaré[136].

B. La difficile frontière des usages prohibés : marketing et produits préjudiciables

L'article 54 du Règlement EEDS prohibe cinq catégories d'usages : les décisions préjudiciables aux personnes (a), les décisions discriminatoires à l'égard de groupes (b), les activités de publicité et de marketing (c), le développement de produits ou services préjudiciables (d), et les activités contraires aux dispositions éthiques nationales (e). Le projet de ligne directrice M5.2 consacre des développements substantiels à ces interdictions, sans cependant parvenir à dissiper toutes les zones d'ombre[137].

Nous proposons de les résumer en trois principaux points : (1) l'asymétrie informationnelle. Un

[132] Projet M5.2, §. 6.1, p. 14.
[133] *Ibid.*, pp. 14-21.
[134] *Ibid.*, pp. 27-28.
[135] *Ibid.*, p. 29.
[136] *Ibid.*, §. 6.7.4, p. 30.
[137] Projet M5.2, §. 9.

demandeur disposant de véritables intentions discriminatoires ne les révélera jamais dans sa demande, rendant le contrôle *ex ante* par l'ORAD inefficace à prévenir les usages détournés les plus préjudiciables ; (2) la temporalité défavorable du contrôle : les violations seront découvertes seulement lors du monitoring *ex post*, lorsqu'un préjudice sera probablement déjà constaté ; (3) l'insuffisance de la solution offerte : les clauses d'engagement recommandées pour éviter les usages prohibés ne fonctionnent que sur base de la bonne foi des utilisateurs des données, mettant ainsi en évidence le décalage entre la promesse protectrice de l'EEDS et sa réalité opérationnelle.

C. Les pistes de réflexion additionnelles : l'aveu d'une « œuvre » inachevée

La ligne directrice M5.2 se distingue par la lucidité avec laquelle elle assume le caractère inachevé de son travail. Sa section 9, intitulée « *Areas of further exploration* », énumère sept chantiers ouverts qui mériteront un approfondissement via les résultats de la consultation publique. Sont ainsi identifiés : (1) l'alignement continu entre les ORAD quant à l'évaluation des demandes (§9.1), qui suppose la mise en place de mécanismes de coordination — comparables, en matière de protection des données, au rôle du Comité européen de la protection des données ; (2) la clarification de la frontière entre innovation et marketing (§9.2), dont la ligne directrice admet qu'elle constitue un point imprécis ; (3) l'interprétation de l'interdiction du développement des produits préjudiciables dans le contexte de la recherche médicale impliquant des substances contrôlées (§9.3), question particulièrement sensible pour la recherche sur les addictions et les psychédéliques thérapeutiques ; (4) la définition d'une procédure européenne standard pour l'évaluation des demandes par les ORAD (§9.4), ce qui revient à reconnaître l'insuffisance d'une harmonisation seulement par les principes ; (5) l'organisation d'un soutien éthique et juridique aux ORAD (§9.5), enjeu central pour assurer la capacité de ces organismes à évaluer les demandes d'accès ; (6) le traitement des décisions automatisées et de leurs effets potentiellement préjudiciables (§9.6) ; et (7) la construction d'un système de surveillance permettant d'identifier les usages détournés des données (§9.7).

II. L'INTÉRÊT SUPÉRIEUR DES PARTICIPANTS À LA RECHERCHE : LA NOTIFICATION DES CONSTATATIONS SIGNIFICATIVES

Le projet de ligne directrice M8.2 quant à lui couvre l'une des questions éthiques les plus délicates posées par la réutilisation secondaire des données de santé : que faire lorsque l'analyse de données conduit à la découverte d'une information médicale significative (ci-après « constatation(s) significative(s) ») pour la personne dont les données ont été utilisées ? Les articles 58(3) et 61(5) du Règlement EEDS imposent aux ORAD-une procédure spécifique en matière de constatations significatives, dont la ligne directrice M8.2 précise les contours opérationnels en distinguant préalablement les constatations incidentes de celles qui sont significatives. Les premières se définissent comme des informations révélées fortuitement au cours d'une recherche, en dehors du champ de la question scientifique initiale, et non intentionnellement recherchée par les investigateurs[138]. Les secondes sont des constatations qui présentent une pertinence médicale directe pour la santé de la personne dont les données ont été traitées[139]. Cette définition évite une notification de toute découverte incidente, lequel aboutirait à une surcharge informationnelle préjudiciable à la personne et matériellement insoutenable pour les détenteurs de

[138] Projet M8.2, §. 5.1.

[139] *Ibid.*

données. Il est bien évidemment entendu que la procédure de notification n'est applicable que lorsqu'il est possible d'identifier directement (via des identifiants personnels) ou indirectement (via une pseudonymisation avec accès à la clé de réidentification) la personne concernée[140].

Cette procédure de notification implique trois acteurs dont il convient de préciser les responsabilités. L'utilisateur de données signale la découverte significative à l'ORAD[141], qui la transmet au détenteur de données. C'est le détenteur qui assure, le cas échéant, la notification à la personne concernée ou au professionnel de santé qui la prend en charge[142]. L'ORAD n'est responsable ni de la validation clinique du résultat, ni de la notification directe à l'individu. Il ne joue qu'un rôle d'intermédiaire. La décision de notification est toutefois laissée à l'appréciation du détenteur des données en fonction de ce qui est autorisé ou requis par le droit national[143]. Le projet M8.2 révèle également une tension entre le droit de la personne à ne pas être informée[144] et l'obligation potentielle de notification des constatations découlant de la réutilisation de ses données. A ce sujet, elle laisse le soin aux États membres d'établir des procédures permettant d'assurer que le droit à ne pas être informé est appliqué lors du déclenchement de la procédure de notification[145].

III. LA CONFIGURATION TECHNIQUE ET ORGANISATIONNELLE DE L'INFRASTRUCTURE COMMUNE INDISPENSABLE AUX ÉCHANGES ENTRE AUTORITÉS COMPÉTENTES

Le projet de spécification technique M7.3 présente HealthData@EU, l'infrastructure transfrontalière instituée par l'article 75 du Règlement EEDS, en deux composantes essentielles. D'une part, la plateforme centrale HealthData@EU opérée par la Commission européenne[146] et d'autre part, les points de contact nationaux déployés par les États membres pour connecter leurs environnements nationaux à la plateforme centrale[147]. En effet, chaque État membre désigne un Point de Contact National (PCN) qui sert d'intermédiaire unique entre les systèmes nationaux et la plateforme centrale.

Aucune communication directe entre États membres n'est possible — tout transite obligatoirement par la plateforme centrale[148], ce qui garantit une traçabilité complète mais crée une dépendance technique envers la Commission. Chaque message échangé — qu'il s'agisse d'une demande d'accès aux données, d'une décision de permis ou d'une mise à jour du catalogue — suit un flux identique en douze étapes, au cours duquel il est successivement validé, chiffré, signé, transmis, déchiffré, authentifié et enregistré à des fins d'audit[149]. Deux couches distinctes assurent ce processus : une couche « métier » qui vérifie que le contenu du message est conforme aux exigences du Règlement EEDS, et une couche « transport » qui garantit la sécurité technique de la transmission[150]. À chaque étape, un accusé de réception signé est renvoyé à l'expéditeur, assurant qu'aucun message ne peut être perdu ou contesté.

Avant de se connecter à l'infrastructure, les États membres peuvent tester leurs systèmes via un outil de conformité mis à disposition par la Commission, dont l'usage est recommandé mais non obligatoire[151]. Ce cadre

[140] *Ibid.,* §. 5.3.
[141] *Ibid.,* §. 7.1, step 2.
[142] *Ibid.,* steps 3 and 4.
[143] *Ibid.,* §. 7.2, Figure 1.
[144] Considérant 67 et art. 58(3) du Règlement EEDS.
[145] Projet M8.2, p. 23.
[146] M7.3, §. 2.1.
[147] *Ibid.,* Annexe 2
[148] *Ibid.,* p. 14-15.
[149] *Ibid.,* §. 7.2.
[150] *Ibid,* §. 6.
[151] *Ibid.*, §. 8.

technique, aussi robuste soit-il, laisse entière une question juridique centrale que M7.3 ne tranche pas : en cas de défaillance dans la chaîne de transmission, la responsabilité reste indéterminée entre le point de contact national, la Commission et les ORAD destinataires des demandes d'accès.

IV. L'ARCHITECTURE DES ENVIRONNEMENTS DE TRAITEMENT SÉCURISÉS

Les environnements de traitement sécurisés (ETS) constituent, selon la spécification M7.4, une plateforme virtuelle conçue pour permettre une réutilisation sécurisée des données de santé tout en maintenant la conformité aux obligations de protection et de confidentialité des données[152]. Leur définition juridique est empruntée au Règlement (UE) 2022/868 sur la gouvernance des données, qui les décrit comme des environnements physiques ou virtuels permettant à leur opérateur de déterminer et superviser toutes les actions à effectuer sur les données, de leur accessibilité à leur exportation[153]. Dans le périmètre de l'EEDS, l'article 73 du Règlement (UE) 2025/327 en fixe les exigences de base, que M7.4 décline en dix-huit exigences numérotées (EHDSR-1 à EHDSR-18), articulées autour de trois impératifs : la sécurité des données, l'accès restreint aux seules personnes nominativement désignées dans le permis de données, et le contrôle des sorties garantissant que seuls des résultats agrégés et anonymisés peuvent quitter l'environnement[154].

Le cycle de vie de l'ETS passe par six étapes[155]. L'environnement est d'abord créé sur mesure une fois le permis délivré par l'ORAD, typiquement par le déploiement d'une machine virtuelle isolée. Les données sont ensuite transmises par le détenteur de données vers l'ETS, où l'ORAD procède à leur préparation technique — pseudonymisation, anonymisation, agrégation, etc…— avant de les mettre à disposition du chercheur dans un espace dédié. Le chercheur analyse les données à l'aide des outils fournis par l'ETS, conformément à des exigences strictes[156]. À l'issue de l'analyse, toute extraction de résultats est soumise à validation préalable de l'OADS (EHDSR-12, EHDSR-13), et l'ensemble des données doit être supprimé dans les six mois suivant l'expiration du permis, sans exception pour les sauvegardes (OPR-5 ; art. 68(12) EEDS, cité en M7.4, §4.5.2, p. 26).

Les exigences opérationnelles du projet M7.4 s'organisent en six catégories couvrant la gestion des accès, l'audit et la conformité, la surveillance et la gestion des incidents, la gestion des risques, et la maintenance[157]. Concernant la gestion des accès, chaque utilisateur doit disposer d'une identité unique, non transférable, authentifiée par authentification multifactorielle, et les droits doivent être strictement limités au minimum nécessaire à la réalisation du projet autorisé[158]. Sur le plan de la traçabilité, tous les accès et toutes les opérations effectuées dans l'ETS doivent être journalisés, conservés au minimum un an — et plus longtemps si justifié— et disponibles à tout moment pour vérification et audit[159]. En cas d'incident de sécurité, l'opérateur technique de l'ETS doit notifier l'ORAD dans les 24 heures, fournir un rapport détaillé dans les 72 heures et un rapport final dans le mois, en cohérence avec les exigences de la Directive NIS2[160]

Malgré ces spécifications déjà bien précises, le projet M7.4 laisse ouverte la question des mesures de sécurité organisationnelles et

[152] M7.4, Executive Summary, p. 6.
[153] *Ibid.*, §. 3.1, p. 9, citant DGA, art. 2).
[154] *Ibid.*, §. 3.1, pp. 9-10; §. 4.4, pp. 19-22.
[155] *Ibid.*, §. 3.2, pp. 9-10)
[156] *Ibid.*, §. 4.3.3, p. 18)
[157] *Ibid.*, §. 4.5, pp. 22-41.
[158] *Ibid.*, §. 4.5.2, pp. 27-29.
[159] Voy. EHDSR-6, EHDSR-7, EHDSR-8 ; OPR-16, OPR-17 ; art. 73(1)(e) EEDS, cités dans M7.4, §. 4.5.4, pp. 35-36.
[160] Voy. OPR-18, OPR-19 ; M7.4, §. 4.5.4, p. 36.

techniques communes aux ETS. Il renvoie aux actes d'exécution que la Commission doit adopter en vertu de l'article 73(5) du Règlement EEDS avant mars 2027[161].

Conclusion

La lecture des quatre projets de lignes directrices révèle un important travail abordant à la fois des considérations substantielles (finalités de réutilisation des données, droits des personnes), procédurales (procédure de notification des découvertes, gestion des demandes d'accès) et techniques (infrastructure commun, sécurité) dans une perspective d'harmonisation européenne. Cette harmonisation technique et des pratiques indispensable pour garantir une évaluation uniforme des demandes d'accès et un seuil minimal commun de sécurité des données de santé disponibles au niveau des catalogues nationaux.

Leur soumission à consultation publique permettra sans aucun doute aux experts, aux professionnels de santé, aux organisations de patients et aux chercheurs de participer à la construction d'un espace de données de santé dont le pilier fondamental est l'innovation en santé sans le sacrifice de la protection des individus.

AUTRES PUBLICATIONS TEHDaS 2

17. 09.2025

M4.1.1 Draft guideline on fees related to the EHDS regulation

Second section: 4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

7.09.2025

M6.1 Guideline for health data holders on making personal and non-personal electronic health data available for reuse

6.05.2025

D6.2 Guideline for data users on good application and access practice

17.09.2025

D6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access

17.09.2025

D6.4 Technical Specifications for Data Access Application Management System (DAAMS) for Health Data Access Bodies (HDABs)

17.09.2025

M7.3 Draft Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure

12.09.2025

M7.4 Draft technical, functional and security specifications of Secure Processing Environments

[161] M7.4, §. 4.4, p. 19 ; EHDSR-18.

La Commission européenne propose une simplification du cadre règlementaire applicable aux dispositifs médicaux



Le 16 décembre 2025, la Commission européenne a présenté une proposition de règlement visant à réviser de manière ciblée les deux règlements de l'Union européenne relatifs aux dispositifs médicaux (règlement (UE) 2017/745, dit « MDR ») et aux dispositifs médicaux de diagnostic in vitro (règlement (UE) 2017/746, dit « IVDR »). Cette initiative s'inscrit dans une démarche de simplification du cadre réglementaire européen destinée à le rendre plus efficace, plus proportionné et mieux adapté aux évolutions technologiques, tout en maintenant un niveau élevé de protection de la santé publique.

La Commission justifie cette révision par les difficultés rencontrées depuis l'entrée en application du MDR et de l'IVDR : complexité des procédures, délais de certification importants, capacités limitées des organismes notifiés, coûts élevés de mise en conformité et risques pesant sur la disponibilité de certains dispositifs, en particulier pour les petites et moyennes entreprises.

La proposition prévoit notamment une simplification de certaines obligations réglementaires, un recours accru aux outils numériques, une plus grande proportionnalité des exigences au regard du niveau de risque des dispositifs ainsi qu'une amélioration de l'efficacité des procédures d'évaluation de conformité. Elle vise également à soutenir l'innovation et la compétitivité du secteur européen des technologies de santé tout en préservant les garanties de sécurité et de performance applicables aux dispositifs médicaux.

Le texte comporte enfin plusieurs dispositions destinées à mieux articuler le cadre applicable aux dispositifs médicaux avec les autres législations européennes récentes, notamment en matière d'intelligence artificielle.

À ce stade, la proposition est en cours d'examen par le Parlement européen et le Conseil.

DOCUMENTS DE RÉFÉRENCE

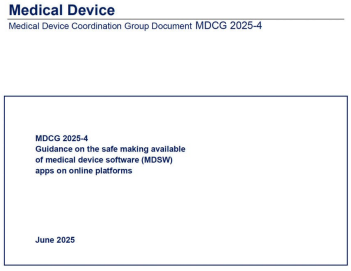
- **Fiche d'information de la Commission européenne** – Présentation synthétique des principales mesures de simplification proposées pour les dispositifs médicaux et les dispositifs médicaux de diagnostic in vitro
- **Proposition de règlement *COM(2025)* 1023 final** – Texte de la proposition de révision ciblée du MDR et de l'IVDR
- **Questions & Answers de la Commission européenne** – Questions-réponses détaillant les objectifs et les effets attendus de la réforme

Aperçu général du MDCG et de ses guides

Le *Medical Device Coordination Group* (MDCG) est le groupe de coordination institué par les règlements européens relatifs aux dispositifs médicaux (art. 103) et aux dispositifs médicaux de diagnostic in vitro (art. 98). Composé de représentants des autorités compétentes des États membres et présidé par la Commission européenne, il contribue à une mise en œuvre harmonisée de ces règlements au sein de l'Union européenne.

Dans ce cadre, le MDCG publie régulièrement des guides d'orientation (« guides MDCG ») destinés à accompagner l'application pratique des règlements MDR et IVDR. Ces guides abordent de nombreuses questions relatives à l'interprétation et à la mise en œuvre du cadre européen applicable aux dispositifs médicaux. Bien que dépourvus de caractère juridiquement contraignant, ils constituent aujourd'hui des références importantes pour l'interprétation et l'application du cadre juridique de l'Union européenne applicable aux technologies de santé.

*Les contributions qui suivent présentent trois guides récents du MDCG consacrés aux logiciels médicaux et à l'intelligence artificielle, portant respectivement sur la qualification et la classification des logiciels, leur mise à disposition sur les plateformes en ligne et l'articulation entre les règlements relatifs aux dispositifs médicaux et l'*AI Act.



L'encadrement de la mise à disposition des applications qualifiées de dispositifs médicaux sur les plateformes en ligne. Commentaire du guide MDCG 2025-4

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration croissante des technologies numériques dans le domaine de la santé transforme en profondeur les paradigmes de la prise en charge médicale. Les applications logicielles bouleversent notre mode de vie et occupent une place de plus en plus prépondérante dans les parcours de soins, couvrant un spectre extrêmement vaste d'utilisations, allant des algorithmes complexes destinés à piloter des pompes à insuline aux applications capables de détecter et de diagnostiquer des cancers de la peau.

La disponibilité directe de ces applications sur des plateformes de téléchargement grand public soulève toutefois des défis réglementaires inédits. L'accès facilité pour les patients et les professionnels de santé exige une vigilance accrue quant à la sécurité, la performance et la conformité de ces produits aux exigences du règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[162] et du règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[163].

C'est dans ce contexte de convergence entre le droit des produits de santé et le droit du numérique qu'a été publié, le 16 juin 2025, le guide MDCG 2025-4 *« Guidance on the safe making available of medical device software (MDSW) apps on online platforms »*. Approuvé par le Groupe de coordination en matière de dispositifs médicaux (« MDCG »), ce document vise à clarifier les rôles, les responsabilités et les

[162] 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, *JOUE* L. 117 du 5 mai 2017.

[163] 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, *JOUE* L. 117 du 5 mai 2017.

obligations d'information des fournisseurs de plateformes d'applications. Ce texte s'attache particulièrement à articuler les exigences du MDR et de l'IVDR avec celles introduites par le règlement (UE) 2022/2065 sur les services numériques, plus connu sous le nom de Digital Services Act (« DSA »)[164].

L'analyse de ce guide révèle l'émergence d'une architecture réglementaire stratifiée, où les obligations de conformité ne reposent plus exclusivement sur les fabricants, mais s'étendent désormais aux intermédiaires technologiques. Il convient d'examiner en détail les dispositions de ce guide, en dégageant des perspectives opérationnelles pour les acteurs de l'écosystème numérique en santé, tout en s'inscrivant dans la continuité des analyses portant sur le droit européen de la santé numérique.

I. LA QUALIFICATION JURIDIQUE DES OPERATEURS DE PLATEFORMES : UNE DISTINCTION DETERMINANTE POUR L'IMPUTATION DES RESPONSABILITES

L'un des apports majeurs du guide MDCG 2025-4 réside dans la clarification de l'applicabilité simultanée de plusieurs cadres juridiques de l'Union européenne à un même produit numérique.

La mise à disposition ou la mise en service d'un logiciel qualifié de dispositif médical (*Medical Device Software*, ci-après « MDSW ») ne peut intervenir que si le produit satisfait à l'ensemble des législations d'harmonisation applicables.

Afin d'appréhender les responsabilités respectives, le guide rappelle la terminologie réglementaire du cycle de vie du produit. La « mise sur le marché » correspond à la première mise à disposition d'un dispositif sur le marché de l'Union. Dans l'écosystème des applications, le téléchargement initial ou l'intégration (*upload*) du MDSW par le fabricant sur la plateforme correspond à cette étape cruciale. Par la suite, la « mise à disposition sur le marché » englobe toute fourniture d'un dispositif destiné à être distribué, consommé ou utilisé, la période durant laquelle l'application est accessible via la plateforme relevant de cette définition. Ces définitions permettent de scinder l'acte technologique d'hébergement en actes juridiques distincts déclenchant des responsabilités spécifiques.

Le guide envisage ainsi deux configurations réglementaires principales pour les fournisseurs de plateformes, selon qu'ils agissent en tant que simples intermédiaires ou en tant qu'opérateurs économiques de la chaîne de distribution.

Dans la première configuration, la plateforme joue un rôle d'infrastructure technique reliant les fabricants de MDSW aux patients. Selon l'article 3 du DSA, une plateforme en ligne est définie comme un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse des informations au public. Lorsque le fournisseur de la plateforme propose exclusivement des applications développées par des tiers, il agit uniquement en tant que service d'intermédiation. Sous ce régime, la plateforme facilite la conclusion de contrats à distance entre les consommateurs et les professionnels mais n'est pas considérée comme un distributeur ou un importateur au sens du MDR ou de l'IVDR. Ce statut lui permet de bénéficier des exemptions de responsabilité prévues par le DSA pour les contenus hébergés, à condition qu'elle ne joue pas un rôle actif dans la distribution et qu'elle respecte ses obligations de diligence.

La seconde configuration se présente lorsque le fournisseur de la plateforme

[164] 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), *JOUE* L. 277 du 27 octobre 2022.

s'implique directement dans la chaîne d'approvisionnement. Si la plateforme met à disposition son propre MDSW, ou si elle agit de manière à transférer la propriété ou les droits d'utilisation directs à l'utilisateur, elle revêt la qualification d'opérateur économique, à savoir de distributeur ou d'importateur. À titre d'exemple, le guide mentionne que si le fabricant de l'application est basé en dehors de l'Union européenne et que la plateforme est basée dans l'Union, cette dernière assume le rôle d'importateur. Dans ce scénario, l'applicabilité protectrice du DSA s'efface au profit des obligations strictes de la législation sectorielle (articles 13 ou 14 du MDR/IVDR[165]). L'importateur doit alors s'assurer que le fabricant a formellement désigné un mandataire au sein de l'Union, et le distributeur doit vérifier de manière proactive la sécurité et les performances du dispositif.

II. LES OBLIGATIONS DE TRANSPARENCE ET D'IDENTIFICATION : UNE MISE EN ŒUVRE DU PRINCIPE « KNOW YOUR BUSINESS CUSTOMER »

La sécurité des patients naviguant sur les plateformes numériques repose fondamentalement sur la transparence de l'information.

À cet effet, le MDCG 2025-4 impose aux plateformes, même lorsqu'elles n'agissent qu'en tant que services d'intermédiation, de concevoir leurs interfaces de manière à ce que les fabricants puissent se conformer à leurs obligations d'information.

Conformément aux articles 30 et 31 du DSA, qui consacrent le principe du « *Know Your Business Customer* » (« KYBC »), les plateformes doivent recueillir et afficher des informations précises avant d'autoriser un professionnel à proposer ses produits. L'interface de la plateforme doit impérativement permettre aux fabricants de fournir leurs coordonnées complètes (nom, adresse, numéro de téléphone et adresse électronique), les éléments permettant une identification sans ambiguïté des produits proposés, tout signe distinctif identifiant le professionnel (marque déposée, logo), ainsi que les informations relatives à l'étiquetage et au marquage conformes à la législation de l'Union (Chapitre III de l'Annexe I du MDR/IVDR).

L'obligation d'inclure le Single Registration Number (« SRN ») et l'Identifiant Unique des Dispositifs (« UDI-DI ») revêt une importance stratégique. Le SRN relie directement l'acteur économique à la base de données européenne EUDAMED, tandis que l'UDI-DI constitue la clé de voûte de la traçabilité des dispositifs, essentielle en cas de rappel de produit ou de signalement d'incidents graves. Par ailleurs, l'exigence d'un lien vers l'eIFU (*electronic Instructions for Use*) souligne la transition vers une dématérialisation complète de la documentation médicale, garantissant un accès permanent aux instructions cliniques.

Une des recommandations les plus pragmatiques du guide concerne l'architecture de l'information au sein des plateformes elles-mêmes. Pour pallier le risque de confusion chez le consommateur entre une application de bien-être et un véritable dispositif médical, le MDCG recommande fortement de créer une délimitation claire dans les bibliothèques d'applications.

Cette catégorie distincte « Dispositif Médical » ne devrait être proposée comme option aux développeurs qu'une fois qu'ils ont fourni l'ensemble des informations de conformité obligatoires énumérées précédemment. Cette mesure opère comme un mécanisme de filtrage ex-ante, empêchant un développeur de revendiquer de manière fallacieuse une finalité médicale

[165] Les articles 13 et 14 de ces deux règlements sont respectivement consacrés aux obligations générales des importateurs et à celles des distributeurs.

sans avoir préalablement satisfait aux rigueurs réglementaires.

III. LES MÉCANISMES DE VÉRIFICATION ET DE SURVEILLANCE : DE L'ÉVALUATION PRÉALABLE A L'INJONCTION DE RETRAIT

La protection des patients requiert une dynamique de vérification continue. Le guide MDCG 2025-4 détaille les devoirs de vérification des plateformes à travers deux phases temporelles distinctes, assorties de mécanismes d'action corrective.

Avant même de permettre à un professionnel de proposer son application MDSW, la plateforme doit procéder à une évaluation préalable. Le niveau d'exigence juridique requis ici est celui des « meilleurs efforts ». La plateforme doit s'efforcer d'évaluer si les informations requises (coordonnées, SRN, UDI-DI, etc.) sont fiables, complètes et rendues disponibles pour les utilisateurs. Bien que le DSA n'impose pas à la plateforme de se substituer aux autorités compétentes, l'incapacité d'une plateforme à démontrer qu'elle a déployé ses meilleurs efforts pourrait compromettre son exemption de responsabilité en tant qu'hébergeur.

L'obligation de surveillance se poursuit au stade post-publication. Une fois que le professionnel est autorisé à proposer ses produits, le fournisseur de la plateforme est tenu d'effectuer des contrôles aléatoires. Pour cette surveillance, la norme juridique glisse vers l'exigence d'« efforts raisonnables ». La plateforme doit vérifier si les produits proposés ont été identifiés comme illégaux en croisant les données avec des bases de données officielles en ligne, librement accessibles et lisibles par machine. Cette disposition implique opérationnellement que les plateformes d'applications intègrent des requêtes automatisées vers les bases de données institutionnelles, telles qu'EUDAMED ou les registres des autorités nationales compétentes, afin d'identifier les certificats suspendus ou les produits rappelés.

Le cœur de la régulation des contenus illicites repose sur le mécanisme d'alerte et d'action. Les plateformes d'applications doivent mettre en œuvre des mécanismes permettant à toute entité de signaler la présence d'un contenu illégal. La réception d'un tel signalement est réputée conférer au fournisseur une « connaissance ou conscience effective » de l'illicéité du contenu. Dès l'acquisition de cette connaissance, la plateforme doit prendre des « décisions rapides et diligentes » concernant le retrait du contenu pour conserver son immunité d'intermédiaire. De surcroît, le guide rappelle que les autorités nationales compétentes ont le pouvoir d'émettre des injonctions spécifiques directement à l'encontre des fournisseurs de plateformes pour contraindre la suppression d'un contenu illégal.

Enfin, le guide réserve un traitement particulier aux « Très Grandes Plateformes en Ligne » (Very Large Online Platforms – « VLOPs »), désignées par la Commission européenne.

Conformément aux articles 34 et 35 du DSA, ces acteurs doivent procéder, au moins une fois par an, à des évaluations des risques systémiques découlant de la conception ou du fonctionnement de leur service, y compris la diffusion de contenus illicites tels que des dispositifs médicaux non conformes. Ils sont par la suite tenus de mettre en œuvre des mesures d'atténuation proportionnées, transférant ainsi une part de la politique de prévention des risques aux départements de conformité de ces entreprises.

IV. INTERDEPENDANCES NORMATIVES : L'ARTICULATION AVEC L'IA ACT ET L'ESPACE EUROPÉEN DES DONNÉES DE SANTÉ

L'analyse de l'opérationnalisation du guide MDCG 2025-4 ne saurait être

complète sans la replacer dans le macro-écosystème du droit européen du numérique en santé. Le guide s'inscrit dans une architecture réglementaire complexe où interagissent de multiples textes fondateurs.

La publication du guide MDCG 2025-4 intervient de manière quasi concomitante avec celle du guide MDCG 2025-6[166], publié le 19 juin 2025, qui aborde spécifiquement l'interaction entre le MDR/IVDR et le nouveau règlement sur l'Intelligence Artificielle (IA Act)[167]. De nombreuses applications MDSW intègrent aujourd'hui des modèles d'apprentissage automatique. Sous l'IA Act, ces logiciels médicaux, dès lors qu'ils nécessitent l'intervention d'un organisme notifié au titre du MDR, sont classés comme des systèmes d'IA à haut risque. Pour les plateformes d'applications, cette superposition réglementaire signifie que la vérification de conformité s'alourdit. Le marquage CE de l'application ne devra plus seulement attester de la performance clinique, mais également de la robustesse algorithmique, de l'absence de biais discriminatoires et de la transparence de l'IA. L'information transparente exigée à l'égard du patient devra ainsi s'étendre aux paramètres de l'IA, afin d'assurer que l'utilisateur final comprenne les limites du diagnostic généré par l'application.

Par ailleurs, la question du traitement des données de santé par ces applications renvoie inévitablement aux exigences de l'Espace Européen des Données de Santé (EEDS)[168]. L'adoption du règlement sur l'EEDS instaure de nouvelles normes d'interopérabilité pour les dossiers médicaux électroniques et les applications de bien-être revendiquant une telle interopérabilité. Une application MDSW téléchargée depuis un magasin d'applications européen devra, à terme, s'insérer de manière sécurisée dans l'infrastructure de santé du patient.

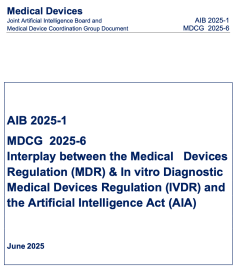
En conclusion, le guide MDCG 2025-4 marque une étape décisive dans la maturation du droit européen de la santé numérique. En clarifiant le statut des plateformes de téléchargement en ligne, il comble un vide juridique qui permettait jusqu'alors à certaines applications logicielles de se soustraire à la rigueur de la matériovigilance. En liant les obligations sectorielles du MDR et de l'IVDR aux obligations horizontales de régulation de l'internet portées par le DSA, les instances européennes créent un filet de sécurité où la responsabilité est partagée entre le concepteur médical et l'hébergeur technologique. Les plateformes en ligne ne peuvent plus prétendre à une neutralité aveugle ; elles sont désormais contraintes d'exercer un rôle de vigie sanitaire, assumant des devoirs de vérification préalable, de surveillance continue et de réaction immédiate face aux contenus illicites. Cette structuration est la condition essentielle pour préserver la confiance des citoyens et garantir que l'innovation numérique ne sacrifie jamais l'exigence clinique.

MDCG 2025-4 - *Guidance on the safe making available of medical device software (MDSW) apps on online platforms*, June 2025

[166] AIB 2025-1 / MDCG 2025-6, *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AI ACT)*, June 2025.

[167] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

[168] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.


Medical Devices
Joint Artificial Intelligence Board and Medical Device Coordination Group Document
AIB 2025-1
MDCG 2025-6

AIB 2025-1
MDCG 2025-6
Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)
June 2025

L'articulation opérationnelle entre le règlement sur les dispositifs médicaux et la législation sur l'intelligence artificielle. Commentaire du Guide MDCG 2025-6

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration croissante et inéluctable des technologies d'intelligence artificielle (« IA ») au sein des dispositifs médicaux bouleverse en profondeur le paysage technologique et réglementaire européen de la santé. Jusqu'à récemment, l'encadrement de ces innovations numériques reposait exclusivement sur le règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[169] et le règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[170]. Bien que ces deux textes fondateurs imposent des exigences particulièrement strictes en matière de sécurité, de performance clinique et de gestion des risques liés aux logiciels dispositifs médicaux, ils n'ont pas été originellement conçus pour appréhender les vulnérabilités spécifiques, évolutives et inédites inhérentes aux systèmes algorithmiques complexes. L'opacité des réseaux de neurones profonds, la dérive des données d'apprentissage, les biais cognitifs encodés ou encore les menaces avancées en matière de cybersécurité constituent autant de défis que l'approche traditionnelle de la conformité médicale peinait à endiguer de manière exhaustive.

Afin de combler ces lacunes normatives tout en garantissant un niveau particulièrement élevé de protection des droits fondamentaux, de la santé et de la sécurité des citoyens de l'Union européenne, le législateur a adopté le règlement (UE) 2024/1689 fixant des règles harmonisées concernant l'intelligence artificielle, communément désigné sous l'acronyme « *AI Act* »[171]. L'entrée en vigueur de ce texte à vocation transversale instaure de fait un modèle de double conformité pour les fabricants de dispositifs médicaux intégrant de l'IA, dispositifs désormais catégorisés sous l'appellation de « *Medical Device Artificial Intelligence* » (« MDAI »). Cette dualité réglementaire, bien qu'absolument justifiée sur le plan de la politique de sécurité publique européenne, engendre une complexité opérationnelle majeure pour les opérateurs économiques. Ces derniers doivent désormais naviguer entre des corpus juridiques aux philosophies distinctes, dont les terminologies, les exigences

[169] 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, *JOUE* L. 117 du 5 mai 2017.

[170] 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, *JOUE* L. 117 du 5 mai 2017.

[171] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

documentaires et les cycles d'évaluation se superposent, créant un risque tangible de paralysie administrative et d'engorgement des organismes notifiés.

C'est précisément dans ce contexte d'incertitude juridique, et en réponse à une attente pressante de la part de l'industrie des technologies médicales, que le Bureau de l'intelligence artificielle (« AIB ») et le Groupe de coordination des dispositifs médicaux (« MDCG ») ont publié, en juin 2025, le document d'orientation conjoint AIB 2025-1 / MDCG 2025-6, intitulé « *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AI ACT)* ». Ce guide stratégique, structuré sous la forme d'une foire aux questions, constitue la pierre angulaire de la nouvelle architecture de mise en conformité. Il a pour vocation première d'expliciter l'application simultanée et complémentaire de ces textes, en parfaite adéquation avec l'approche du nouveau cadre législatif européen, afin d'assurer que l'innovation médicale ne soit pas entravée par des redondances procédurales injustifiées.

L'analyse exégétique de ce guide révèle une volonté manifeste des autorités européennes de rationaliser les efforts de mise en conformité. Le législateur encourage activement l'intégration des nouvelles exigences de l'AI Act au sein des processus de gestion de la qualité et des architectures documentaires déjà exigés par le MDR et l'IVDR. Toutefois, cette synergie, évidente sur le plan théorique, se heurte à des défis pratiques considérables lorsqu'il s'agit de décliner de manière purement opérationnelle des concepts novateurs tels que la gouvernance algorithmique des données, l'explicabilité des modèles, la surveillance humaine par conception, ou encore la qualification juridique des modifications substantielles apportées aux systèmes d'apprentissage continu.

La présente analyse s'attache à décrypter les mécanismes de qualification et de classification des MDAI, les stratégies d'optimisation de la fusion des systèmes de gestion de la qualité (« SMQ » pour système de management de la qualité) et de la documentation technique, ainsi que les nouvelles obligations pesant sur le cycle de vie complet de ces dispositifs médicaux de nouvelle génération. De la conception rigoureuse des jeux de données d'entraînement jusqu'à la surveillance post-commercialisation proactive, cette étude intègre également les dynamiques réglementaires adjacentes. Seront également abordés les liens avec l'Espace européen des données de santé (EEDS)[172] et les conséquences de la nouvelle directive sur la responsabilité du fait des produits défectueux[173] afin d'en définir des repères clairs et utiles sur le terrain.

I. PERIMETRE D'APPLICATION ET HEURISTIQUE DE CLASSIFICATION DES DISPOSITIFS MDAI

A. Précisions terminologiques : une indispensable traduction des rôles opérationnels

La toute première étape de la mise en conformité conjointe exige une maîtrise absolue des chevauchements lexicaux et des divergences terminologiques entre la législation sur l'IA et la législation sectorielle médicale. Le guide MDCG 2025-6 prend le soin de lever d'emblée toute ambiguïté concernant l'identification des opérateurs économiques et des différents acteurs de la chaîne de soins. Sur

[172] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.

[173] Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil, JOUE du 18 novembre 2024.

le plan strictement juridique, l'entité qualifiée de « fabricant » au sens de l'article 2 du MDR et de l'IVDR correspond très exactement à l'entité qualifiée de « fournisseur » (*provider*) selon les dispositions de l'AI Act. Il incombe par conséquent au fabricant du dispositif médical d'assumer l'intégralité des obligations incombant au fournisseur du système d'IA, regroupant ainsi les responsabilités de conception, de validation et de mise sur le marché sous une seule et même entité juridique.

Une distinction encore plus critique sur le plan de la responsabilité est opérée concernant les entités situées en bout de chaîne de déploiement. L'AI Act introduit le concept novateur de « déployeur », défini de manière extensive à l'article 3, paragraphe 4 comme toute personne physique ou morale, autorité publique, agence ou tout autre organisme qui utilise un système d'IA sous son autorité, à l'exception d'une utilisation dans le cadre d'une activité personnelle non professionnelle. Le guide MDCG 2025-6 précise expressément que ce concept spécifique à l'AI Act ne saurait en aucun cas être confondu avec la notion d'« utilisateur » telle qu'elle est définie et appréhendée sous le MDR et l'IVDR.

Afin de clarifier cette dichotomie essentielle pour la mise en œuvre des obligations réglementaires, il convient de se référer à la typologie de ces acteurs de santé :

Terme selon le MDR / IVD	**Terme équivalent ou distinct selon l'AI Act**	**Définition opérationnelle dans le secteur médical**
Fabricant (*Manufacturer*)	Fournisseur (*Provider*)	L'entité juridique qui conçoit, développe et met sur le marché le logiciel médical intégrant l'IA, assumant l'entière responsabilité de la double conformité.
Aucun équivalent direct	Déployeur (*Deployer*)	L'établissement de santé, l'hôpital, la clinique ou l'autorité de santé publique qui acquiert le MDAI, l'intègre dans son infrastructure informatique clinique et en gère l'exploitation sous sa propre autorité.
Utilisateur (*User*)	Non applicable directement au sens du déployeur	Le professionnel de santé (médecin, radiologue, infirmier) qui manipule directement l'interface du dispositif pour établir un diagnostic, ou le patient lui-même dans le cas de thérapies numériques (DTx).

Cette distinction s'avère fondamentale en pratique, car elle détermine de manière univoque la répartition des responsabilités en matière de transparence algorithmique, de fourniture des notices d'utilisation spécifiques et d'obligations de surveillance humaine. Le fabricant doit concevoir son système non seulement pour qu'il soit cliniquement efficace entre les mains de l'utilisateur final, mais également pour qu'il fournisse au déployeur les métriques de fonctionnement (logs) et la transparence nécessaires à la gestion des risques institutionnels et éthiques.

B. Le mécanisme de déclenchement : quand un MDAI devient-il une IA à haut risque ?

Le cœur névralgique de l'articulation entre les deux cadres législatifs réside dans la détermination du niveau de risque du système d'IA. L'AI Act a été structuré selon une approche proportionnée, n'imposant ses obligations les plus contraignantes qu'aux seuls systèmes d'IA qualifiés de « haut risque ». Selon l'article 6, paragraphe 1 de l'AI Act, et tel qu'explicité en détail par le guide MDCG 2025-6, un dispositif MDAI revêt la qualification de système d'IA à haut risque si, et seulement si, deux conditions juridiques cumulatives sont strictement remplies.

Premièrement, le MDAI doit constituer un composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union énumérée à l'annexe II de l'AI Act (laquelle inclut le MDR et l'IVDR), ou le système d'IA doit être lui-même un dispositif médical au sens de ces mêmes règlements. Le guide précise par ailleurs que la Commission européenne élabore des lignes directrices horizontales pour affiner ce concept de « composant de sécurité », mais son application dans le domaine médical est généralement évidente dès lors que le logiciel a une finalité diagnostique ou thérapeutique.

Deuxièmement, condition déterminante, le dispositif médical concerné doit être soumis à une procédure d'évaluation de la conformité réalisée par une tierce partie, à savoir un organisme notifié, conformément aux dispositions de classification du MDR ou de l'IVDR. Cette règle d'assujettissement conditionnel crée une architecture réglementaire où l'intervention d'un organisme notifié agit comme l'interrupteur exclusif déclenchant les obligations de l'AI Act relatives au haut risque.

Le tableau de classification fourni par le MDCG permet de cartographier cette dynamique d'application avec précision.

Classification	Notified Body Involved?	AIA High-Risk (Art. 6(1)) conditions fulfilled?
MDR Class I (non-sterile, non-measuring, non-reusable surgical)	❌ No	❌ No
MDR Class I (sterile, measuring, reusable surgical)	✅ Yes	✅ Yes
MDR Class IIa, IIb, III	✅ Yes	✅ Yes
MDR Annex XVI[10]	✅ Yes	✅ Yes
IVDR Class A (non-sterile)	❌ No	❌ No
IVDR Class A)	✅ Yes	✅ Yes
IVDR Class B, C, D	✅ Yes	✅ Yes
In-house device according to Art. 5(5) MDR/IVDR	❌ No	❌ No

10 Note: Except for non-invasive devices which are classified as Class I in accordance with 'Guidance on qualification and classification of Annex XVI products - A guide for manufacturers and notified bodies'.

L'analyse scrupuleuse de cette matrice de classification met en exergue des points d'attention stratégiques majeurs pour les fabricants. Un logiciel médical intégrant de l'IA et classé en classe I sous le MDR échapperait techniquement à la qualification de haut risque de l'AI Act. Toutefois, il convient de rappeler que la règle 11 de l'annexe VIII du MDR tend aujourd'hui à classifier la quasi-totalité des logiciels d'aide à la décision clinique en classe IIa ou supérieure, rendant l'échappatoire de la classe I purement marginale en pratique, sauf exceptions très spécifiques ou logiciels intégrés à des dispositifs de classe I mesurants.

Il est également indispensable de souligner que l'AI Act s'applique de plein droit aux produits ne revendiquant aucune destination médicale, mais qui relèvent du champ d'application du MDR par l'intermédiaire de son Annexe XVI, tels que les équipements de stimulation cérébrale à visée non médicale ou certains logiciels esthétiques. Dès lors que ces produits d'imitation médicale intègrent une IA et requièrent l'intervention d'un organisme notifié en raison de leur profil de risque inhérent, ils basculent inévitablement dans la catégorie des systèmes d'IA à haut risque de l'AI Act. À l'inverse, les algorithmes diagnostiques développés, fabriqués et utilisés exclusivement au sein d'un même établissement de santé (bénéficiant de la clause d'exemption « *in-house* » de l'article 5 paragraphe 5 du MDR ou de l'IVDR) échappent à l'obligation de certification par un organisme notifié. Par effet domino, ils échappent logiquement à la qualification de système d'IA à haut risque de l'article 6 paragraphe 1 de l'AI Act, créant ainsi un environnement réglementaire allégé pour la recherche et l'innovation intra-hospitalière, bien que la conformité aux exigences générales de sécurité et de performance demeure impérative.

C. L'indépendance stricte de la classification des risques : une dichotomie maintenue

Une confusion persistante parmi les opérateurs économiques, et parfois même au sein des directions des affaires réglementaires, consiste à présumer qu'une qualification d'« IA à haut risque » au titre de l'AI Act entraîne mécaniquement une surclassification du dispositif médical sous le MDR ou l'IVDR. Le guide MDCG 2025-6 réfute formellement et définitivement cette hypothèse. La classification d'un système d'IA comme étant à haut risque en vertu de l'article 6 paragraphe 1 de l'AI Act n'implique en aucun cas que le dispositif médical ou le dispositif médical de diagnostic in vitro doive basculer dans une classe de risque supérieure selon les règles de classification de l'annexe VIII du MDR ou de l'annexe VIII de l'IVDR.

La relation de causalité est strictement unilatérale : c'est exclusivement la classification MDR/IVDR qui, en déterminant la nécessité de recourir à un organisme notifié, engendre la qualification AI Act de haut risque. L'AI Act n'a donc aucune incidence sur la détermination de la classe de risque médicale. Néanmoins, la qualification AI Act impose un niveau de contrôle réglementaire, de transparence algorithmique et de surveillance humaine considérablement accru, augmentant la complexité de l'évaluation de la conformité sans pour autant modifier l'étiquette de classe (qu'il s'agisse d'un dispositif IIa, IIb ou III) du dispositif médical.

De surcroît, le guide rappelle avec force que même si un dispositif MDAI n'est pas qualifié de haut risque sous l'AI Act (par exemple un dispositif *in-house*), le fabricant ou le fournisseur reste impérativement tenu de respecter certaines obligations fondamentales de ce texte transversal. Sont notamment visées les dispositions de l'article 5, qui énumèrent les pratiques d'IA strictement interdites au sein de l'Union européenne, ainsi que les obligations de l'article 50 relatives à la transparence, qui imposent par exemple d'informer les utilisateurs lorsqu'ils interagissent avec certains systèmes d'IA de type agent

conversationnel (chatbot) ou système de reconnaissance des émotions, obligations dont l'application est totalement indépendante de la classification MDR/IVDR.

D. Dispositions transitoires : la gestion du calendrier d'application et des dispositifs hérités

L'approche opérationnelle nécessite de prendre en compte avec la plus grande rigueur le calendrier d'application du nouveau cadre. Si l'AI Act est officiellement entré en vigueur de manière globale en 2024, les dispositions spécifiques relatives aux systèmes d'IA à haut risque relevant de l'Annexe II (qui inclut explicitement le MDR et l'IVDR) ne s'appliqueront pleinement et de manière opposable qu'à partir du 2 août 2027. Le guide MDCG 2025-6 apporte à ce titre des clarifications indispensables sur la gestion épineuse des dispositifs dits « hérités » (*legacy devices*).

Si un dispositif médical intégrant une IA a été mis sur le marché de l'Union ou mis en service avant cette date fatidique du 2 août 2027, les exigences contraignantes de l'AI Act pour les systèmes à haut risque ne s'appliquent pas de manière rétroactive. Cependant, cette protection transitoire est assortie d'une condition résolutoire majeure : si ce système d'IA hérité fait l'objet d'une modification significative de sa conception ou de sa finalité à compter du 2 août 2027, il perd instantanément le bénéfice de cette exemption et bascule sous l'empire complet et immédiat de l'AI Act, incluant toutes les obligations afférentes aux systèmes d'IA à haut risque de l'Annexe I. En revanche, tout dispositif médical intégrant une IA mise sur le marché ou mis en service pour la toute première fois à partir de cette date pivot du 2 août 2027 devra naître en pleine conformité avec les deux cadres législatifs, imposant aux équipes de développement d'intégrer ces doubles contraintes dès les premières phases de conception.

II. FUSION STRATÉGIQUE ET DOCUMENTAIRE : L'INTÉGRATION DES SYSTÈMES DE GESTION DE LA QUALITE (SMQ)

A. Le principe de flexibilité : l'article 8 paragraphe 2 de l'AI Act comme levier d'efficience réglementaire

La mise en œuvre d'une double conformité stricte, si elle devait être gérée en silos étanches, conduirait inévitablement à une paralysie administrative des fabricants de technologies médicales et à l'engorgement définitif des organismes notifiés, lesquels opèrent déjà sous une tension systémique depuis l'entrée en application du MDR et de l'IVDR. Pleinement conscient de ce risque majeur pour la compétitivité et la capacité d'innovation de l'industrie européenne, le législateur a introduit un mécanisme d'efficience déterminant à l'article 8 paragraphe 2 de l'AI Act. Ce paragraphe fondamental permet aux fabricants de dispositifs médicaux de choisir d'intégrer les processus de test, les mécanismes de *reporting*, les informations spécifiques et la documentation exigés par la législation sur l'IA directement et organiquement dans les procédures documentaires déjà établies en vertu du MDR ou de l'IVDR.

Le guide MDCG 2025-6 insiste de manière particulièrement appuyée sur cette disposition libératoire. Il encourage très vivement les fabricants de MDAI à exploiter cette flexibilité procédurale afin d'éviter les redondances de tests, de réduire les charges administratives supplémentaires et de garantir la cohérence structurelle de leurs processus internes. Sur le plan purement opérationnel, cela signifie qu'un fabricant n'est en aucun cas tenu d'élaborer un dossier technique isolé et spécifique à l'AI Act, ni de maintenir un système de gestion de la qualité (SMQ) parallèle et déconnecté de la norme ISO 13485. Une documentation technique unique et un SMQ intégré, astucieusement conçus pour démontrer la conformité aux exigences

générales de sécurité et de performance du MDR/IVDR tout en absorbant de manière granulaire les exigences spécifiques liées à l'IA, constituent la voie royale, pragmatique et recommandée vers la conformité. Toutefois, le guide formule une mise en garde explicite : cette fusion documentaire et cette rationalisation des procédures ne dispensent en rien le fabricant d'une démonstration de conformité exhaustive. Le système MDAI doit répondre de manière démontrable, auditable et sans équivoque à toutes les exigences matérielles applicables des deux règlements européens simultanément.

B. L'extension conceptuelle du système de gestion de la qualité : au-delà du risque médical classique

Les articles 10 du MDR et de l'IVDR imposent d'ores et déjà la mise en œuvre, le maintien et l'amélioration continue d'un SGQ strictement proportionné à la classe de risque et au type spécifique du dispositif médical Dans une approche en miroir, l'article 17 de l'AI Act introduit une obligation symétrique pour les systèmes d'IA à haut risque, exigeant la mise en place d'un SMQ couvrant au moins treize aspects procéduraux obligatoires, lesquels doivent également être mis en œuvre de manière proportionnée à la taille de l'organisation du fournisseur. Le guide MDCG 2025-6 explicite de manière très claire que les obligations du SMQ prévues par l'AI Act sont ciblées très spécifiquement sur la nature algorithmique du système et sont donc intrinsèquement complémentaires au SMQ global du dispositif médical exigé par les textes sectoriels.

Afin que le SMQ existant d'un fabricant de dispositifs médicaux (généralement adossé à la norme ISO 13485) devienne pleinement conforme à l'AI Act, il convient de procéder à une refonte de la politique qualité pour y incorporer de nouveaux macro-processus. Les ajouts opérationnels indispensables, qui nécessitent souvent l'implication d'ingénieurs en science des données et d'experts en éthique algorithmique, incluent notamment :

1. La gouvernance et la gestion fine des données : l'établissement de protocoles de niveau ingénierie stricts régissant la provenance, la collecte, le nettoyage, la représentativité statistique et l'évaluation continue des biais au sein des jeux de données d'entraînement, de validation et de test.
2. La conservation des enregistrements : la mise en place de capacités techniques avancées de journalisation automatique (logs) inaltérables, permettant la traçabilité complète des événements et du comportement de l'algorithme tout au long du cycle de vie opérationnel du système.
3. La transparence et la surveillance humaine : l'intégration de processus ergonomiques garantissant que la conception de l'interface utilisateur permet aux professionnels de santé d'exercer un contrôle critique effectif, de comprendre le cheminement de la décision algorithmique et, de manière cruciale, de pouvoir contourner ou annuler les décisions de l'IA si le contexte clinique l'exige.
4. La stratégie de conformité réglementaire intégrée : l'adaptation du plan de développement logiciel pour que chaque jalon de conception et de vérification intègre conjointement et harmonieusement les impératifs de conformité du MDR et de l'AI Act.

Il convient de noter que l'élaboration de normes harmonisées européennes et internationales pertinentes (notamment par le Comité technique mixte 21 du CEN/CENELEC[174]) est actuellement en

[174] Le comité technique mixte 21 (souvent abrégé JTC21 pour Joint Technical Committee 21) est un groupe de travail créé conjointement par les deux principaux organismes européens de normalisation :

cours à la date de rédaction de ce commentaire. Ces futurs standards viendront cristalliser ces nouvelles exigences sous forme de spécifications auditables. Dans l'intervalle, la réingénierie des processus qualité doit impérativement s'inspirer des lignes directrices horizontales publiées par la Commission européenne afin de garantir un alignement précoce avec les attentes des évaluateurs.

C. Gestion des risques et du cycle de vie : l'intégration des risques liés aux droits fondamentaux

Tant le cadre du MDR/IVDR (notamment via l'application de la norme harmonisée ISO 14971 relative à l'application de la gestion des risques aux dispositifs médicaux) que l'AI Act (au travers de son article 9) imposent un système de gestion des risques structuré comme un processus itératif, systématique et continu, s'étendant sur l'intégralité du cycle de vie du dispositif, des premières phases de conception pré-clinique jusqu'au démantèlement post-commercialisation. Néanmoins, l'intégration de l'AI Act contraint les fabricants à élargir considérablement le périmètre classique de l'analyse des risques médicaux, créant un véritable défi conceptuel pour les ingénieurs qualité.

En effet, l'évaluation ne doit plus se limiter exclusivement aux risques cliniques directs pesant sur le patient ou l'utilisateur (tels que la mauvaise attribution d'un traitement due à un faux positif). L'AI Act impose d'identifier, d'analyser et d'atténuer les « risques connus et raisonnablement prévisibles que le MDAI à haut risque peut poser pour les droits fondamentaux » (considérant n°65). Le guide MDCG 2025-6 précise ainsi que les fabricants doivent intégrer dans leurs matrices de risques, l'évaluation des biais dans les données d'apprentissage pouvant mener à une discrimination interdite (risque éthique et légal), la robustesse du système d'apprentissage automatique face aux cyberattaques sophistiquées (risque sécuritaire), et la fiabilité de l'interface homme-machine au regard de la surveillance humaine.

De plus, ce processus enrichi de gestion des risques doit intégrer des mesures organisationnelles garantissant un usage fiable en milieu clinique réel. Cela implique la documentation des mesures d'atténuation qui dépassent la simple modification du code source, pouvant inclure la mise en place de programmes de formation spécifiques et obligatoires destinés aux déployeurs et aux utilisateurs. Il s'agit d'une évolution paradigmatique : le fabricant est désormais tenu de s'assurer que l'environnement de déploiement dispose de la maturité et des compétences nécessaires pour interagir avec l'IA sans engendrer de nouveaux risques systémiques liés à la dépendance technologique ou à l'automatisation excessive.

III. EXIGENCES DOCUMENTAIRES ET REGLES D'ECHANTILLONNAGE DES ORGANISMES NOTIFIES

La constitution de la documentation technique, qui sert de fondement probatoire à toute évaluation de la conformité, obéit également au principe primordial de l'intégration et de la rationalisation. Les annexes II et III du MDR et de l'IVDR imposent déjà la fourniture de descriptions extrêmement détaillées de l'architecture logicielle, de la destination médicale, des méthodes de traitement des données cliniques, ainsi que des stratégies complètes

---

le CEN (comité européen de normalisation) le CENELEC (comité européen de normalisation électrotechnique). Sa mission principale est d'élaborer des normes européennes harmonisées spécifiquement dédiées à l'intelligence artificielle. La Commission européenne a formellement mandaté ce comité pour traduire les obligations juridiques de l'AI Act en spécifications techniques et opérationnelles claires.

de gestion des risques et des résultats de l'évaluation clinique. De son côté, l'article 11 et l'annexe IV de l'AI Act exigent des éléments complémentaires fortement axés sur la redevabilité algorithmique, l'explicabilité du modèle et la traçabilité de sa construction. Ces éléments incluent une documentation approfondie des choix de conception de l'architecture du réseau de neurones, la description des ressources informatiques déployées pour les phases d'entraînement et de test, les métriques précises de performance algorithmique, ainsi que les pratiques détaillées de gouvernance des données employées.

Le guide MDCG 2025-6 confirme et sécurise la position selon laquelle les fabricants doivent établir un ensemble unique et cohérent de documentation technique démontrant la satisfaction croisée de toutes ces exigences. Une interrogation opérationnelle majeure pour l'industrie concernait la méthodologie d'évaluation de cette volumineuse documentation par les organismes notifiés, telle que définie par l'annexe VII de l'AI Act, et particulièrement son articulation avec les règles d'échantillonnage strictes prévues par le MDR/IVDR.

Le guide apporte une réponse univoque et particulièrement rassurante : les règles d'échantillonnage de la procédure d'évaluation de la conformité qui régissent le dispositif médical restent pleinement applicables à la partie IA du système. Par conséquent, pour les dispositifs relevant de la classe IIa ou IIb (sous le MDR) ou des classes B ou C (sous l'IVDR), l'organisme notifié évaluera la documentation technique spécifique à l'AI Act en suivant les mêmes règles d'échantillonnage représentatif par catégorie ou par groupe générique de dispositifs, telles que minutieusement définies dans le document d'orientation MDCG 2019-13[175]. Cette précision réglementaire constitue une avancée décisive pour l'industrie des technologies médicales. Elle permet d'éviter une évaluation systématique, individuelle et chronophage de chaque variante logicielle mineure d'un algorithme d'IA au sein d'une même gamme de produits, limitant ainsi de manière significative l'explosion des coûts d'audit et la congestion des délais d'accès au marché européen.

IV. GOUVERNANCE DES DONNÉES : LA FONDATION JURIDIQUE ET TECHNIQUE DE LA FIABILITÉ ALGORITHMIQUE

A. L'article 10 de l'AI Act et la taxonomie réglementaire des données

Si le MDR exige déjà que les données cliniques utilisées pour l'évaluation des performances soient robustes, fiables et représentatives de la population visée afin de démontrer la sécurité du dispositif (conformément à l'Annexe XIV du MDR et détaillé dans le document MDCG 2020-1[176]), l'AI Act, par le biais de son article 10, s'aventure beaucoup plus loin dans la granularité et la rigueur de l'ingénierie des données. La gouvernance des données n'est plus considérée uniquement comme un moyen de valider une allégation médicale en fin de processus ; elle devient une exigence essentielle, autonome et préalable, conditionnant la légalité même du développement du système d'IA (**Page suivante**).

[175] MDCG 2019-13 Rev.1, *Guidance on sampling of MDR Class IIa / Class IIb and IVDR Class B / Class C devices for the assessment of the technical documentation*, December 2024.

[176] MDCG 2020-1, *Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software*, March 2020.

L'AI ACT impose une taxonomie juridique stricte des données utilisées au cours du cycle de vie du modèle d'apprentissage. Afin d'harmoniser les pratiques, l'article 3 de l'AI ACT définit réglementairement les concepts fondamentaux de la science des données, que le guide MDCG rappelle :

Type de données (Art. 3 AI Act)	Définition et utilité dans le développement du MDAI
Données d'entraînement (*Training data*)	Données utilisées pour entraîner le système d'IA par l'ajustement (*fitting*) de ses paramètres apprenants (ex: les poids d'un réseau de neurones).
Données de validation (*Validation data*)	Données utilisées pour fournir une évaluation du système d'IA entraîné et pour ajuster ses hyperparamètres non apprenants, afin de prévenir les phénomènes de surapprentissage (*overfitting*) ou de sous-apprentissage (*underfitting*).
Ensemble de données de validation	Un ensemble de données distinct ou une partie de l'ensemble de données d'entraînement, utilisé par le biais d'une séparation fixe ou variable (*split*).
Données de test (*Testing data*)	Données utilisées pour fournir une évaluation totalement indépendante du système d'IA afin de confirmer les performances attendues avant sa mise sur le marché ou sa mise en service.

Le guide MDCG 2025-6 souligne avec insistance que ces différents ensembles de données de formation, de validation et de test doivent, en vertu de l'AI Act, être « *d'une grande qualité, pertinents, suffisamment représentatifs et, dans la mesure du possible, exempts d'erreurs et complets au vu de la destination prévue* » (considérant n°67). L'obligation d'avoir des jeux de données dotés de propriétés statistiques appropriées impose aux fabricants de documenter minutieusement et scientifiquement les protocoles de collecte de ces données.

Les données d'entraînement et de test doivent refléter de manière exhaustive et proportionnée les caractéristiques de la population cible. Cela inclut des variables telles que l'âge, le sexe, le genre, la race, l'origine ethnique, la localisation géographique, ainsi que les comorbidités spécifiques au contexte clinique visé. Cette exigence drastique est d'une importance vitale pour maîtriser le risque de dérive des données, s'assurer de la généralisation des performances du modèle au-delà de l'échantillon d'apprentissage, et éviter des défaillances dramatiques de précision lors d'un déploiement dans des contextes cliniques non anticipés par les développeurs.

B. Atténuation des biais algorithmiques et respect inconditionnel des droits fondamentaux

La nouveauté radicale et philosophiquement marquante de l'AI Act réside dans l'obligation positive d'examiner en profondeur les ensembles de données et de mitiger les biais algorithmiques susceptibles d'affecter la santé, d'avoir une incidence négative sur les droits fondamentaux ou de conduire à une

discrimination prohibée par le droit de l'Union européenne. Dans le domaine de la santé numérique, un algorithme d'analyse dermatologique entraîné de manière disproportionnée sur des phototypes clairs et affichant des performances significativement dégradées sur des peaux foncées constitue l'archétype du biais discriminatoire et d'un risque inacceptable pour l'équité des soins et la sécurité des patients.

Les fabricants de dispositifs MDAI doivent concevoir des processus statistiques et d'assurance qualité permettant la détection et la correction précoce de ces biais dès la phase de constitution des bases de données. De surcroît, le guide MDCG 2025-6 met en avant l'importance cruciale des exigences de journalisation (logging) automatique imposées par l'AI Act. Ces capacités techniques intégrées visent à faciliter la traçabilité des décisions de l'IA et l'identification rétrospective de situations où des biais latents se manifesteraient uniquement lors de l'exploitation post-commercialisation par le déployeur, ou à la suite d'une modification logicielle en conditions réelles.

C. L'interaction stratégique avec le RGPD et l'Espace européen des données de santé

La gestion, la collecte et le traitement de ces gigantesques volumes de données médicales, par nature éminemment sensibles, posent immédiatement le défi de l'articulation avec le Règlement général sur la protection des données (« RGPD »). Le guide MDCG 2025-6 précise de manière sans équivoque que les pratiques de gouvernance et de gestion des données à caractère personnel doivent être pleinement conformes aux dispositions du RGPD, incluant le respect des principes de minimisation et de transparence quant à la finalité initiale de la collecte auprès du patient. Toutefois, l'AI Act, conscient des nécessités techniques de l'apprentissage automatique, introduit une dérogation exceptionnelle et ciblée à son article 10 paragraphe 5. Cette disposition autorise le traitement de catégories particulières de données à caractère personnel (telles que les données révélant l'origine ethnique ou les données concernant la santé) s'il est strictement et techniquement nécessaire à des fins exclusives de détection et de correction des biais algorithmiques, et ce, sous réserve de la mise en place de garanties de sécurité renforcées comme la pseudonymisation avancée ou le chiffrement de bout en bout.

Néanmoins, l'accès à des jeux de données de santé massifs, parfaitement représentatifs et de haute qualité, tels qu'exigés par l'AI Act, constituera sans aucun doute le principal goulot d'étranglement pour les développeurs d'IA en Europe. C'est précisément à ce stade qu'intervient le récent règlement (UE) 2025/327 relatif à l'Espace européen des données de santé (EEDS ou EHDS), une initiative législative phare souvent mise en exergue dans l'écosystème de la santé numérique.

Comme le soulignent avec pertinence les travaux de l'Action conjointe TEHDAS[177], l'EEDS a pour vocation de structurer et de fluidifier l'utilisation secondaire des données de santé à l'échelle continentale, en s'appuyant sur un réseau interconnecté d'Organismes responsables de l'accès aux données de santé (« HDAB »). En fournissant aux industriels et aux chercheurs un accès réglementé, sécurisé et standardisé à des données harmonisées issues des dossiers médicaux électroniques de toute l'Union, l'infrastructure de l'EEDS constituera le carburant vital permettant aux fabricants de satisfaire aux lourdes exigences de représentativité et d'absence d'erreurs de

[177] L'action conjoint TEDHAS (*Towards the European Health Data Space*) est une initiative européenne majeure visant à accompagner les Etats membres et la Commission européenne dans le développement et le partage transfrontalier des données de santé pour une utilisation secondaire, c'est-à-dire pour la recherche, l'innovation et l'élaboration de politiques de santé.

l'article 10 de l'AI Act. Cette interdépendance législative démontre que la robustesse des modèles d'IA européens dépendra intrinsèquement de l'opérationnalisation réussie de l'EEDS et du respect de l'éthique européenne de la donnée.

V. PRECISION, ROBUSTESSE, CYBERSECURITE ET L'INTERFACE AVEC L'EVALUATION CLINIQUE

A. La traduction de l'évaluation clinique en exigences algorithmiques quantifiables

Bien que l'AI Act n'utilise pas explicitement la nomenclature médicale classique d'« évaluation clinique » (propre au MDR) ou d'« évaluation des performances » (propre à l'IVDR), il n'en instaure pas moins des obligations de résultat strictes en matière d'exactitude, de robustesse algorithmique et de cybersécurité, qui se superposent et se confondent directement avec les objectifs de preuve clinique du MDR. Le guide MDCG 2025-6 clarifie ce point en indiquant que les critères de performance de l'AI Act doivent être interprétés et traités comme des composantes intégrales de l'évaluation clinique exigée par le cadre médical.

Sur le plan purement opérationnel, cela implique que le plan d'évaluation clinique ou le plan d'évaluation des performances du dispositif doit être significativement étendu. Il ne suffit plus de démontrer que le logiciel aide à diagnostiquer une pathologie ; le plan doit désormais intégrer les protocoles statistiques de validation des réseaux neuronaux, définir des seuils de tolérance scientifiquement justifiés pour les faux positifs et les faux négatifs, et inclure des analyses de sensibilité du modèle face à des données bruitées ou de qualité dégradée (robustesse). La démonstration de la performance algorithmique devient ainsi le prérequis indispensable à la démonstration du bénéfice clinique global.

B. Le croisement des investigations cliniques et des tests en conditions réelles

Une des zones de friction potentielles majeures entre les deux textes résidait dans les exigences de test *in vivo* avant la mise sur le marché. D'une part, le MDR impose la réalisation d'investigations cliniques pour valider l'efficacité et la sécurité d'un dispositif médical en conditions d'utilisation réelles. D'autre part, l'AI Act introduit un nouveau concept juridique : les « tests en conditions réelles » obligatoires pour les systèmes d'IA à haut risque avant leur commercialisation, tel que prévu par son article 60.

Le document d'orientation du MDCG apporte ici une clarification opérationnelle majeure qui soulagera considérablement les promoteurs d'études. Il affirme de manière catégorique que lorsqu'un MDAI fait l'objet d'une investigation clinique ou d'une étude de performance en vertu des dispositions du MDR ou de l'IVDR, ce processus rigoureux est juridiquement qualifié et formellement accepté comme équivalent à un test en conditions réelles au sens de l'AI Act.

L'AI Act prévoit en effet explicitement que de tels tests en conditions réelles sont autorisés « sans préjudice du droit de l'Union ou du droit national relatif aux essais en conditions réelles de systèmes d'IA à haut risque qui sont des dispositifs médicaux » (article 60). Cette équivalence conceptuelle prévient la nécessité absurde pour le fabricant de devoir soumettre deux protocoles d'expérimentation distincts à des comités d'éthique de la recherche ou à des autorités compétentes différentes. Elle garantit ainsi une continuité logique et temporelle dans le recueil des preuves cliniques et des performances algorithmiques.

C. La sécurité par la conception : la cybersécurité à l'ère de l'intelligence artificielle

La robustesse d'un système MDAI ne se limite pas à la précision de ses prédictions cliniques dans un environnement contrôlé ; elle englobe de manière indissociable sa résilience face aux perturbations extérieures et aux actes de malveillance. Si le MDR et l'IVDR imposent déjà des exigences générales de sécurité des systèmes d'information (complétées de longue date par les orientations spécifiques du MDCG 2019-16 sur la cybersécurité des dispositifs médicaux[178]), l'AI Act apporte une focalisation extrêmement ciblée sur les menaces structurelles inhérentes à l'architecture même de l'IA.

Les fabricants ont l'obligation de mettre en œuvre une démarche de cybersécurité dès la conception (*security by design*) qui soit spécifiquement capable de contrer les vecteurs d'attaque propres à l'apprentissage automatique. Le guide MDCG attend des fabricants qu'ils préviennent et documentent les parades contre des menaces telles que :

- l'empoisonnement du modèle (*Model poisoning*) : l'altération malveillante ou la corruption des données d'entraînement visant à introduire des failles ou à dégrader subrepticement la performance de l'algorithme diagnostique.
- les attaques adversariennes (*Adversarial attacks*) : la manipulation des prédictions de l'algorithme en phase d'inférence, par l'introduction de modifications infimes et souvent imperceptibles pour l'œil humain dans les données d'entrée (par exemple, l'ajout d'un bruit calculé sur une radiographie, conduisant l'IA à ignorer une tumeur).

Les dossiers techniques doivent démontrer de manière irréfutable que le modèle IA est capable de détecter ces anomalies de manière proactive au cours de son exploitation, ou *a minima* de conserver un comportement de sécurité résiduel contrôlé en cas de compromission avérée des données, afin de ne pas mettre en danger la vie du patient.

VI. TRANSPARENCE, EXPLICABILITE ET SURVEILLANCE HUMAINE : REPENSER L'ERGONOMIE DE LA DECISION MEDICALE

L'intégration de l'intelligence artificielle en pratique clinique quotidienne soulève un enjeu de confiance majeur de la part du corps médical, de plus en plus réticent face aux outils prescripteurs, et des patients. L'approche européenne postule fermement que la technologie, aussi avancée soit-elle, doit demeurer un outil d'assistance à la décision et non un oracle médical inviolable. Cette philosophie humaniste se traduit juridiquement par de lourdes obligations en matière de transparence (définies à l'article 13 de l'AI Act) et de contrôle humain (définies à l'article 14 de l'AI Act).

L'AI Act impose une obligation juridiquement contraignante aux développeurs : concevoir les MDAI à haut risque de manière à ce que leur fonctionnement global soit suffisamment transparent pour permettre aux « déployeurs » d'interpréter correctement les résultats générés et d'utiliser le système de manière pleinement appropriée. Cette notion de transparence va bien au-delà de la simple fourniture d'une notice d'utilisation classique conforme aux exigences générales de sécurité et de performance du MDR. La documentation fournie doit expliciter avec pédagogie les caractéristiques de performance, les capacités réelles de l'IA,

[178] MDCG 2019-16 Rev.1, *Guidance on Cybersecurity for medical devices*, July 2020.

mais surtout ses limites inhérentes et ses angles morts.

Le fonctionnement en « boîte noire » absolue est formellement proscrit dans les environnements de soins à haut risque. L'architecture du modèle doit intégrer, par conception, des niveaux d'explicabilité (*XAI - Explainable AI*) permettant aux médecins, qui restent les utilisateurs finaux de la donnée, de comprendre la logique sous-jacente ou les paramètres déterminants ayant conduit à une prédiction clinique donnée (par exemple, via des cartes de chaleur sur une image médicale identifiant les zones ayant focalisé l'attention de l'algorithme).

Corollaire de cette transparence, la surveillance humaine imposée par l'article 14 de l'AI Act exige que l'interface homme-machine soit ergonomiquement conçue pour permettre à une personne physique d'exercer un véritable contrôle critique sur la machine. Concrètement, le professionnel de santé doit disposer de l'autonomie et des moyens techniques nécessaires pour ignorer, outrepasser, ou annuler purement et simplement une recommandation de l'IA sans subir de contrainte technique ou de lourdeur applicative, assurant ainsi que la responsabilité de la décision médicale finale demeure incontestablement humaine. De plus, les systèmes d'IA conçus pour interagir directement avec des personnes physiques (tels que des agents conversationnels médicaux de triage ou des applications de thérapie comportementale) doivent être obligatoirement accompagnés d'une information claire, signifiant au patient qu'il interagit avec un système d'intelligence artificielle, à moins que cette nature algorithmique ne soit évidente compte tenu du contexte d'utilisation.

VII. ÉVOLUTION DU PRODUIT ALGORITHMIQUE : MODIFICATION SUBSTANTIELLE (AI ACT) VERSUS CHANGEMENT SIGNIFICATIF (MDR)

L'une des problématiques réglementaires les plus épineuses, abondamment débattue dans la littérature spécialisée et directement adressée par le MDCG, concerne le cycle de vie du logiciel après sa certification initiale. Les algorithmes d'IA, particulièrement ceux fondés sur des modèles d'apprentissage profond (*Deep Learning*) et d'apprentissage continu (*Continuous Learning*), ont pour vocation naturelle d'être réentraînés avec de nouvelles données et mis à jour fréquemment afin d'optimiser et d'affiner leurs performances diagnostiques ou prédictives au fil du temps.

Dans ce contexte évolutif, le MDR utilise le concept de « changement significatif » apporté à la conception ou à la finalité prévue, qui déclenche automatiquement la nécessité d'une nouvelle évaluation et d'une approbation par l'organisme notifié (conformément aux dispositions transitoires et aux procédures de l'annexe IX). Parallèlement et sur un plan sémantique très proche, l'AI Act introduit la notion de « modification substantielle ». Le risque systémique d'un désalignement conceptuel entre ces deux définitions est d'imposer aux fabricants des évaluations redondantes, longues et coûteuses pour la moindre mise à jour logicielle de routine ou d'amélioration mineure du modèle, tuant ainsi l'agilité inhérente et indispensable au développement de logiciels médicaux modernes.

Afin de résoudre cette quadrature du cercle réglementaire et de préserver la compétitivité de l'industrie, le guide MDCG 2025-6, en s'appuyant sur l'Annexe IV de l'AI Act, valide formellement l'utilisation et la pertinence des plans de contrôle des changements prédéterminés (*PCCP - Predetermined Change Control Plans*). Selon cette doctrine opérationnelle particulièrement attendue, si les modifications futures du MDAI (par exemple, des réentraînements planifiés de l'algorithme sur des jeux de données d'architecture similaire pour améliorer la

précision de 2%) ont été préalablement définies, minutieusement documentées, analysées en termes de risques résiduels, et surtout validées par l'organisme notifié lors du moment précis de l'évaluation initiale de la conformité, la situation change radicalement.

L'implémentation ultérieure de ces changements pré-approuvés et encadrés par l'enveloppe du PCCP, et qui figurent dans la documentation technique requise à l'annexe IV de l'AI Act, ne constitue pas une « modification substantielle » au sens juridique de l'AI Act, pas plus qu'un « changement significatif » au titre du MDR. Ce mécanisme d'anticipation réglementaire est le seul garant d'un cycle de vie logiciel viable sur le marché européen. L'industrie s'attend désormais à ce que des forums internationaux harmonisés, tels que l'International Medical Device Regulators Forum (« IMDRF ») abondamment cité dans les travaux sectoriels, publient très rapidement des orientations complémentaires plus détaillées afin de normaliser la rédaction et l'évaluation de ces précieux PCCP par les organismes notifiés.

VIII. SURVEILLANCE APRES COMMERCIALISATION ET GESTION DU RISQUE JURIDIQUE

Une fois le dispositif MDAI marqué CE et déployé au sein des infrastructures de santé sur le marché européen, la procédure de conformité ne s'arrête pas ; elle entre au contraire dans sa phase d'observation la plus critique et la plus exigeante. L'AI Act vient renforcer de manière drastique la portée, la profondeur et les capacités d'investigation du système de surveillance après commercialisation (*Post-Market Surveillance, « PMS »*) déjà imposé par le chapitre VII du MDR.

La surveillance algorithmique doit impérativement être proportionnée à la nature hautement dynamique et évolutive de l'IA. Pour les systèmes d'IA dits « apprenants en continu », qui adaptent dynamiquement leurs poids synaptiques ou leur comportement post-déploiement en fonction des nouvelles données cliniques traitées dans les établissements de santé, le PMS est élevé au rang d'instrument exclusif et central de sécurisation clinique.

Les fabricants ont l'obligation légale de mettre en place des canaux de télémétrie robustes et sécurisés permettant de rapatrier et d'analyser les données de journalisation issues des environnements d'exploitation des déployeurs. L'objectif est de détecter en temps quasi réel l'apparition de phénomènes délétères tels que la dérive de performance, les apparitions insidieuses de biais discriminatoires qui n'auraient pas été détectés lors des tests de représentativité initiaux, ou les failles de cybersécurité émergentes. Lorsqu'un risque systémique ou une anomalie clinique est identifié grâce à ce monitorage continu, des actions correctives de sécurité doivent être implémentées et communiquées de manière diligente et transparente à toutes les parties prenantes pertinentes, incluant les patients, les professionnels utilisateurs, les établissements déployeurs, ainsi que les autorités compétentes et les organismes notifiés.

Cet enchevêtrement complexe d'obligations de surveillance de la donnée trouve également un écho direct et menaçant dans l'évolution parallèle du droit de la responsabilité civile européen. Les dysfonctionnements d'un algorithme diagnostique ayant causé un retard de prise en charge, un préjudice corporel, ou la corruption du dossier médical d'un patient tomberont de plein droit sous le coup de la nouvelle directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux. La doctrine juridique a récemment et abondamment mis en exergue que cette refonte majeure inclut désormais expressément et sans équivoque les logiciels autonomes et les systèmes d'intelligence artificielle dans sa définition stricte du « produit ».

Plus fondamentalement, pour pallier l'asymétrie d'information structurelle dont

souffrent les victimes face à l'opacité des boîtes noires algorithmiques, la directive prévoit des mécanismes redoutables de présomption de défectuosité et d'inversion de la charge de la preuve. Dans ce contexte contentieux hautement inflammable, si un fabricant est assigné en justice et qu'il refuse ou s'avère incapable de fournir les données de journalisation (logs) exigées par l'AI Act pour expliquer le cheminement décisionnel de l'IA, le juge pourra présumer que le produit était défectueux au sens de la directive. Le maintien d'un PMS rigoureux, couplé aux obligations de transparence documentaire et de conservation des enregistrements exigées conjointement par l'AI Act et le MDR, ne constitue donc pas seulement une obligation de conformité administrative. Il représente le bouclier juridique primaire et indispensable du fabricant pour se défendre efficacement en cas de contentieux sériel sur la responsabilité des produits de santé numériques.

CONCLUSION : L'AVÈNEMENT DE LA CONFORMITÉ SYSTÉMIQUE PAR CONCEPTION

L'adoption conjointe et simultanée du règlement sur les dispositifs médicaux (MDR/IVDR) et de la loi sur l'intelligence artificielle (AI Act), orchestrée sur le plan purement opérationnel par les orientations pragmatiques du guide MDCG 2025-6, marque assurément une étape décisive dans la maturité de la réglementation européenne de la santé numérique. Le législateur européen a définitivement acté le fait que le logiciel médical n'est plus un simple automate déterministe prédictif. Il est désormais perçu, à juste titre, comme une entité évolutive, vulnérable aux biais de ses concepteurs, et potentiellement génératrice de risques systémiques dépassant largement le strict cadre de la sécurité clinique individuelle, pour empiéter sur le terrain des droits fondamentaux et de la sécurité des données.

L'étude du document MDCG 2025-6 révèle une ingénierie réglementaire exigeante mais qui tente sincèrement de rester pragmatique, dont la philosophie centrale repose sur l'intégration des obligations plutôt que sur leur superposition. En incitant fortement les fabricants à fusionner leurs systèmes de gestion de la qualité, leur documentation technique, leurs évaluations cliniques et leurs protocoles de contrôle des changements, le Groupe de coordination des dispositifs médicaux offre une voie de passage étroite mais praticable pour éviter la fragmentation administrative et l'asphyxie économique de l'industrie technologique européenne de la santé.

Cependant, cette simplification d'ordre formel et procédural ne saurait occulter l'élévation substantielle du niveau d'exigence technique et scientifique requis pour opérer sur ce marché. La gouvernance absolue et traçable des données d'entraînement, l'éradication proactive et documentée des biais discriminatoires, la résilience aux attaques sophistiquées de cybersécurité par la conception, ainsi que la garantie d'une interface suffisamment transparente pour permettre le maintien du libre arbitre et du jugement critique du médecin prescripteur, constituent désormais le socle minimal, non négociable, d'accès au marché intérieur européen.

Pour les fabricants de technologies médicales, le passage d'une culture historique de la certification ponctuelle d'un dispositif figé à une culture de la conformité algorithmique systémique et continue s'impose comme un impératif de survie. Dans ce processus de transformation industrielle, la synergie avec des dispositifs d'infrastructures majeurs, tels que l'Espace européen des données de santé, sera déterminante pour alimenter légalement ces algorithmes voraces en données de haute fiabilité et représentativité. À l'aube de l'application pleinement contraignante des dispositions de l'AI Act prévue en août 2027 pour les dispositifs médicaux, qu'ils soient hérités (et modifiés) ou de conception nouvelle, la capacité de l'industrie, des

hôpitaux déployeurs et des organismes notifiés à s'approprier collectivement les clés de lecture de ce guide MDCG conditionnera non seulement la compétitivité et l'agilité de l'innovation médicale européenne, mais garantira surtout le maintien d'une confiance inaltérable des professionnels de santé et des patients dans la médecine algorithmique de demain.

MDCG 2025-6 FAQ on Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), June 2025


Medical Device
Medical Device Coordination Group Document MDCG 2019-11 rev. 1

MDCG 2019-11 Rev.1
Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

October 2019
June 2025 rev.1

Lignes directrices relatives à la qualification et à la classification des logiciels dans le cadre du règlement (UE) 2017/745 et du règlement (UE) 2017/746. Analyse opérationnelle de la révision MDCG 2019-11 rev. 1

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

Le paysage réglementaire européen applicable aux technologies médicales traverse une période de mutation systémique, propulsée par une numérisation exponentielle des parcours de soins et par l'émergence d'outils algorithmiques d'une complexité inédite. Dans ce contexte de transformation où le droit tente d'épouser le rythme de l'innovation technologique, le Groupe de coordination en matière de dispositifs médicaux (« MDCG ») a publié, en juin 2025, la révision 1 de ses lignes directrices MDCG 2019-11[179].

Ce document, fondamental pour l'écosystème de la santé numérique, est expressément consacré à la qualification et à la classification des logiciels dispositifs médicaux (ci-après désignés par l'acronyme anglophone « MDSW », pour *Medical Device Software*) au titre du règlement (UE) 2017/745 relatif aux dispositifs médicaux (« MDR » acronyme anglais pour *medical device regulation*)[180] et du règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[181].

[179] MDCG 2019-11 rev.1, *Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746*, June 2025.

[180] 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, *JOUE* L. 117 du 5 mai 2017.

[181] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et

Publiée près de six ans après la version originelle d'octobre 2019, cette mise à jour réglementaire était particulièrement attendue par les fabricants, les éditeurs de logiciels, les organismes notifiés et les établissements de soins.

Si l'architecture globale et la philosophie du texte demeurent inchangées, cette révision introduit des clarifications sémantiques profondes et des précisions opérationnelles majeures qui traduisent une volonté ferme d'adaptation du droit de l'Union européenne aux réalités technologiques contemporaines. L'intégration explicite de l'intelligence artificielle au sein du périmètre de qualification, la prise en compte exigeante des architectures logicielles modulaires, l'attention inédite portée aux logiciels de prévention en vertu de la Règle 11 de classification, et l'articulation stratégique avec le nouveau règlement sur l'Espace européen des données de santé[182] (« EEDS ») constituent les axes cardinaux de cette évolution doctrinale.

L'analyse exhaustive de cette révision révèle un glissement paradigmatique : le passage d'une approche réglementaire historiquement centrée sur le support physique vers une régulation purement fonctionnelle, intrinsèque à la nature de la donnée et à l'action opérée sur celle-ci.
L'abandon définitif de la notion de « logiciel autonome » (*standalone software*) au profit d'une qualification fondée exclusivement sur la finalité médicale revendiquée par le fabricant en est l'illustration la plus éclatante.
La présente analyse propose un décryptage approfondi des nouveautés introduites par la révision de juin 2025 du guide MDCG 2019-11. Il s'agit d'examiner les implications pratiques, juridiques et opérationnelles pour les opérateurs de la santé numérique, en démontrant comment ces lignes directrices s'insèrent dans un corpus juridique européen de plus en plus dense, marqué par la convergence entre le droit des produits de santé, le droit des données et la régulation de l'intelligence artificielle.

I. L'ÉVOLUTION DU CHAMP D'APPLICATION ET LA REDÉFINITION CONCEPTUELLE DU LOGICIEL DISPOSITIF MÉDICAL

La première évolution notable de la révision de ce guide réside dans la clarification rigoureuse du champ d'application du document et la redéfinition des contours techniques et juridiques de ce qui constitue un logiciel dispositif médical. Le législateur européen et le MDCG actent ici la dématérialisation croissante des solutions de santé.

A. L'abandon de la notion de logiciel autonome au profit d'une approche fonctionnelle

Une clarification sémantique aux conséquences opérationnelles majeures est l'abandon explicite et définitif du terme « logiciel autonome » (*standalone software*), un concept hérité de l'ère des anciennes directives 93/42/CEE[183] et 98/79/CE[184]. La révision de juin 2025 consacre le principe directeur selon lequel un logiciel doit être qualifié et classifié en fonction de sa destination propre, de manière totalement indépendante de sa localisation physique, de son environnement d'exécution ou de son support d'hébergement.

abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE* L. 117 du 5 mai 2017.

[182] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* du 5 mars 2025.

[183] Directive 93/42/CEE du Conseil du 14 juin 1993 relative aux dispositifs médicaux, *JOCE* L. 169 du 12 juillet 1993.

[184] Directive 98/79/CE du Parlement européen et du Conseil du 27 octobre 1998 relative aux dispositifs médicaux de diagnostic in vitro, *JOCE* L. 331 du 7 décembre 1998.

Que le logiciel soit physiquement embarqué dans un dispositif matériel lourd comme un scanner IRM, qu'il opère sur un serveur distant via une architecture en nuage (*Cloud computing*), qu'il prenne la forme d'une application mobile téléchargée directement par un patient sur son smartphone, ou qu'il soit intégré en tant que micro-service au sein d'un vaste système d'information hospitalier, la méthode et la rigueur de la qualification demeurent strictement identiques.

Cette approche fonctionnelle oblige les fabricants à se concentrer exclusivement sur la nature de l'action effectuée sur les données. Selon les termes précis du guide, un logiciel est défini comme un ensemble d'instructions qui traite des données d'entrée pour créer des données de sortie. Si la création ou la modification de ces données de sortie est régie par une finalité médicale telle que définie à l'article 2, point 1, du MDR (diagnostic, prévention, suivi, prédiction, pronostic, traitement ou atténuation d'une maladie), le logiciel revêt irréfutablement la qualification de MDSW.

Cette dématérialisation de la pensée réglementaire permet de capturer efficacement l'ensemble des architectures modernes, et tout particulièrement les solutions en mode SaaS (*Software as a Service*), qui dominent aujourd'hui le marché de la santé numérique et échappaient parfois à une qualification aisée sous l'ancien paradigme.

B. L'intégration formelle de l'intelligence artificielle et l'articulation avec l'AI Act

Face à la prolifération exponentielle des algorithmes d'apprentissage automatique (*machine learning*), des réseaux de neurones profonds et des grands modèles de langage (*Large Language Models*) déployés en santé, le guide MDCG 2019-11 révisé inclut désormais explicitement l'Intelligence Artificielle Dispositif Médical (« MDAI » - *Medical Device Artificial Intelligence*) dans son champ d'application.

Cette reconnaissance formelle marque une étape cruciale dans la taxonomie réglementaire européenne, actant que l'IA n'est plus une technologie émergente périphérique mais une composante centrale des dispositifs médicaux logiciels.

La qualification d'un système d'IA en tant que MDSW obéit aux mêmes règles fondamentales que les logiciels algorithmiques traditionnels : elle dépend intrinsèquement de sa destination médicale. Toutefois, cette inclusion textuelle opère une jonction directe et complexe avec le règlement (UE) 2024/1689 sur l'intelligence artificielle (communément appelé AI Act)[185], entré en vigueur durant l'été 2024.

Les fabricants de MDAI se trouvent désormais confrontés à un défi d'ingénierie réglementaire sans précédent. Ils doivent concevoir leur stratégie de mise sur le marché de manière bicéphale, en satisfaisant simultanément aux exigences générales de sécurité et de performances de l'Annexe I du MDR ou du IVDR, et aux obligations strictes de transparence, de gouvernance des données, d'explicabilité et de contrôle humain imposées aux systèmes d'IA à haut risque par l'AI Act.

L'accent mis sur la MDAI reflète une préoccupation aiguë des autorités de régulation quant à la nature probabiliste, évolutive et parfois opaque de ces systèmes. Le guide souligne de manière implicite que le traitement de données d'entrée complexes, telles que des images radiologiques en haute résolution, des séquences génomiques ou des données textuelles non structurées issues de dossiers patients, dans le but de générer des

[185] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE* du 12 juillet 2024.

prédictions diagnostiques ou des recommandations thérapeutiques, constitue une action sur la donnée qui dépasse de très loin la simple recherche, l'archivage ou la compression sans perte (**page suivante**).

Une telle action qualifie irréfutablement ces outils d'IA de dispositifs médicaux.

Critère d'évaluation	Approche antérieure (Directives / MDCG initial)	Approche MDCG 2019-11 rev.1 (Juin 2025)	Impact Opérationnel pour l'industrie
Localisation du logiciel	Importance accordée au caractère « autonome » ou embarqué du logiciel.	Indifférence totale de la localisation (Cloud, mobile, serveur local, embarqué).	Obligation d'évaluer la fonction algorithmique pure, abstraction faite de l'infrastructure d'hébergement.
Nature de la technologie	Traitement uniforme des logiciels déterministes et des algorithmes complexes.	Inclusion explicite et traitement spécifique de la MDAI (Medical Device AI).	Nécessité d'aligner le dossier technique MDR avec les exigences de l'AI Act (explicabilité, gouvernance des données).
Action sur la donnée	Frontière parfois floue entre recherche simple et aide à la décision.	Distinction claire : l'altération de la représentation des données à des fins cliniques est un acte médical.	Les moteurs de recherche utilisant le traitement du langage naturel (NLP) pour influencer une décision clinique sont des MDSW.

C. La clarification réglementaire des produits de l'Annexe XVI sans finalité médicale

La section 3.1 du guide révisé a été substantiellement enrichie pour clarifier l'applicabilité des règles de qualification et de classification aux logiciels relatifs aux produits listés à l'Annexe XVI du Règlement (UE) 2017/745. Ces produits, bien que structurellement dépourvus de finalité médicale[186], sont soumis aux exigences de sécurité et de performance du MDR en raison de leur profil de risque physiologiquement similaire à celui des dispositifs médicaux traditionnels.

La révision du guide établit une distinction opérationnelle et juridique fondamentale pour les éditeurs de logiciels intervenant dans ce secteur particulièrement lucratif mais historiquement sous-réglementé.

Le texte distingue désormais deux scénarios distincts.

D'une part, si un logiciel est spécifiquement conçu et destiné à fournir des informations permettant de déterminer la finalité non médicale ou esthétique d'un produit de l'Annexe XVI, ce logiciel est lui-même qualifié de produit de l'Annexe XVI et se trouve soumis de plein droit au MDR. C'est typiquement le cas d'un algorithme de modélisation 3D avancée utilisé par un chirurgien plasticien pour prédire et visualiser les résultats d'une rhinoplastie ou pour aider un patient à sélectionner la taille et la forme spécifiques d'un implant mammaire esthétique.

D'autre part, si le logiciel se contente de piloter techniquement ou d'influencer directement les performances matérielles d'un équipement de l'Annexe XVI, sans fournir d'information ou d'aide à la décision quant à sa finalité esthétique, ce

[186] A l'instar des équipements de liposuccion esthétique, des lasers d'épilation à lumière pulsée, des équipements de stimulation cérébrale non médicale ou des implants de comblement dermique à visée purement esthétique.

logiciel n'est pas qualifié de produit de l'Annexe XVI de manière indépendante. Il est, en revanche, considéré comme une partie intégrante de cet équipement ou comme un accessoire de celui-ci, et suit par conséquent le régime d'évaluation de la conformité du matériel qu'il pilote.

Cette clarification sémantique est d'une importance capitale. Elle colmate les brèches juridiques potentielles pour les applications logicielles proliférant dans le secteur de l'esthétique et de la modification corporelle, obligeant les développeurs de ces outils de simulation ou de paramétrage à se soumettre à des évaluations cliniques (ou plutôt, dans ce contexte, à des évaluations démontrant la sécurité et l'absence de risque clinique inacceptable) rigoureuses avant toute mise sur le marché européen.

II. L'EXIGENCE ABSOLUE DE LA DESTINATION ET LA MAITRISE OPÉRATIONNELLE DE LA MODULARITÉ

Le cœur battant de la conformité réglementaire d'un dispositif médical, qu'il soit matériel ou logiciel, réside dans sa déclaration de destination (*intended purpose*). La révision du guide MDCG 2019-11 insiste de manière appuyée et répétée sur l'importance cruciale de la rédaction de cette destination, particulièrement dans le contexte des architectures logicielles complexes, interconnectées et modulaires.

A. La formulation de la destination médicale comme clé de voûte de la conformité

Le guide souligne qu'une formulation claire, exhaustive et sans ambiguïté de la destination est le prérequis absolu et non négociable pour une qualification et une classification correctes du logiciel. La destination, telle que définie conjointement par l'article 2, point 12, du MDR et de l'IVDR, englobe l'utilisation prévue selon les indications fournies par le fabricant sur l'étiquetage, dans les instructions d'utilisation, dans les documents promotionnels ou commerciaux, et de manière absolument cruciale, telles que spécifiées dans l'évaluation clinique pour les dispositifs médicaux ou dans l'évaluation des performances pour les dispositifs de diagnostic in vitro.

La nouveauté opérationnelle réside dans la mise en garde explicite formulée par le MDCG à l'attention des industriels : une destination ambiguë, excessivement large, générique ou mal définie peut inéluctablement conduire à une sur-classification pénalisante sur le plan commercial, ou pire, à une sous-classification erronée, entraînant des risques de non-conformité majeurs lors des audits menés par les organismes notifiés ou lors des inspections des autorités compétentes. Le fabricant a l'obligation impérieuse de s'assurer que chaque fonctionnalité du logiciel ayant une prétention ou un but médical est expressément couverte et justifiée par la déclaration de destination.

Concrètement, l'exigence imposée par l'article 7 du MDR et de l'IVDR rappelle que toute allégation relative à la finalité médicale prévue du MDSW doit être soutenue par un niveau de preuve clinique approprié et irréfutable. Si le département marketing d'un fabricant met en avant, sur le site internet du produit ou dans une brochure commerciale, une fonctionnalité offrant un bénéfice thérapeutique prédictif ou diagnostique, mais que cette fonctionnalité est absente de la destination officielle documentée et n'est pas corroborée par les données de l'évaluation clinique, le logiciel enfreint les exigences fondamentales des règlements. Dans une telle situation, le logiciel ne peut légalement être revêtu du marquage CE en tant que dispositif médical, et s'expose à des mesures de police sanitaire incluant le retrait immédiat du marché européen. Cette exigence impose un alignement total et permanent entre les équipes d'ingénierie, les affaires réglementaires, la direction

médicale et les services commerciaux de l'entreprise.

B. L'opérationnalisation rigoureuse des architectures modulaires (Section 7)

La tendance technologique lourde et irréversible en santé numérique est le développement de systèmes d'information hospitaliers (« SIH »), de dossiers patients informatisés (« « DPI) et de plateformes de santé vastes et multifonctionnels, où des fonctionnalités administratives (facturation, gestion des lits), logistiques et purement médicales (aide à la prescription, analyse d'images) cohabitent au sein d'un même environnement logiciel.

Pour faire face à cette complexité architecturale, la Section 7 du guide, consacrée aux modules, a fait l'objet d'une mise à jour et d'une élaboration conceptuelle substantielle.

Le guide entérine et précise la possibilité pour un fabricant de diviser un produit logiciel global en plusieurs modules distincts, certains étant qualifiés de MDSW en raison de leur finalité clinique, et d'autres non. Toutefois, cette approche de conception modulaire n'est pas une simple facilité administrative ; elle exige une rigueur architecturale absolue et une traçabilité sans faille.

Les nouvelles directives opérationnelles adressées aux fabricants concernant la modularité imposent un cadre strict :

1. L'indépendance de la conformité réglementaire : chaque module individuel qualifié de MDSW doit satisfaire de manière totalement indépendante aux exigences réglementaires de sécurité et de performance qui lui sont applicables, comme s'il s'agissait d'un dispositif autonome. L'évaluation clinique et la gestion des risques doivent être documentées pour chaque module médical de façon isolée.
2. L'alignement global du système : la fonctionnalité collective de l'ensemble des composants interconnectés - qu'ils soient médicaux ou non médicaux - doit s'aligner parfaitement sur la destination déclarée globale du système, sans introduire de contradictions opérationnelles, de failles de sécurité ou de risques inacceptables pour le patient ou l'utilisateur.
3. Des frontières architecturales imperméables : le fabricant doit fournir, dans sa documentation technique, une représentation architecturale d'une grande précision, délimitant visuellement et techniquement les frontières exactes entre les modules MDSW et les modules non-MDSW. Les interfaces (API, flux de données, protocoles d'échange) entre ces différents modules doivent faire l'objet d'une analyse de risque spécifique et exhaustive.
4. La gestion systémique des risques d'interface : une défaillance d'un module non-médical (par exemple, un module de gestion des identités provoquant une corruption de la base de données, ou un module de facturation saturant la mémoire du serveur) ne doit en aucun cas compromettre la sécurité, la disponibilité continue, ou l'intégrité clinique des données utilisées par le module médical (par exemple, un algorithme de calcul de dose d'insuline ou un outil d'aide à la décision thérapeutique). L'évaluation des risques, selon la norme ISO 14971, doit expressément et obligatoirement prendre en compte ces interactions inter-modules et démontrer la mise en place de mesures de mitigation efficaces.

Cette clarification détaillée sur la modularité offre une flexibilité stratégique précieuse aux éditeurs de logiciels de santé. Elle leur permet de circonscrire et de limiter

le périmètre fastidieux et coûteux du marquage CE aux seules fonctionnalités véritablement médicales, allégeant ainsi significativement le fardeau réglementaire de la maintenance des fonctionnalités administratives de leurs logiciels. Cependant, cet allègement n'est consenti qu'à la condition expresse que la ségrégation technique, documentée par le respect strict de normes telles que l'IEC 62304 sur le cycle de vie du logiciel[187], soit démontrée comme infaillible devant l'organisme notifié.

III. L'ÉVOLUTION DE LA CLASSIFICATION SOUS L'EMPIRE DE LA RÈGLE 11 : LE TOURNANT DE LA PRÉVENTION (SECTION 4.2.1)

L'un des apports conceptuels et opérationnels les plus déterminants de la révision de juin 2025 concerne la Règle 11 de l'Annexe VIII du MDR. Cette règle constitue, depuis l'entrée en application du règlement, la clef de voûte de la classification des logiciels médicaux en Europe.

Contrairement aux règles applicables au matériel physique, qui évaluent les risques liés au contact invasif ou à l'échange d'énergie, la Règle 11 a été spécifiquement conçue pour capturer les risques indirects inhérents aux logiciels. Le préjudice ne provient pas d'une défaillance mécanique, mais des conséquences délétères d'une information inexacte, incomplète ou erronée fournie par l'algorithme, conduisant le clinicien ou le patient à prendre une mauvaise décision de gestion médicale.

A. L'élargissement de la sous-règle 11a et l'intégration formelle de la « prévention »

La Règle 11 précise, dans sa construction tripartite, que les logiciels destinés à fournir des informations utilisées pour prendre des décisions à des fins diagnostiques ou thérapeutiques relèvent par défaut de la classe IIa. Des exceptions rehaussent cette classification si de telles décisions peuvent entraîner la mort ou une détérioration irréversible de l'état de santé (classe III), ou une détérioration grave de l'état de santé ou nécessiter une intervention chirurgicale majeure (classe IIb).

La nouveauté juridique majeure de la révision du guide réside dans l'ajout d'une clarification explicite concernant les dispositifs logiciels destinés à prévenir le risque de maladie au sein du périmètre d'application de cette sous-règle 11a.

Jusqu'à la publication de ce document révisé, une vaste zone grise réglementaire subsistait quant à la classification exacte des logiciels relevant de la médecine prédictive et préventive. De nombreux fabricants tentaient stratégiquement de classer des applications de prévention avancées (par exemple, des algorithmes prédisant le risque de survenue d'un diabète gestationnel, analysant des biomarqueurs pour anticiper un risque cardiovasculaire, ou évaluant des données génomiques pour déterminer une prédisposition oncologique) dans la catégorie résiduelle de la classe I (sous-règle 11c). Leur argumentaire reposait sur le fait que ces outils ne posaient pas de diagnostic clinique formel et ne proposaient pas de thérapie immédiate, échappant ainsi, selon eux, aux rigueurs de la sous-règle 11a.

La révision du guide MDCG coupe net à cette interprétation minimaliste. Le document précise désormais, sans

[187] La norme IEC 62304 est la norme internationale de référence qui définit les processus de cycle de vie du développement des logiciels de dispositifs médicaux. Son objectif principal est de minimiser les risques pour les patients en imposant une rigueur stricte dans la manière dont le logiciel est conçu, testé, publié et maintenu. Dans le cadre du marquage CE dispositif médical, démontrer la conformité à la norme IUEC 62304 est un moyen privilégié par les fabricants pour prouver aux autorités et aux organismes notifiés que le logiciel a été développé de manière sûre, traçable et contrôlée.

équivoque, qu'un dispositif logiciel destiné à prévenir le risque de maladies ou de pathologies en analysant des paramètres physiologiques (le guide cite expressément l'exemple de l'analyse du placement des vertèbres dorsales ou de la rigidité artérielle) doit être considéré comme fournissant des informations utilisées pour prendre des décisions à des fins de diagnostic, la prévention s'assimilant ici à la détection potentielle précoce de pathologies.

En conséquence directe, ces logiciels de prévention clinique relèvent *a minima* de la classe IIa, rendant obligatoire l'intervention d'un organisme notifié pour l'évaluation de leur conformité avant le marquage CE.

De plus, le guide rappelle que si l'information préventive s'avère erronée (faux négatif) et peut conduire à une inaction médicale entraînant *in fine* une détérioration grave de l'état de santé du patient (par exemple, un logiciel prédisant un risque nul d'infarctus chez un patient à très haut risque, conduisant à l'arrêt injustifié d'une surveillance cardiologique), la classification algorithmique doit logiquement être rehaussée en classe IIb, voire en classe III selon la sévérité du préjudice anticipé.

Sous-règle (Règle 11)	Domaine d'application clarifié (Juin 2025)	Impact sur la classification	Obligation d'Organisme Notifié
Sous-règle 11a	Décisions diagnostiques, thérapeutiques ET prévention du risque de maladie.	Classe IIa minimum (IIb ou III selon la gravité du préjudice potentiel).	OUI (Impact majeur pour les ex-Classe I de prévention).
Sous-règle 11b	Surveillance des processus physiologiques (et paramètres vitaux si danger immédiat).	Classe IIa (ou IIb si danger immédiat).	OUI
Sous-règle 11c	Toutes les autres finalités médicales mineures ne relevant pas du diagnostic, du traitement ou de la prévention clinique.	Classe I (catégorie devenue résiduelle et exceptionnelle)	NON (Autocertification possible, sous réserve d'absence de fonction de mesure).

B. La confirmation du cadre d'évaluation des risques de l'IMDRF

Le guide réaffirme avec force et renforce opérationnellement l'utilisation du cadre conceptuel élaboré par l'IMDRF (*International Medical Device Regulators Forum*) pour évaluer le risque inhérent aux logiciels médicaux. L'Annexe III du document MDCG fournit une matrice d'équivalence permettant d'aligner les catégories de risque de l'IMDRF avec les classes du MDR issues de la Règle 11.

Cette méthodologie d'évaluation impose au fabricant de croiser systématiquement deux variables fondamentales lors de la rédaction de son dossier de gestion des risques :

- L'importance de l'information fournie par le logiciel pour la décision de santé : le logiciel aide-t-il directement à traiter ou diagnostiquer (impact majeur) ? Concourt-il à diriger la gestion clinique (impact modéré) ? Ou sert-il simplement à éclairer et informer la gestion clinique (impact mineur) ?
- L'état de la situation de soins ou l'état du patient : la situation médicale est-elle critique (urgence vitale), sérieuse (maladie chronique grave) ou non grave ?

En clarifiant explicitement que la « prévention » est assimilée sur le plan réglementaire à une aide à la décision diagnostique, le MDCG harmonise la lecture de la Règle 11 à travers toute l'Europe. Cette doctrine empêche fermement le contournement réglementaire par l'usage d'allégations purement « préventives », de « suivi de style de vie » ou de « bien-être » lorsque la fonction intrinsèque et le mécanisme d'action de l'outil relèvent bel et bien d'une analyse clinique prédictive agissant sur le parcours de soin du patient.

IV. L'ÉMERGENCE DES THÉRAPEUTIQUES NUMÉRIQUES (DTX) ET L'EXEMPLE DE LA CLASSE I

Pour faciliter l'appropriation des règles de qualification et de classification, le MDCG a considérablement enrichi la section 3.2 du guide avec de nouveaux exemples concrets illustrant la frontière complexe entre les logiciels relevant du MDR et ceux qui en sont exclus.

A. Les logiciels destinés à « traiter » : la consécration des DTx (Section 3.2)

Une attention institutionnelle particulière a été accordée aux dispositifs thérapeutiques numériques (*Digital Therapeutics* ou « DTx »). Ces logiciels innovants ne se contentent plus d'observer, de surveiller une condition médicale ou d'aider un médecin à formuler un diagnostic ; ils visent activement et de manière autonome à traiter ou atténuer une maladie ou un trouble chez le patient.

Parmi les exemples novateurs introduits dans la version de juin 2025, on relève des cas d'usage reflétant l'état de l'art de la psychiatrie et de la neurologie numérique :

- traitement ciblé de la dyslexie : le guide cite un MDSW spécifiquement destiné à traiter les enfants atteints de dyslexie en améliorant l'analyse visio-orthographique des mots écrits. Le logiciel modifie activement et dynamiquement la présentation des éléments visuels à l'écran pour entraîner le cerveau de l'enfant à traiter simultanément un plus grand nombre d'éléments distincts lors de la fixation oculaire, accélérant ainsi la vitesse de reconnaissance des mots pendant la lecture. En opérant une action directe sur le processus cognitif et neurologique du patient à des fins thérapeutiques correctives, le logiciel se qualifie indéniablement de MDSW.
- aide au traitement de la schizophrénie : un autre exemple frappant concerne un MDSW permettant aux patients atteints de schizophrénie de suivre quotidiennement leurs symptômes et de recevoir des interventions médicales personnalisées basées sur leurs réponses à des évaluations. Le patient interagit avec divers modules thérapeutiques axés sur l'observance médicamenteuse, la régulation de l'humeur, le fonctionnement social, et surtout, la gestion active des hallucinations auditives. La fourniture d'interventions psycho-éducatives personnalisées et réactives dans le but exclusif de soulager ou de gérer les symptômes d'une pathologie psychiatrique lourde caractérise sans ambiguïté l'intention thérapeutique du logiciel.
- réalité virtuelle et réhabilitation neurologique : sont également formellement cités des logiciels recommandant des exercices de réadaptation musculo-squelettiques personnalisés pour soulager la douleur, ou des systèmes fonctionnant de concert avec des casques de réalité virtuelle immersifs pour traiter le syndrome complexe du membre fantôme chez

les personnes amputées. Dans ce dernier cas, le logiciel crée un avatar numérique simulant en temps réel les mouvements du membre manquant pour tromper le cortex cérébral et atténuer la douleur neuropathique.

Ces exemples illustrent la prise en compte mature par les régulateurs européens de la thérapie cognitivo-comportementale numérique et de la neuro-réhabilitation en tant qu'interventions médicales à part entière, soumises au même niveau d'exigence clinique qu'une molécule pharmacologique.

B. Le nouvel exemple de Classe I : Une catégorie devenue l'exception (Annexe IV)

Afin d'équilibrer l'élévation générale de la classification induite par l'interprétation stricte de la Règle 11, le MDCG a pris soin d'ajouter un nouvel exemple de logiciel relevant spécifiquement de la classe I dans l'Annexe IV du document.

Bien que le maintien de logiciels en classe I devienne exceptionnel sous l'empire du MDR, la doctrine réglementaire rappelle que cette classe d'autocertification reste réservée aux logiciels présentant un profil de risque absolument minime, dont les informations fournies n'influencent pas directement, ni de manière significative, une décision de diagnostic ou d'acte thérapeutique (relevant ainsi de la sous-règle 11c résiduelle).

L'ajout de cet exemple pratique vise à guider avec précision les fabricants de petites applications d'accompagnement (par exemple, de simples outils de saisie de journal de bord sans analyse prédictive, ou des logiciels de communication de base entre professionnels de santé n'altérant en rien la donnée médicale transmise) dans leur processus d'auto-certification. Cette précision est vitale pour éviter un engorgement inutile et préjudiciable des organismes notifiés, déjà sous forte tension capacitaire en Europe.

V. L'ARTICULATION STRATÉGIQUE ET JURIDIQUE AVEC L'ESPACE EUROPÉEN DES DONNÉES DE SANTE

L'une des mises à jour les plus structurantes de la révision figure à l'Annexe I, section c.1 du guide. Le document intègre désormais formellement les implications du nouveau règlement (UE) 2025/327 relatif à l'EEDS, un texte législatif majeur et entré en vigueur en un temps record. Cette actualisation minutieuse témoigne d'un changement de paradigme fondamental vers une réglementation de la santé davantage axée sur la donnée, sa portabilité et son interopérabilité.

A. Le défi réglementaire des dossiers médicaux électroniques

L'Annexe I c.1 aborde la question épineuse de la qualification et de la classification des systèmes d'information en santé, et plus spécifiquement des systèmes de dossiers médicaux électroniques (« DME », ou « EHR » pour *Electronic Health Record*).

Historiquement, sous les anciennes directives, les dossiers patients informatisés étaient majoritairement considérés comme de simples bases de données de stockage, d'archivage ou d'outils administratifs. À ce titre, ils échappaient généralement à la qualification de dispositif médical, la simple action d'archivage étant expressément exclue par l'étape 3 de l'arbre de décision de qualification du MDCG.

Toutefois, la réalité technologique a rattrapé le droit. Les DME modernes ne sont plus de passives bases de données ; ils intègrent de plus en plus des fonctionnalités actives d'aide à la décision clinique, des moteurs de règles générant des alertes d'interactions médicamenteuses en temps réel, ou des modules d'analyse de cohortes pour le suivi épidémiologique automatisé.
En outre, le règlement EEDS, dans son chapitre II, impose désormais de nouvelles

exigences drastiques de certification et d'autodéclaration de conformité (marquage CE spécifique EEDS) pour tous les systèmes de dossiers médicaux électroniques commercialisés sur le marché européen.

Le présent guide clarifie les frontières juridiques et techniques entre ces deux cadres réglementaires massifs - le MDR pour la sécurité clinique et l'EEDS pour l'interopérabilité des données - :

- **Interopérabilité et Cybersécurité** : l'accent est mis sur la capacité du logiciel médical à interagir de manière fluide et sécurisée avec le système de santé élargi. Les fabricants de MDSW qui revendiquent dans leurs spécifications une interopérabilité avec les systèmes DME doivent désormais démontrer leur conformité non seulement aux exigences du MDR (notamment en matière d'ingénierie logicielle et de validation clinique), mais également aux exigences applicables de l'EEDS.
- **Intégrité de la décision clinique** : le guide souligne avec insistance que l'interaction complexe entre un module MDSW (par exemple, un algorithme d'aide au diagnostic) et un dossier médical régi par l'EEDS ne doit compromettre en aucune circonstance l'intégrité des données de santé transitant sur le réseau, ni la cybersécurité du système global hospitalier, ni, in fine, la validité de la décision clinique prise par le praticien sur la base de ces données échangées.
- **Gouvernance de l'utilisation primaire des données** : l'EEDS vise à faciliter l'utilisation primaire des données (pour la continuité des soins transfrontaliers) par la standardisation des formats d'échange (comme le format européen d'échange de dossiers de santé électroniques - EEHRxF). Un fabricant de MDSW extrayant des données d'un DME pour alimenter son algorithme doit s'assurer de la qualité intrinsèque et sémantique de ces données d'entrée. Si le logiciel utilise des données corrompues, mal formatées ou incomplètes issues d'un registre EEDS pour générer une recommandation de traitement vitale, le risque d'erreur diagnostique doit être scrupuleusement anticipé et mitigé dans le dossier de gestion des risques du MDR.

L'intégration des préceptes de l'EEDS dans le guide MDCG oblige les éditeurs de logiciels médicaux à abandonner la logique des systèmes fermés pour adopter une posture de conception en « écosystème ouvert et sécurisé ». Un MDSW n'est plus évalué de manière isolée en laboratoire, mais en tant que nœud d'un vaste réseau européen de partage de données de santé, entraînant des responsabilités accrues en matière d'adoption de standards (ex. HL7 FHIR) et de cyber-résilience face aux menaces.

La révision 1 du guide MDCG 2019-11, publiée en juin 2025, ne se contente pas de procéder à un simple toilettage administratif d'un texte vieux de six ans ; elle acte de manière spectaculaire l'alignement définitif du cadre réglementaire européen sur la réalité technologique foisonnante du marché de la santé numérique.

Pour les fabricants de logiciels dispositifs médicaux, cette révision impose une analyse d'écart urgente et rigoureuse de l'ensemble de leur portefeuille de produits et de leur Système de Management de la Qualité (« SMQ »). Les implications opérationnelles jalonnent l'ensemble du cycle de vie du dispositif :

1. **Refonte de la stratégie réglementaire et de la destination** : l'intransigeance renforcée sur la règle 11, et tout particulièrement la requalification formelle de la « prévention » en acte

d'aide au diagnostic, témoigne de la primauté absolue accordée par le régulateur européen à la sécurité des patients face aux dérives possibles des allégations marketing. De nombreux logiciels de prévention, jusqu'alors confortablement installés en classe I, devront migrer vers la classe IIa, nécessitant la constitution de dossiers techniques complexes, des évaluations cliniques robustes en vie réelle (RWD) et l'intervention coûteuse d'organismes notifiés.

2. **Maîtrise de l'ingénierie modulaire** : l'élaboration détaillée sur la modularité (Section 7) offre une voie de passage pragmatique aux industriels développant des plateformes hospitalières complexes. Cependant, cette souplesse réglementaire est conditionnée à une excellence en matière d'ingénierie logicielle (IEC 62304) : la ségrégation technique entre les modules médicaux et non médicaux doit être documentée, auditée et prouvée comme étant infaillible.
3. **Mise en conformité croisée (MDR, AI Act, EEDS)** : en abandonnant la notion géographique de « logiciel autonome » au profit d'une analyse fonctionnelle centrée sur l'algorithme, en intégrant formellement l'intelligence artificielle (MDAI) dans son périmètre, et en tissant des liens réglementaires serrés avec l'AI Act et le règlement sur l'Espace européen des données de santé, le MDCG impose une vision holistique. Le fabricant ne répond plus seulement au MDR ; il devient un acteur de la donnée européenne, responsable de l'explicabilité de ses algorithmes et de la cybersécurité des flux d'informations transitant par les dossiers médicaux électroniques.

En définitive, pour l'écosystème de la santé numérique en Europe, ce guide révisé constitue une boussole incontournable. Il exige une maturité réglementaire transversale, où l'ingénierie informatique, l'expertise en cybersécurité, l'éthique de la gouvernance des données et l'évaluation clinique doivent fusionner dès l'idéation du produit. Si le fardeau de la preuve imposé à l'industrie est particulièrement lourd, il constitue la condition politique et juridique sine qua non pour asseoir la confiance absolue des professionnels de santé et des patients dans les technologies qui façonneront la médecine prédictive, préventive et personnalisée de demain.

Le défi du fabricant n'est plus seulement de concevoir un code informatique performant, mais de garantir son intégrité au sein d'un espace de santé européen devenu unifiant, complexe et hautement interconnecté.

MDCG 2019-11 rev.1 - Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

L'évaluation clinique commune des dispositifs médicaux à l'épreuve de la pratique

par Sarah BISTER

Avocate au Barreau de Paris
Docteure en Droit public, Université Toulouse Capitole

L'intégration européenne dans le domaine de la santé numérique et des technologies médicales franchit une nouvelle étape décisive avec l'adoption, le 17 octobre 2025, du règlement d'exécution (UE) 2025/2086 de la Commission européenne[188]. Ce texte, particulièrement attendu par l'écosystème de l'innovation médicale, établit les règles de procédure détaillées applicables à l'interaction au cours des évaluations cliniques communes (ci-après « ECC ») des dispositifs médicaux (« DM ») et des dispositifs médicaux de diagnostic in vitro (« DMDIV ») au niveau de l'Union européenne. Il s'inscrit dans le prolongement direct et opérationnel du règlement (UE) 2021/2282 concernant l'évaluation des technologies de la santé (ci-après « règlement ETS » ou « HTA Regulation »)[189], qui vise à harmoniser les méthodologies d'évaluation à l'échelle des Vingt-Sept.

Historiquement, l'évaluation des technologies de la santé au sein de l'Union européenne se caractérisait par une fragmentation institutionnelle et méthodologique préjudiciable. Les Etats membres opéraient selon des doctrines disparates, imposant aux développeurs de technologies de la santé (« DTS ») de soumettre de multiples dossiers cliniques pour accéder aux différents marchés nationaux. Cette duplication des efforts non seulement générait une charge administrative et financière considérable pour l'industrie, mais retardait également l'accès des patients aux innovations médicales cruciales. Si le règlement ETS est entré en application de manière échelonnée depuis le 12 janvier 2025 pour les médicaments contenant de nouvelles substances actives en oncologie et les thérapies innovantes, le présent règlement d'exécution 2025/2086 vient parachever l'édifice juridique permettant d'étendre ce mécanisme centralisé aux technologies médicales les plus innovantes et complexes.

La philosophie sous-jacente à ce nouveau cadre normatif est double. D'une part, il s'agit de garantir que les évaluations cliniques communes soient menées selon les standards scientifiques les plus rigoureux, en mutualisant l'expertise clinique et épidémiologique des Etats membres. D'autre part, il convient de préserver la souveraineté des Etats membres quant aux décisions relatives à la tarification, au remboursement et à l'organisation de leurs systèmes de soins, des prérogatives qui demeurent une compétence strictement nationale en vertu du principe de subsidiarité. L'évaluation clinique commune se limite ainsi à l'analyse de la sécurité, de l'efficacité et de la valeur clinique ajoutée, sans empiéter sur l'évaluation économique (coût-efficacité)

[188] Règlement d'exécution (UE) 2025/2086 de la Commission du 17 octobre 2025 établissant, conformément au règlement (UE) 2021/2282 concernant l'évaluation des technologies de la santé, les règles de procédure applicables à l'interaction au cours des évaluations cliniques communes de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro au niveau de l'Union, à l'échange d'informations concernant l'élaboration et la mise à jour de ces évaluations et à la participation à ces dernières, ainsi que des modèles pour ces évaluations cliniques communes, *JOUE* du 20 octobre 2025.

[189] Règlement (UE) 2021/2282 du Parlement européen et du Conseil du 15 décembre 2021 concernant l'évaluation des technologies de la santé et modifiant la directive 2011/24/UE, *JOUE* L. 458 du 22 décembre 2021.

qui reste l'apanage des agences nationales telles que la Haute Autorité de santé (HAS) en France ou le G-BA en Allemagne.

Le texte délimite avec une grande précision les obligations incombant aux développeurs, le rôle central du groupe de coordination des États membres, la fonction de secrétariat assurée par l'Agence européenne des médicaments (« EMA »), ainsi que la contribution indispensable des organismes notifiés et des experts individuels. L'analyse de ce règlement révèle une architecture procédurale sophistiquée, rythmée par des délais impératifs et structurée autour de modèles de dossiers standardisés.

Toutefois, la transition d'un système d'évaluation national à un modèle supranational soulève des défis opérationnels et stratégiques majeurs pour les fabricants de dispositifs médicaux. À l'aune des thématiques portées par le droit européen du numérique en santé, ce commentaire propose une analyse exhaustive et doctrinale du règlement d'exécution (UE) 2025/2086, en décryptant ses mécanismes juridiques, ses implications pratiques pour les industriels (notamment face à l'intégration de l'intelligence artificielle), et les garanties procédurales entourant la protection des données et le secret des affaires.

I. L'ARCHITECTURE DE LA SÉLECTION : CIBLER L'INNOVATION DE RUPTURE ET LE BESOIN MÉDICAL NON SATISFAIT

L'évaluation clinique commune n'a pas vocation à s'appliquer à l'exhaustivité des dispositifs médicaux mis sur le marché européen. Une telle approche engorgerait instantanément le système. Le mécanisme repose sur un processus de sélection rigoureux, visant à concentrer les ressources de l'Union sur les technologies présentant le plus fort potentiel d'impact sur la santé publique et l'organisation des soins.

A. Les critères d'éligibilité matérielle et la dimension numérique

Conformément à l'articulation entre le règlement ETS et le présent règlement d'exécution, le champ d'application matériel de l'évaluation clinique commune est circonscrit aux dispositifs médicaux à haut risque. Sont ainsi concernés les dispositifs médicaux relevant des classes IIb et III au sens du règlement (UE) 2017/745 (« MDR » acronyme anglais pour *medical device regulation*)[190], ainsi que les dispositifs médicaux de diagnostic in vitro de classe D au sens du règlement (UE) 2017/746 (« IVDR » acronyme anglais pour *in vitro diagnostic regulation*)[191]. Cette limitation aux classes de risque les plus élevées témoigne d'une volonté de proportionnalité dans l'action de l'Union.

Cependant, l'appartenance à ces classes de risque constitue une condition nécessaire mais non suffisante. La sélection s'opère *in fine* sur la base de critères cumulatifs ou alternatifs stricts, reflétant les priorités de santé publique et technologiques de l'Union. Les dispositifs retenus doivent répondre à l'un ou plusieurs des critères suivants :

- premièrement, la réponse à des besoins médicaux non satisfaits ou la qualification de premier de leur catégorie thérapeutique (« *first-in-class* ») ;
- deuxièmement, et c'est ici que le droit des dispositifs médicaux croise le droit du numérique en santé, l'intégration de logiciels fondés sur

[190] 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, *JOUE* L. 117 du 5 mai 2017.

[191] 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, *JOUE* L. 117 du 5 mai 2017.

l'intelligence artificielle (« IA »), les technologies d'apprentissage automatique (*machine learning*) ou des algorithmes complexes. Cette inclusion spécifique de l'IA démontre la prise de conscience par le législateur européen de la nécessité d'évaluer de manière rigoureuse et centralisée les dispositifs médicaux numériques (Software as a Medical Device - SaMD), dont les performances algorithmiques peuvent avoir des répercussions cliniques majeures ;

- troisièmement, la présence d'une dimension transfrontalière pertinente, une valeur ajoutée significative à l'échelle de l'Union, ou des implications majeures pour l'organisation des systèmes de soins et les patients.

B. Le rôle du groupe de coordination et la procédure de recommandation

L'article 7, paragraphe 4, du règlement (UE) 2021/2282 confie à la Commission la compétence d'adopter, au moins tous les deux ans, une décision d'exécution actant la sélection définitive des dispositifs soumis à l'évaluation clinique commune. Cette décision souveraine est toutefois organiquement conditionnée par une recommandation préalable du groupe de coordination des États membres sur l'évaluation des technologies de la santé.

Ce groupe de coordination ne statue pas de manière isolée ou arbitraire ; il fonde ses recommandations sur l'expertise technique des groupes d'experts désignés au titre de l'article 106, paragraphe 1, du règlement (UE) 2017/745[192]. L'EMA, agissant en qualité de secrétariat de l'ETS, joue ici un rôle de courroie de transmission central. Le règlement d'exécution 2024/2699 lui impose de fournir à la Commission les informations sur les avis scientifiques de ces groupes d'experts au plus tard 15 jours après la fin de chaque trimestre[193].

L'article 2 du règlement 2025/2086 institue une obligation d'information proactive. Dès l'adoption de la recommandation par le groupe de coordination, le secrétariat de l'ETS a l'obligation d'informer les développeurs de technologies de la santé quant à la sélection ou la non-sélection de leur dispositif. En cas de sélection, cette notification doit impérativement être assortie des raisons ayant conduit à cette recommandation. Cette exigence de motivation est fondamentale : elle garantit le respect du droit à une bonne administration et offre aux industriels la visibilité stratégique indispensable pour anticiper la préparation de leur dossier clinique complexe. À l'inverse, si un dispositif examiné n'est pas retenu, le développeur en est également

---

[192] Cet article précise : *« 1. La Commission, au moyen d'actes d'exécution et en concertation avec le GCDM, veille à ce que des groupes d'experts soient désignés pour évaluer l'évaluation clinique dans les différentes disciplines médicales, conformément au paragraphe 9 du présent article, et pour communiquer leurs points de vue sur l'évaluation des performances de certains dispositifs médicaux de diagnostic in vitro, conformément à l'article 48, paragraphe 6, du règlement (UE) 2017/746 et, au besoin, pour des catégories ou groupes de dispositifs, ou pour des dangers particuliers liés à des catégories ou groupes de dispositifs, dans le respect des principes des compétences scientifiques, de l'impartialité, de l'indépendance et de la transparence les plus élevées. Les mêmes principes s'appliquent lorsque la Commission décide de désigner des laboratoires spécialisés conformément au paragraphe 7 du présent article ».*

[193] Article 3, paragraphe 2 du règlement d'exécution (UE) 2024/2699 de la Commission du 18 octobre 2024 établissant, en application du règlement (UE) 2021/2282 du Parlement européen et du Conseil, les règles de procédure détaillées applicables à la coopération du groupe de coordination des États membres sur l'évaluation des technologies de la santé et la Commission avec l'Agence européenne des médicaments sous forme d'échange d'informations en ce qui concerne l'évaluation clinique commune des médicaments, des dispositifs médicaux et des dispositifs médicaux de diagnostic in vitro et en ce qui concerne la consultation scientifique commune sur les médicaments et les dispositifs médicaux, *JOUE du 21 octobre 2024.*

informé afin de préserver la sécurité juridique de ses opérations de mise sur le marché nationales.

II. LA SYNERGIE PROCÉDURALE : L'INTÉRACTION ENTRE LA CERTIFICATION ET L'ÉVALUATION

L'un des apports doctrinaux et opérationnels majeurs du règlement d'exécution 2025/2086 réside dans sa volonté d'arrimer la procédure d'évaluation clinique commune au calendrier de la certification de conformité (marquage CE), tout en préservant l'étanchéité et la stricte confidentialité de ce dernier processus. Ce séquençage est le point névralgique de la réforme, car il conditionne le délai d'accès au marché.

A. La gestion de la confidentialité et le lancement de l'évaluation

Le considérant 3 du règlement rappelle une contrainte juridique forte : la confidentialité inhérente au processus de certification par les organismes notifiés interdit à la Commission de lancer l'adoption de la décision de sélection avant l'achèvement complet dudit processus. La divulgation prématurée d'informations relatives à un dispositif en cours de certification constituerait une violation du secret des affaires et pourrait fausser le jeu de la concurrence.

Toutefois, le considérant 4 expose la nécessité d'un équilibre. Pour éviter que l'ECC n'accuse un retard qui serait in fine préjudiciable aux patients et à la compétitivité du marché européen, l'évaluation doit impérativement débuter dès que le certificat de conformité est formellement délivré au titre du MDR ou de l'IVDR. Ce lancement « en flux tendu » impose une coordination logistique et informationnelle inédite entre des acteurs jusqu'alors cloisonnés : les organismes notifiés, l'EMA (secrétariat de l'ETS) et les développeurs.

B. Les obligations de notification et le rôle pivot d'EUDAMED

L'article 4 du règlement d'exécution crée une obligation de communication en temps réel à la charge des organismes notifiés. Ces derniers doivent informer le secrétariat de l'ETS des résultats du processus de certification pour tout dispositif figurant dans la recommandation du groupe de coordination. Cette notification (octroi du certificat, refus, ou retrait de la demande) doit intervenir dans un délai extrêmement bref de sept jours.

En miroir, l'article 3 impose au développeur de technologies de la santé dont le dispositif a été recommandé de fournir au secrétariat de l'ETS le certificat de conformité et la notice d'utilisation certifiée, également dans un délai de sept jours suivant la délivrance ou la requête du secrétariat. De surcroît, le sous-groupe sur les évaluations cliniques communes (sous-groupe ECC) peut exiger du développeur des informations additionnelles jugées nécessaires pour la détermination du périmètre de l'évaluation.

Cependant, le législateur européen, conscient de la charge administrative pesant sur l'industrie – une préoccupation vivement relayée par MedTech Europe – a introduit un principe de *« dites-le-nous une fois »* (en anglais *once-only principle*). L'article 3, paragraphe 4, et l'article 4, paragraphe 3, mentionnent que les organismes notifiés et les DTS sont dispensés de cette transmission documentaire directe si les informations requises sont déjà dûment et pleinement accessibles dans la base de données européenne sur les dispositifs médicaux (« EUDAMED »), conformément aux articles 33 du MDR et 30 de l'IVDR.

Cette disposition consacre le rôle central d'EUDAMED comme clé de voûte de l'écosystème réglementaire européen de la santé. D'un point de vue pratique pour les fabricants, la maîtrise des composants de l'Identification Unique des Dispositifs (ou *unique device identification* -UDI) – tels que le Basic UDI-DI, l'UDI-DI et l'UDI-PI

– devient cruciale, car toute erreur de catégorisation ou de hiérarchisation dans EUDAMED pourrait bloquer la conformité et retarder le déclenchement de l'ECC. L'automatisation des transferts de données via des interfaces machine-to-machine vers EUDAMED apparaît ainsi comme un levier stratégique indispensable pour sécuriser ce flux d'informations critiques.

C. Le traitement des situations exceptionnelles

Le règlement anticipe l'éventualité de discordances politiques ou scientifiques entre la recommandation du groupe de coordination et la décision finale de la Commission. Lorsque la Commission décide, dans des cas particuliers justifiés (article 7, paragraphe 4 du règlement ETS), de sélectionner un dispositif médical qui n'avait pas été recommandé initialement, l'article 2, paragraphe 2, du règlement d'exécution entre en jeu. Le secrétariat de l'ETS notifie immédiatement le DTS de cette décision inopinée.

Le développeur est alors astreint aux mêmes obligations de transmission documentaire dans les sept jours, assurant ainsi qu'aucun dispositif d'intérêt public majeur n'échappe à l'évaluation clinique commune pour des raisons purement procédurales ou de désaccord institutionnel préalable.

III. LA DÉTERMINATION DU PÉRIMÈTRE DE L'ÉVALUATION : LA CRISTALLISATION DES BESOINS CLINIQUES EUROPÉENS

La phase de détermination du périmètre de l'évaluation (« *scoping* ») constitue le cœur stratégique et scientifique de l'ECC. Elle a pour objet de déterminer avec précision les questions de recherche auxquelles le rapport clinique final devra répondre, conditionnant ainsi l'utilité pratique du rapport pour les autorités nationales de remboursement. Si le périmètre est mal défini, l'évaluation risque de ne pas répondre aux exigences spécifiques d'un Etat membre, forçant ce dernier à exiger des évaluations nationales complémentaires, ce qui ruinerait l'objectif même du règlement.

A. La méthodologie PICO et l'élaboration de la proposition

Le règlement d'exécution 2025/2086 structure cette phase fondamentale autour de la méthodologie PICO (Population de patients, Intervention, Comparateurs, Résultats de santé ou Outcomes).

La procédure s'enclenche formellement à l'article 7 : dès que le sous-groupe ECC désigne un évaluateur et un coévaluateur parmi les experts des Etats membres, le secrétariat informe le développeur du début du processus. L'article 11 précise ensuite que l'évaluateur, assisté de son coévaluateur, est chargé d'élaborer une première « proposition de périmètre ».

La construction de ce cadre de référence s'appuie sur la notice d'utilisation certifiée transmise par le fabricant, mais également sur l'historique réglementaire du dispositif. En effet, l'évaluateur doit obligatoirement consulter le document final de consultation scientifique si le dispositif a fait l'objet d'une consultation scientifique commune préalable (JSC - *Joint Scientific Consultation*) au titre des articles 16 à 21 du règlement ETS. L'avis scientifique initial rendu par les groupes d'experts du MDR est également intégré à la réflexion.

La difficulté institutionnelle inhérente au processus de *scoping* européen réside dans la disparité historique des pratiques cliniques et des comparateurs exigés à travers les différents Etats membres. Afin d'atteindre l'objectif explicite du considérant 16 — à savoir traduire les besoins légitimes de tous les Etats membres par le *« plus petit nombre possible d'ensembles de paramètres de l'évaluation »* — la proposition initiale est partagée via la plateforme informatique de l'ETS avec l'ensemble des membres du sous-groupe ECC. Sur la base de leurs retours, une proposition consolidée est

établie, censée synthétiser l'exigence clinique européenne.

B. L'implication des experts et la finalisation du périmètre

Le processus de *scoping* intègre formellement la consultation d'experts indépendants pour ancrer l'évaluation dans la réalité clinique et le vécu des patients. L'article 11, paragraphe 3, impose au secrétariat de l'ETS de partager la proposition consolidée avec des experts cliniques et des représentants de patients préalablement sélectionnés, leur offrant la possibilité d'apporter des contributions substantielles.

L'article 12 encadre strictement la temporalité de cette phase. La finalisation du périmètre s'opère lors d'une réunion de consolidation du sous-groupe ECC. Le délai de rigueur est fixé à 60 jours maximum après la réception des informations post-certification, ou 10 jours après l'adoption de la décision de la Commission portant sélection du dispositif, l'échéance la plus tardive s'appliquant.

Afin de garantir le respect du principe du contradictoire et de clarifier les attentes méthodologiques, l'article 13 octroie une prérogative essentielle au développeur : ce dernier peut solliciter une « réunion d'explication du périmètre de l'évaluation » en présence du sous-groupe ECC. Cette réunion doit se tenir dans les 20 jours suivant la finalisation du périmètre.1 Sur le plan opérationnel, cette étape est vitale pour les équipes d'accès au du fabricant, car elle permet de dissiper les ambiguïtés sur les comparateurs exigés et de structurer l'analyse des données cliniques en conséquence.

IV. LE FARDEAU PROBATOIRE ET LES CONTRAINTES TEMPORELLES : LE DÉFI DU DOSSIER A 100 JOURS

Une fois le périmètre formellement figé, la charge de la preuve repose intégralement sur le développeur, qui doit démontrer la valeur clinique de son dispositif au regard des multiples paramètres PICO retenus. Cette étape cristallise les plus vives inquiétudes de l'industrie.

A. La règle couperet des 100 jours

L'article 14 du règlement d'exécution fixe un délai de 100 jours, courant à compter de la notification de la demande de la Commission, pour que le développeur soumette sous forme numérique le dossier complet de l'évaluation clinique.

Ce délai de 100 jours représente un défi opérationnel colossal. Dans la pratique, le périmètre PICO consolidé au niveau européen peut intégrer des sous-populations de patients ou des comparateurs (souvent des traitements médicamenteux ou des chirurgies alternatives) qui n'étaient pas les comparateurs primaires étudiés lors des essais cliniques originaux menés par le fabricant pour l'obtention de son marquage CE.

Le fabricant se trouve alors dans l'obligation de produire, en un peu plus de trois mois, de nouvelles synthèses de données.

Face à cette contrainte temporelle sévère, la réalisation de nouveaux essais cliniques est matériellement impossible. Les industriels devront impérativement s'appuyer sur des revues systématiques de la littérature de dernière minute, des méta-analyses en réseau et des comparaisons indirectes de traitements pour combler les vides probatoires entre leurs données cliniques et les exigences du PICO européen.

Les analystes du secteur anticipent que les entreprises, en particulier les PME dont les ressources réglementaires sont limitées, devront massivement recourir à l'intelligence artificielle générative et à des outils analytiques avancés pour simuler de multiples PICO, cartographier les preuves existantes et automatiser la rédaction des

trames documentaires dans les temps impartis[194].

Le législateur a toutefois prévu une soupape de sécurité, bien que minime. L'article 14, paragraphe 3, permet au secrétariat de l'ETS, avec l'accord des évaluateurs, de prolonger ce délai initial de 30 jours maximum dans des cas dument justifiés.

B. Les exigences formelles et le dialogue itératif

Le format du dossier n'est pas libre. L'annexe I du règlement 2025/2086 définit un modèle impératif extrêmement détaillé pour les dispositifs médicaux, aligné sur les principes stricts de la médecine factuelle. Le développeur doit documenter l'historique des révisions, fournir une synthèse des données probantes ventilées par paramètre PICO, justifier méthodologiquement tout écart par rapport aux orientations du groupe de coordination, et caractériser minutieusement l'état pathologique, la population visée, et le parcours de soins actuel en Europe. S'il omet des données pour un PICO spécifique, il a l'obligation d'en expliquer les raisons.

Le règlement organise ensuite un dialogue itératif, soumis à des délais drastiques, pour pallier les éventuelles lacunes du dossier soumis. A la suite de la soumission, la Commission dispose de 15 jours ouvrables pour confirmer si le dossier respecte les exigences formelles de l'article 9 du règlement ETS.

Si la Commission identifie des informations manquantes lors de cette vérification (la « deuxième demande »), l'article 14, paragraphe 4, n'octroie au développeur que 15 jours pour les fournir. Ce délai est même réduit à 7 jours si la Commission estime que seules des « informations mineures » font défaut. De plus, au cours de la phase d'évaluation elle-même, les évaluateurs peuvent exiger des clarifications ou des analyses supplémentaires (article 14, paragraphe 5). Le délai pour répondre est fixé par les évaluateurs eux-mêmes en fonction de la complexité de la demande, mais il ne peut être inférieur à 7 jours ni excéder 30 jours.

Ces fenêtres de tir d'une extrême brièveté exigent des industriels de maintenir des équipes d'experts cliniques et de statisticiens mobilisées et en alerte maximale tout au long de la procédure d'évaluation.

V. LA PHASE D'ÉVALUATION : L'ÉLABORATION DES RAPPORTS, LES GARANTIES DE TRANSPARENCE ET LA PROTECTION DU SECRET DES AFFAIRES

La traduction de l'évaluation clinique en un livrable opposable s'effectue par la rédaction du rapport d'évaluation clinique commune et de son rapport de synthèse. Cette phase confronte les impératifs de transparence publique aux exigences légitimes de protection des intérêts commerciaux.

A. La rédaction et les droits limités de l'industriel

L'article 16 encadre la rédaction des projets de rapports par l'évaluateur et le coévaluateur, en utilisant les modèles standardisés des annexes III, IV et V. Au cours de ce processus, l'avis des experts individuels (cliniciens et patients) est à nouveau sollicité, et les projets sont transmis au sous-groupe ECC pour recueil d'observations.

Le règlement octroie une garantie procédurale au développeur, mais en circonscrit strictement la portée. Conformément à l'article 16, paragraphe 4, le secrétariat de l'ETS transmet les projets

[194] Costello Medical, *Navigating the Challenges of Joint Clinical Assessment for Advanced Therapy Medicinal Products: Harmonising or Hampering HTA?*, https://www.costellomedical.com/what-we-do/value-and-access/challenges-for-advanced-therapy-medicinal-products/, dernier accès le 25 avril 2026.

révisés au développeur. Ce dernier ne dispose alors que de 7 jours pour réagir. Son intervention est cantonnée à deux actions exclusives :

1. Signaler les inexactitudes « purement techniques ou factuelles ».
2. Identifier les informations qu'il considère comme confidentielles, à charge pour lui de démontrer rigoureusement leur « caractère commercialement sensible ».

Il est fondamental de souligner que ce délai et ce cadre juridique interdisent au fabricant de contester le fond des conclusions scientifiques ou méthodologiques de l'évaluation à ce stade. La relecture est un simple contrôle de matérialité et de confidentialité.

B. L'intégration des données de vie réelle en cours d'évaluation

La nature des dispositifs médicaux implique une génération continue de données cliniques via les études de suivi clinique après commercialisation (SCAC ou en anglais PMCF). L'article 16, paragraphe 5, appréhende cette dynamique en prévoyant un mécanisme d'inclusion des données nouvelles survenant pendant l'évaluation.

Si le développeur soumet de nouvelles données cliniques de sa propre initiative, le sous-groupe ECC met « tout en œuvre » pour les prendre en considération. La contrainte devient absolue si ces nouvelles données parviennent au secrétariat au plus tard 60 jours après la confirmation par la Commission de la conformité formelle du dossier initial : dans ce cas, le sous-groupe a l'obligation d'intégrer ces données à son analyse. Cette disposition est favorable à l'industrie, lui permettant de consolider son dossier avec les résultats d'essais cliniques fraîchement publiés.

C. La finalisation temporelle des rapports

L'article 17 fixe la temporalité globale de la phase d'évaluation. Le sous-groupe ECC est tenu de finaliser les projets révisés dans les 165 jours suivant la confirmation de la recevabilité du dossier par la Commission. Une fois finalisés, ces documents sont transmis au groupe de coordination pour approbation formelle. En vertu de l'article 12, paragraphe 2, du règlement ETS, ce groupe dispose de 30 jours pour les endosser (**Page suivante**).

Le tableau ci-dessous résume les différentes phases d'évaluation et le calendrier qui y est associé :

Phase de la procédure d'ECC	Acteur responsable	Délai prescrit ou imparti
Finalisation du périmètre (*Scoping*)	Sous-groupe ECC	Max. 60 jours après réception des données post-certification
Soumission du dossier clinique	Développeur (DTS)	100 jours après la demande formelle (extensible de 30 jours)
Vérification de recevabilité	Commission européenne	15 jours ouvrables après la soumission du dossier
Intégration obligatoire de données nouvelles	Sous-groupe ECC	Données reçues max. 60 jours après la confirmation de recevabilité
Relecture pour confidentialité/erreurs	Développeur (DTS)	7 jours après réception des projets de rapports révisés
Finalisation des rapports	Sous-groupe ECC	165 jours après la confirmation de recevabilité du dossier
Approbation finale	Groupe de coordination	30 jours après réception des rapports finalisés.

De la soumission du dossier recevable jusqu'à l'approbation finale, la phase d'évaluation s'étend donc sur une durée maximale de 195 jours (165 + 30). Ce calendrier serré démontre la volonté de l'Union de ne pas entraver l'accès au marché, tout en exerçant une pression capacitaire immense sur les agences nationales d'évaluation. Pour soutenir cet effort massif, l'Agence exécutive européenne pour la santé et le numérique (« HaDEA ») a d'ailleurs signé en janvier 2025 un contrat-cadre de 35 millions d'euros avec un consortium de 21 pays européens (mené par l'INAMI-RIZIV belge) chargé de mener matériellement ces évaluations et consultations conjointes[195].

D. Le traitement des données : Secret des affaires et RGPD

La publication des rapports d'ECC et des rapports de synthèse constitue l'aboutissement de la procédure, assurant la transparence requise par le public et les professionnels de la santé. Cependant, le règlement encadre minutieusement cette divulgation pour protéger le secret des affaires. L'article 21 précise que la publication n'intervient qu'après examen par la Commission de l'avis du sous-groupe ECC concernant les requêtes de confidentialité formulées par le développeur.

Afin de prévenir tout contentieux, la Commission doit fournir au développeur, avant publication, la liste des informations qu'elle refuse de considérer comme confidentielles, en l'informant explicitement de son droit de former un recours administratif ou juridictionnel contre ce refus d'expurgation.

En matière de protection des données à caractère personnel (« RGPD »), l'article 22 désigne la Commission comme

[195] HaDEA, *From theory to practice: implementing the EU Health Technology Assessment Regulation*, 22 January 2025.

responsable du traitement. Il établit des règles strictes : l'identité et les données de santé des patients impliqués dans les ECC ne sont jamais publiées. Les données personnelles des experts et représentants sont conservées pour une durée n'excédant pas 15 ans après la cessation de leur participation (ou 3 ans s'ils n'ont pas été sélectionnés). Enfin, l'indépendance de l'expertise est garantie par l'obligation, pour chaque expert individuel, de signer un accord de confidentialité et de faire l'objet d'une évaluation rigoureuse de ses intérêts déclarés (conflits d'intérêts) par la Commission (article 8 et 9).

VI. L'ADAPTABILITÉ DU CADRE : LES MISES A JOUR DE L'ÉVALUATION ET L'ENJEU DE L'INTÉLLIGENCE ARTIFICIELLE

L'évaluation d'un dispositif médical n'est pas un acte statique, mais s'inscrit dans un continuum lié au cycle de vie du produit. Ce principe est particulièrement pertinent pour les dispositifs numériques intégrant des algorithmes d'intelligence artificielle adaptative (*machine learning*), dont les performances et l'impact clinique peuvent évoluer de manière significative après leur déploiement initial en vie réelle.

L'article 19 du règlement d'exécution 2025/2086 orchestre les modalités de mise à jour des évaluations cliniques communes. Une réévaluation peut être déclenchée selon deux voies distinctes. Soit elle était explicitement requise dans le rapport d'évaluation clinique initial (par exemple, dans l'attente des résultats finaux d'un registre de cohorte ou d'une étude à long terme), soit elle est sollicitée à l'initiative du développeur lui-même, qui transmet de nouvelles données probantes susceptibles d'améliorer son évaluation. Dans ce second scénario, le groupe de coordination dispose d'un pouvoir discrétionnaire pour inclure, ou non, cette mise à jour dans son programme de travail annuel.

D'un point de vue procédural, le sous-groupe ECC s'attache à désigner les mêmes évaluateurs et experts que lors de l'évaluation originelle, afin de capitaliser sur la connaissance préexistante du dossier. Une étape décisionnelle cruciale intervient alors : le sous-groupe doit statuer sur la nécessité, ou non, de modifier le périmètre de l'évaluation (le PICO). Si le périmètre clinique demeure inchangé, le processus de révision s'enclenche immédiatement sur la base du dossier mis à jour (délais de 165 jours pour les rapports). À l'inverse, si l'évolution des pratiques médicales ou des caractéristiques du dispositif justifie une mise à jour du périmètre, une nouvelle phase de *scoping* est ouverte, nécessitant la consultation des Etats membres (avec un délai de 60 jours pour finaliser ce nouveau périmètre). La finalisation des rapports actualisés s'étend alors jusqu'à 345 jours à compter de la décision de mise à jour par le groupe de coordination.

L'intégration de ce mécanisme de mise à jour est fondamentale pour l'industrie. Elle permet d'adapter l'évaluation des logiciels dispositifs médicaux (SaMD) qui, de par leur nature, font l'objet d'itérations fréquentes (mises à jour logicielles, amélioration des algorithmes d'IA) altérant potentiellement leur profil clinique.

Conclusion

Le règlement d'exécution (UE) 2025/2086 marque une rupture doctrinale et opérationnelle majeure dans l'appréhension de l'innovation médicale au sein de l'Union européenne. En substituant un processus d'évaluation clinique rationnel et centralisé à la myriade de procédures nationales, la Commission européenne entend positionner l'Europe comme un marché unifié et prévisible, capable de valoriser et d'absorber rapidement les thérapies les plus disruptives, à l'instar des dispositifs embarquant de l'intelligence artificielle.

La codification méticuleuse des délais procéduraux, des obligations de transparence institutionnelle et des droits de la défense accordés aux développeurs – notamment via le respect du contradictoire

et la protection des secrets d'affaires – démontre une volonté manifeste de sécuriser juridiquement le dispositif. Par ailleurs, l'arrimage de ce processus à l'infrastructure numérique de la base de données EUDAMED consacre l'interopérabilité des systèmes d'information réglementaires à l'échelle de l'Union.

Toutefois, l'efficience théorique de ce cadre réglementaire se heurtera inévitablement à l'épreuve de la réalité opérationnelle. Les réserves émises par les acteurs de l'industrie, notamment MedTech Europe, mettent en lumière le risque d'une charge administrative asymétrique. L'extrême rigidité des délais impartis aux développeurs (la règle des 100 jours), combinée à l'étendue potentielle et hétérogène des périmètres d'évaluation (PICO) générés par la synthèse des besoins de vingt-sept Etats membres, exigera un changement de paradigme stratégique profond au sein des entreprises. Le recours aux outils numériques d'analyse prédictive et à l'intelligence artificielle pour générer les preuves cliniques indirectes requises deviendra un impératif de survie, tout particulièrement pour les PME.

Il appartiendra aux premières évaluations cliniques communes de dispositifs médicaux, dont les prémices étaient prévues pour le premier trimestre 2026, de démontrer si ce nouvel édifice normatif parvient effectivement à concilier l'exigence de rigueur scientifique des autorités de santé avec l'agilité indispensable au déploiement de l'innovation médicale au bénéfice des patients européens.

Règlement d'exécution n° 2025/2086/UE du 17 octobre 2025 établissant, conformément au règlement n° 2021/2282/UE concernant l'évaluation des technologies de la santé, les règles de procédure applicables à l'interaction au cours des évaluations cliniques communes de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro au niveau de l'Union, à l'échange d'informations concernant l'élaboration et la mise à jour de ces évaluations et à la participation à ces dernières, ainsi que des modèles pour ces évaluations cliniques communes, *JOUE* n° L 2025/2086 du 20/10/2025.

COMPLÉMENT UTILE

HTA CG, Annual Work Programme 2025, 28 November 2025, document de programmation du *Health Technology Assessment Coordination Group* précisant les priorités de mise en œuvre du règlement (UE) 2021/2282 sur l'évaluation des technologies de santé, notamment en matière d'évaluations cliniques conjointes et de consultations scientifiques conjointes au niveau de l'Union européenne.

EUROPEAN RESPIRATORY SOCIETY

*Fondée en 1990, la European Respiratory Society (ERS) est la principale société savante européenne dédiée à la santé respiratoire. Basée à Lausanne, elle rassemble plus de 35 000 cliniciens, chercheurs, professionnels de santé et experts issus de plus de 160 pays. L'ERS contribue au développement des connaissances scientifiques dans le domaine des maladies respiratoires, soutient la recherche et la formation médicale continue, et élabore des recommandations cliniques destinées à harmoniser les pratiques et à améliorer la prise en charge des patients. Elle publie notamment plusieurs revues scientifiques de référence, dont l'*European Respiratory Journal (ERJ).

Marieke L. DUIVERMAN et *al.*, « European Respiratory Society Clinical Practice Guideline on Telemedicine in Home Mechanical Ventilation », *European Respiratory Journal*, 2025

La *European Respiratory Society (*ERS) a publié en 2025 ses premières lignes directrices consacrées à l'utilisation de la télémédecine dans le cadre de la ventilation mécanique à domicile. Ces recommandations s'inscrivent dans un contexte de développement des soins à distance pour les patients atteints d'insuffisance respiratoire chronique nécessitant une assistance ventilatoire prolongée.

Les auteurs soulignent que les outils de télésurveillance permettent un suivi continu des paramètres ventilatoires, une détection plus précoce des anomalies techniques ou cliniques et une adaptation plus réactive de la prise en charge. Les données disponibles suggèrent également un potentiel de réduction de certaines hospitalisations évitables ainsi qu'une amélioration de la coordination entre les équipes spécialisées et les patients suivis à domicile.

Les recommandations mettent toutefois en évidence l'hétérogénéité des preuves scientifiques actuellement disponibles et soulignent la nécessité de disposer d'infrastructures numériques adaptées, de garanties en matière de protection des données et d'une formation suffisante des professionnels de santé. Elles insistent également sur la poursuite des travaux de recherche afin de mieux documenter l'impact de ces dispositifs sur les résultats cliniques et l'organisation des soins.

Ces lignes directrices constituent une étape importante dans l'encadrement du recours à la télémédecine pour le suivi des patients sous ventilation mécanique à domicile et témoignent de la place croissante des outils numériques dans la prise en charge des pathologies respiratoires chroniques.

Droit français

Principes d'évaluation de la CNEDiMTS

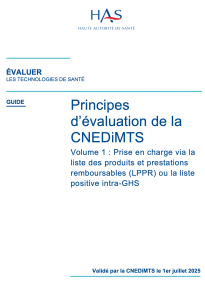
La Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) a publié une série de quatre volumes consacrés à l'évaluation des dispositifs médicaux numériques (DMN) en vue de leur prise en charge par l'Assurance maladie. Ces documents détaillent les critères d'évaluation et les niveaux de preuve attendus pour démontrer leur intérêt clinique.

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS (1er juillet 2025)

par Marie DESMEULES

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Le 1er juillet 2025, la commission spécialisée de la Haute Autorité de Santé (H.A.S.), dite Commission Nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS), a publié un guide actualisé sur ses principes d'évaluation, au sein duquel se recoupent quatre volets, dont le premier porte sur les demandes de prise en charge des dispositifs médicaux via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS (groupes homogènes de séjours).

Ce texte poursuit l'idée d'expliciter aux industriels, aux conseils nationaux professionnels de spécialités (CNP), ainsi qu'aux patients et usagers, les principes d'évaluation mis en œuvre par la commission dès que des dossiers lui sont soumis dans le cadre d'une demande d'inscription d'un dispositif médical pour une prise en charge via la LPPR ou la liste positive intra-GHS.

La notion de dispositif médical (D.M.) est précisée par le **règlement européen n° 2017/745/UE** comme « *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 précises* ». Leur prise en charge, et donc, leur remboursement par l'assurance maladie, dépend du résultat des évaluations effectuées par la CNEDiMTS, qui sera publié sous la forme d'un avis. Celui-ci répond notamment aux questions suivantes :

** Ce D.M., qu'il soit utilisé à l'hôpital ou en ville, doit-il être pris en charge par la solidarité nationale ?*

** Quelle est la valeur ajoutée du D.M. pour le patient, c'est-à-dire le progrès thérapeutique (au sens large) qu'il apporte par rapport aux thérapeutiques existantes ?*

** Quel est l'effectif de la population pour laquelle le remboursement est justifié et pour laquelle le D.M. représente une valeur ajoutée ?*
** Quel est l'impact de ce D.M. sur la santé publique ?*

Pour répondre à ces interrogations, une évaluation de la CNEDiMTS est réalisée. À titre liminaire, il est souligné qu'en complément des exigences posées par le marquage CE des dispositifs médicaux (qui est une procédure obligatoire attestant de la conformité du produit aux exigences de sécurité, de performance et de bénéfices cliniques), ceux-ci font l'objet d'évaluations complémentaires pour pouvoir être pris en charge. Elles se matérialisent sous deux formes :

1. les **modalités de financement** qui prennent en compte le secteur (ambulatoire, utilisation lors d'actes médicaux ou liée à un handicap) et le type de produit (ceux financés à travers des prestations intra GHS (ce qui équivaut aux prestations d'hospitalisation) ou hors GHS) ;
2. les **types d'inscription sur la LPPR**, dont deux modalités coexistent :
   - L'**inscription sous description générique** qui ne nécessite pas d'évaluation par la CNEDiMTS, mais dont le renouvellement d'inscription nécessite des évaluations périodiques.

Durée de l'inscription : 10 ans

   - L'**inscription sous nom de marque**, qui suppose une évaluation du bien-fondé de la demande, en veillant notamment au respect des conditions de forme tenant à la qualité du dossier et de son contenu.

Durée de l'inscription : 5 ans

De fait, le guide formalise les principes généraux applicables aux évaluations après demandes d'inscription sur la LPPR, et dont leur application est visible sur **deux étapes** :

- **Étape 1** : appréciation de la suffisance ou de l'insuffisance du service attendu ou rendu (SA/SR) par le D.M. afin de déterminer s'il peut être remboursé ou non. Cette appréciation se fait sur la base de deux critères cumulatifs (ou le cas échéant, sur des spécifications techniques et conditions particulières de prescription et d'utilisation) :
  - *l'intérêt du produit* : permet de mesurer l'apport du D.M. en fonction de son effet à l'échelle individuelle et du contexte physiopathologique et de la stratégie de prise en charge de référence du patient.
  - *l'intérêt de santé publique* : permet de mesurer l'apport du D.M. à l'échelle collective, et ce, au regard de divers facteurs tels que : l'épidémiologie de la pathologie (incidence et prévalence), l'impact des D.M. sur la santé publique (effets potentiels-prévisibles, adéquation avec les objectifs des programmes de santé publique), les populations cibles du D.M. susceptibles d'être prises en charge et d'être éligibles au remboursement.

Remarque : l'insuffisance est constatée si : efficacité faible, pas de pertinence clinique, non adéquation aux référentiels CNEDiMTS, association injustifiée de D.M. au sein d'un même conditionnement, etc.

Étape 2 : si le SA/SR est suffisant, alors l'appréciation portera ensuite sur le niveau d'amélioration de celui-ci (ASA/ASR), qui permettra la fixation du prix du D.M., ou plus largement, des seuls produits inscriptibles sur la liste LPPR. Cette évaluation se réalise par rapport à des actes ou prestations comparables précisément désignés et considérés comme une référence selon les données actuelles de la science (DAS). Autrement dit, il s'agit de mettre en évidence le bénéfice supplémentaire apporté par le nouveau produit par rapport aux traitements

thérapeutiques spécifiquement indiqués. La commission devra alors s'appuyer sur des données cliniques analysées selon les critères de la médecine fondée sur la preuve ; et choisir le comparateur convenable à l'étude, selon la stratégie de référence et les DAS. Ainsi, le niveau d'ASA/ASR pourra être déterminé sur la base des résultats cliniques ; éléments probatoires apportés par le demandeur d'inscription ; montrant la supériorité clinique du D.M. par rapport au comparateur. À l'issue de cette évaluation, la commission attribue, en raison d'une amélioration constatée (efficacité, réduction de risque, commodité d'emploi, qualité de vie, impact organisationnel, etc.), un niveau d'ASA/ASR (niveau I : amélioration majeure, niveau II : amélioration importante, niveau III : amélioration modérée, niveau IV : amélioration mineure). Sinon, à défaut d'éléments de preuve suffisants, la commission prononce l'absence d'ASA/ASR.

Dans le cadre de ces multiples évaluations, la CNEDiMTS peut avoir recours à une expertise extérieure pour un éclairage sur le contexte physiopathologique, sur la stratégie thérapeutique de référence et sur la pratique clinique, et ceci, formulé dans un rapport écrit. Elle peut également faire appel d'une part, au CNP pour une consultation alternative ou complémentaire à l'expertise extérieure, lequel se positionne en fonction des pratiques professionnelles et des recommandations ; et d'autre part, aux patients et usagers dont la participation est protéiforme : présence de membres associatifs choisis, audition, ou contribution spontanée d'association après le remplissage d'un questionnaire générique. L'implication de ces derniers offre une vision plus large de l'impact de la maladie, de l'état de santé, etc.

Remarques : la qualité de vie est un critère important pour la CNEDiMTS (notamment pour l'évaluation de l'ASA/ASR), complémentaire à celui de la morbi-mortalité, mais qui reste difficile à établir faute de données ou en raison de la faiblesse méthodologique du recueil de ce paramètre dans les études cliniques qui lui sont soumises. Ce critère peut être mesuré par le biais d'échelles validées (génériques ou spécifiques). De plus, sa pertinence dépend de la finalité du D.M.. Il peut donc aussi bien se présenter comme critère de jugement principal que comme critère de jugement secondaire, ce qui peut évoluer après avoir mené des études post-inscription. L'impact organisationnel d'une technologie de santé concerne ses effets cliniques, notamment sur la qualité de vie, avec des répercussions positives ou négatives, à l'échelle individuelle ou collective. Sa reconnaissance repose sur les incidences portées au processus de soins, aux compétences requises pour la mise en œuvre de ce dernier, à la société et à la collectivité. Tout comme le critère de la qualité de vie, son évaluation est limitée par le manque de données, la faiblesse méthodologique des études et le défaut de transposabilité au contexte national.

En outre, l'évaluation repose donc sur l'apport de preuves, toutes de nature variée (méthodes ou critères). Parmi elles se distinguent :

Les investigations cliniques, élément de preuve principal, adaptées aux revendications du demandeur. À défaut de pouvoir fournir de telles preuves, l'industriel devra justifier et argumenter cette impossibilité. Les attentes et exigences de la CNEDiMTS varient en fonction de la catégorie de D.M., de son cycle de vie, des possibilités de recrutement limitées.

Les critères de jugement :

*critère principal : son identification est proposée en conformité avec l'objectif principal de l'étude et son choix est cohérent avec la pathologie traitée et avec les revendications de l'industriel. Celui-ci peut avoir des objets de natures différentes.

*critères intermédiaires ou de substitution : présentent un intérêt lorsque le critère de l'étude clinique met du temps à être établi.

*critères centrés sur le patient : recueil direct de données cliniques prélevées auprès des patients (lesquels assurent ce recueil) via des outils spécifiques : les PROs et les PROMs.

La pertinence clinique de l'effet : c'est-à-dire une mise en balance entre l'effet

obtenu par le D.M. et le traitement de référence.

L'équivalence : cela suppose que le produit évalué doit être utilisé dans des indications et conditions similaires au produit dont l'industriel revendique l'équivalence.

Par ailleurs, il faut noter que l'évaluation revêt un certain particularisme en matière de D.M.C. (D.M. connectés : intègrent des fonctionnalités numériques, peuvent être connectés à un réseau et sont utilisés à des fins de diagnostic, thérapeutiques, de compensation du handicap ou de surveillance). La CNEDiMTS accepte leur inscription sur la LPPR si et seulement si les conditions suivantes sont remplies : dispositifs marqués CE, D.M. à usage individuel, candidats à un financement individualisé par l'assurance maladie, et D.M. ne faisant pas l'objet d'activités de télésurveillance médicale. En dehors de ceci, les critères d'évaluation demeurent identiques à ceux appliqués pour les autres produits faisant l'objet d'une évaluation. Toutefois, les résultats de l'évaluation peuvent être influencés par les spécificités technologiques et leurs impacts sur la santé des individus, sur l'accès aux soins ou encore sur la qualité de la prise en charge.

De manière générale, les demandes d'inscription doivent être en cohérence avec les revendications de l'industriel, et dans le cas des D.M.C., cela entre également en cohérence avec les demandes du fournisseur de la solution technologique. Il est d'ailleurs conseillé aux industriels d'anticiper l'établissement de leur stratégie, en matière d'indications, notamment pour le programme de développement clinique qui en découle, car cela renforce la cohérence du dossier médico-technique, et donc, de la demande. Pour ce faire, la H.A.S. propose un double accompagnement par le biais : de rendez-vous pré-dépôt, qui consistent à renseigner les industriels sur les aspects technico-réglementaires nécessaires à la constitution du dossier ; et de rencontres précoces, qui sont des entretiens visant à répondre aux interrogations des industriels relatives au développement clinique du produit de santé concerné ou à la réalisation d'une étude médico-économique, si une évaluation de l'efficience du produit est envisagée. Dans les deux situations, la CNEDiMTS est absente puisque ces entretiens sont optionnels, non liants, confidentiels et gratuits.De plus, aux termes de l'inscription (5 ans sur la LPPR), les demandes de renouvellement de celle-ci sont formulées par les industriels, à la suite de quoi la CNEDiMTS effectue son évaluation. Une évaluation qui peut aussi résulter de la propre initiative de la commission ou après demande des ministres chargés de la sécurité sociale et de la santé. Celle-ci repose sur la fourniture de nouveaux éléments, de nouvelles données cliniques, en raison de l'évolution du contexte médical. Un processus qui se distingue de la demande d'études post-inscription faite par l'autorité de contrôle afin de confirmer l'intérêt du D.M. pour le patient, en conditions réelles et à long terme, et de répondre éventuellement aux interrogations soulevées lors de la première évaluation

En définitive, ce guide consolide et clarifie les exigences posées par la CNEDiMTS au cours de son évaluation pour les demandes d'inscription sur la LPPR ou la liste positive intra GHS. Une évaluation qui se structure autour de la détermination de la suffisance ou de l'insuffisance du service attendu ou rendu par le dispositif médical, et puis de son amélioration, au regard de données cliniques prouvées et comparables. Il met en exergue l'importance de l'évaluation scientifique et médicale dans la détermination du remboursement des produits de santé, qui passe essentiellement par le bien-fondé du dossier médico-technique constitué par le demandeur, sur lequel pèse une charge probatoire significative.

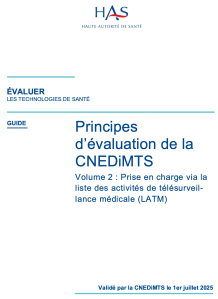
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 1 : Prise en charge via la liste des produits et prestations remboursables (LPPR) ou la liste positive intra-GHS*, 1er juillet 2025.

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM)

par Lukas MARA

Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



En juillet 2025, la Haute Autorité de santé a publié le volume 2 de ses principes d'évaluation de la CNEDiMTS, consacré aux modalités d'inscription des activités de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du Code de la sécurité sociale. Instituée par la loi de financement de la sécurité sociale pour 2022, cette liste constitue désormais le cadre de droit commun de la prise en charge par l'Assurance maladie. Le document rappelle d'emblée que la télésurveillance médicale n'est pas un simple outil numérique. Elle repose sur l'association d'un dispositif médical numérique (DMN) et d'une organisation de soins structurée, impliquant l'analyse des données transmises et l'adaptation de la prise en charge par les professionnels de santé. C'est donc une activité intégrée au parcours de soins qui est évaluée, et non seulement la performance technique du dispositif.

L'inscription sur la liste est subordonnée à un avis préalable de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS). Avant l'examen de l'intérêt de l'activité, plusieurs conditions doivent être remplies : le DMN doit bénéficier d'un marquage CE pour l'indication revendiquée, conformément au règlement (UE) 2017/745, et être conforme aux référentiels de sécurité et d'interopérabilité définis par l'Agence du numérique en santé (ANS). Ces prérequis garantissent la conformité technique du dispositif avant toute analyse médico-économique.

Ainsi, deux modalités d'inscription sont distinguées. La procédure sous ligne générique permet d'intégrer des solutions répondant à des critères prédéfinis, sans évaluation individuelle approfondie. À l'inverse, l'inscription sous nom de marque concerne une solution déterminée et donne lieu à une analyse spécifique par la CNEDiMTS, laquelle dispose d'un délai de 90 jours pour rendre son avis.

La démonstration de l'intérêt attendu constitue le point central de la procédure d'inscription.

Concrètement, la demande d'inscription doit toujours reposer sur une comparaison. Lorsque aucune activité de télésurveillance n'est encore remboursée pour l'indication visée, la référence est le suivi médical habituel. En revanche, si une activité est déjà prise en charge, la nouvelle activité doit démontrer qu'elle apporte un bénéfice au moins équivalent, voire supérieur. Le choix de ce comparateur est donc déterminant dans la construction du dossier.

L'intérêt attendu est apprécié selon trois axes principaux. La commission étudie d'abord l'amélioration clinique de l'état de santé du patient, en particulier la mortalité, la morbidité, la qualité de vie et les risques associés au dispositif. Des critères de jugement centrés sur le patient, comme les Patient Reported Outcome Measures (PROMs), peuvent être utilisés pour quantifier le bénéfice perçu. En second lieu, elle apprécie le gain significatif dans

l'organisation des soins, qu'il s'agisse d'économie de ressources, d'amélioration de la coordination ou de sécurisation du parcours, sans perte de chance pour le patient. Enfin, un intérêt de santé publique peut être reconnu lorsqu'il existe un besoin thérapeutique non satisfait ou un problème collectif identifié. Ces différents facteurs déterminent non seulement l'inscription sur la liste, mais aussi le montant du forfait de prise en charge.

Le guide identifie également plusieurs situations susceptibles de conduire à un avis défavorable. L'absence de données cliniques spécifiques constitue à cet égard un obstacle majeur. De plus, les recherches sur une autre technologie ne suffisent pas sans preuve rigoureuse d'équivalence, pas plus que des performances techniques isolées ne permettent d'établir un bénéfice pour la prise en charge. Par ailleurs, l'indication pour laquelle le remboursement est demandé doit être cohérente avec la population effectivement incluse dans les études cliniques. À défaut, la commission peut limiter son évaluation à la seule population étudiée.

Ainsi, l'inscription est accordée pour une durée maximale de 5 ans. Son renouvellement, loin d'être automatique, suppose la production de nouvelles données, notamment issues d'études post-inscription pour confirmer l'intérêt de l'activité en conditions réelles d'utilisation. Dans le même temps, la CNEDiMTS procède à une estimation de la population cible, sur la base de données épidémiologiques françaises, afin d'anticiper les volumes de prise en charge et d'éclairer l'impact budgétaire.

Enfin, le guide insiste sur l'articulation entre le cadre européen et la décision nationale de remboursement. Si le marquage CE permet la mise sur le marché au sein de l'Union européenne, il ne vaut pas reconnaissance automatique d'un droit à la prise en charge. À travers ses développements méthodologiques, la HAS rappelle que l'accès au remboursement repose sur une appréciation propre au système de santé français, fondée sur la démonstration d'un intérêt clinique, organisationnel ou de santé publique. Ce rappel est loin d'être théorique
: il invite les acteurs à penser, dès la phase de développement, la cohérence entre leur stratégie réglementaire européenne et les exigences spécifiques de l'évaluation nationale.

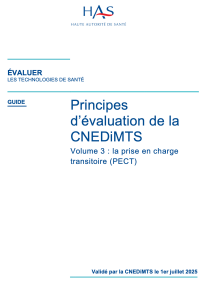
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 2 : Prise en charge via la liste des activités de télésurveillance médicale (LATM)*, 1er juillet 2025

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 3 : la prise en charge transitoire (PECT)

par Amina MOUSTOIFA

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Le 1er juillet 2025, la Haute Autorité de Santé (HAS) vulgarise dans un guide les principes d'évaluation de la Commission nationale d'évaluation des dispositifs médicaux et de technologies de santé (CNEDiMTS) dans le cadre d'une demande d'une prise en charge transitoire (PECT). La CNEDiMTS est une commission spécialisée de la HAS. Son rôle principal est de formuler des recommandations et de rendre des avis avec un regard scientifique sur les dispositifs médicaux.

Pour être tout à fait clair, le guide explique les méthodes d'évaluation de la CNEDiMTS lors d'un contrôle d'éligibilité d'une candidature pour une PECT. Ce

référentiel s'adresse principalement aux futurs porteurs de projets afin qu'ils saisissent les attentes de la CNEDiMTS et réduire les risques d'erreurs.

La PECT est mise en place par l'article 40 de la loi n° 2019-1446 du 24 décembre 2019. La prise en charge transitoire est, comme son nom l'indique, temporaire. Il s'agit d'un dispositif pour la prise en charge des produits de santé et de prestations associées ayant une finalité thérapeutique ou de compensation du handicap.

À ceci près que la PECT ne doit pas être confondue avec la prise en charge anticipée numérique (PECAN). La PECAN est une évaluation faite par la CNEDiMTS dans le périmètre des dispositifs médicaux numériques à visée thérapeutique ou utilisées en télésurveillance médicale. Donc, la PECAN relève d'une autre procédure à part entière distincte de l'évaluation au titre de la PECT. Toutefois, un dispositif médical intégrant une composante numérique peut recourir à la PECT lorsqu'il s'agit d'un logiciel ayant une fonction médicale, par exemple un implant. L'article L162-48 du code de la sécurité sociale pose deux conditions cumulatives à ce dispositif :

1- Le dispositif médical numérique doit avoir des fonctionnalités de télésurveillance médicale
2- Les fonctionnalités du dispositif médical numérique doivent se limiter à la télésurveillance numérique

Sous cet angle précis, le PECT peut intervenir dans le domaine du numérique au titre des dispositifs médicaux ayant une composante numérique.

L'objectif de la PECT est qu'à terme le produit de santé ou la prestation visée puisse intégrer la liste des produits et prestations remboursables (LPPR). Pour savoir quels produits et prestations sont éligibles à la PECT, il faut se référer aux décrets n°2021-204 du 23 février 2021 et n°2023-232 du 30 mars 2023.

La demande de PECT est conditionnée à 15 critères cumulatifs prévus aux articles R.165-90 et L.165-1-5 du code de la sécurité sociale. La demande est évaluée à la fois par le gouvernement et par la CNEDiMTS.

Le gouvernement est le premier à examiner la demande. Son contrôle s'apparente à une vérification formelle consistant à déterminer si la demande remplit 8 des 15 conditions prévues par le Code de la sécurité sociale.

Préalablement, lorsque les ministres en charge de la santé et de la sécurité sociale reçoivent une demande de PECT, ils se concertent avec le service d'évaluation des dispositifs (SED) de la HAS. Ce dernier travaille également avec la direction de la sécurité sociale. À proprement parler, il s'agit d'un filtrage préalable à l'évaluation des critères techniques par la CNEDiMTS.

À la réception du dossier, le SED et la direction de la sécurité sociale vérifient sa recevabilité administrative et scientifique. Dans l'hypothèse où le dossier n'est pas complet, le demandeur, après une notification, a 15 jours pour le compléter. S'il ne le fait pas, la demande est réputée abandonnée. Néanmoins, si le demandeur n'a pas la capacité de compléter son dossier dans le délai imparti, il peut retirer sa demande. Ainsi, ce retrait ne fera pas obstacle au dépôt ultérieur du même dossier.

Cela posé, le SED de la HAS et la direction de la sécurité sociale examinent ces 8 critères :

1- Le dispositif médical doit disposer du marquage CE ;
2- Le demandeur s'engage à réaliser une demande d'inscription à la LPPR dans un délai de 12 mois à compter de sa demande de PECT ;
3- Le demandeur s'engage à informer sans délai, par tout moyen, les ministres chargés de la santé et de la sécurité sociale de sa demande de prise en charge au titre de la LPPR ;
4- Le produit ou la prestation n'a pas déjà fait l'objet d'un refus de PECT ou d'une PECT à laquelle il a été mis fin

selon les cas prévus par II et III de l'article R.165-95 du Code de la sécurité sociale, qui sont :

- L'intervention d'une décision d'inscription ou de refus d'inscription à la LPPR
- Le retrait de la demande d'inscription à la LPPR par l'industriel
- Le retrait du marquage CE dans l'indication
- Les dispositifs médicaux qui relèvent d'une décision de l'Agence nationale de sécurité du médicament et des produits de santé au regard de l'article L.5312-1 du Code de la santé publique
- L'absence de dépôt d'une demande à la LPPR dans les 12 mois suivant sa demande de PECT
- Une condition d'éligibilité n'est plus remplie

5- Le dispositif médical a déjà été refusé au titre d'une demande de PECT par les ministres chargés de la santé et de la sécurité sociale dans la même indication. Autrement dit, une nouvelle demande du même produit ou de la même prestation pour la même indication n'est pas recevable ;

6- Le produit ne fait pas l'objet, dans l'indication considérée, d'une prise en charge financière au titre des prestations d'hospitalisation mentionnées à l'article L.162-22-6 du code de la sécurité sociale ;

7- Lorsque le produit ou la prestation intègre un dispositif médical numérique répondant à la définition mentionnée au premier alinéa du II de l'article L.162-48, ce dernier est conforme aux règles relatives à la protection des données personnelles ainsi qu'aux référentiels mentionnés à l'article L. 1470-5 du Code de la santé publique, comme expliqué plus tôt ;

8- Pour les dispositifs médicaux, le produit n'a pas fait l'objet d'une décision de suspension ou d'interdiction par l'Agence nationale de sécurité du médicament et des produits de santé (ANSM).

Partant de là, si la demande remplit toutes les conditions, l'industriel reçoit une notification favorable concernant sa demande de la part des ministères en charge de la santé et de la sécurité sociale.

Une fois l'étape préalable validée par les autorités ministérielles, la demande est confiée à la CNEDiMTS. Cette dernière dispose de 60 jours pour donner un avis favorable ou défavorable. La décision rendue par la Commission n'est pas attaquable et n'a pas de phase contradictoire. En effet, la décision finale revient aux ministres de la Santé et de la Sécurité sociale, qui ont 10 jours pour rendre une décision.

Durant ces 60 jours, la CNEDiMTS examine la demande de PECT au regard de ses principes. Dans ce guide, la HAS explique chacun de ces sept principes en collaboration avec la CNEDiMTS.

Tout d'abord, « le produit et la prestation sont destinés à traiter une maladie grave ou rare ou à compenser un handicap ». Pour ce critère, la Commission vérifie que le produit de santé ou la prestation associée vise bien, au choix :

- Une maladie grave
- Une maladie rare
- À compenser un handicap.

Au titre de la gravité et de la rareté de la maladie, elle retient plusieurs éléments d'appréciation. Sous l'angle précis de la gravité, la Commission s'appuie sur les facteurs de morbi-mortalité, de handicap, de complications et de risques. Tout comme pour la rareté de la maladie et la compensation d'un handicap, la Commission analyse les études cliniques, les données épidémiologiques ou encore à travers le calcul d'une population cible.

Ensuite, le produit de santé ou la prestation visée doit répondre à « un besoin médical non ou mal couvert ». Pour cela, il faut qu'il n'y ait pas de « comparateurs pertinents ». Entre autres pour évaluer cette condition, la CNEDiMTS passe en revue les alternatives existantes exposées dans la demande. L'objectif est de vérifier si ces alternatives sont pertinentes et/ou permettent de couvrir un besoin médical au regard des données actuelles de la science ou des recommandations professionnelles.

L'essentiel est que le porteur de projet expose clairement dans sa demande toutes les alternatives disponibles. Néanmoins, la Commission précise que l'existence d'alternatives pertinentes ne suffit pas à écarter la demande de PECT, puisqu'elle prend aussi en compte d'autres éléments comme l'offre de soins, la demande ou encore le rapport bénéfices et risques.

De plus, le produit de santé ou la prestation ne doit pas seulement « traiter une maladie grave ou rare ou à compenser un handicap », le dispositif doit également « apporter une amélioration significative de l'état de santé ou de la compensation du handicap des patients ».

Autrement dit, les indications considérées par l'industriel seront approfondies par le service de la Commission sur la base des données scientifiques transmises par le demandeur. L'analyse se fonde sur des critères d'inclusion, de présomption d'amélioration de la qualité de vie du patient ou l'optimisation de son parcours de soins.

De surcroît, le produit ou la prestation associée doit être innovant « au regard des technologies de santé utilisées dans les indications revendiquées ». En d'autres termes, le dispositif ne peut pas se limiter à une simple amélioration, l'innovation doit être caractérisée. Le guide donne l'exemple :

- D'un nouveau mode d'action modifiant la prise en charge d'une pathologie ou d'un handicap
- D'une réorganisation radicale du système d'information
- L'introduction d'une nouvelle technologie ou prestation dans une classe existante

La CNEDiMTS souligne l'importance de détailler les indications considérées dans la demande pour leur permettre de ne pas passer à côté du caractère innovant de certains produits pouvant porter à confusion.

Dans la continuité immédiate, le cinquième critère rejoint le troisième car il exige une efficacité cliniquement pertinente du produit ou de la prestation. À cela près que, cette cinquième condition approfondit son analyse en examinant les effets indésirables au regard de l'effet apporté par le dispositif. Ici, le bénéfice doit être important au regard des effets indésirables.

Au demeurant, pour apprécier les risques, la Commission s'attache à étudier toutes les données cliniques disponibles, le marquage CE fourni et les données de matériovigilance en France et à l'international par l'industriel. Le demandeur doit préciser le stade de développement du dispositif. La CNEDiMTS réalise également un contrôle in concreto en prenant en compte le contexte épidémiologique et physiopathologique.

La sixième condition rappelle l'importance de l'inscription à la LPPR. En effet, il faut que dans l'indication visée, des études déjà en cours et capables de fournir dans les 12 mois suivant la demande de PECT, des données suffisantes et robustes pour que la CNEDiMTS puisse rendre un avis favorable d'inscription à la LPPR. Plus précisément, ces études servent à lever les doutes laissés par les données préliminaires afin de permettre de se prononcer sur une présomption d'efficacité et de sécurité au moment de l'évaluation.

En ultime analyse, le septième critère précise le fait que la procédure de PECT ne s'adresse pas à tous les dispositifs médicaux. À ce titre, un dispositif médical

numérique ayant une visée thérapeutique ou étant utilisé dans le cadre des activités de télésurveillance médicale prévues à l'article L.162-48 du code de la sécurité sociale, fait l'objet d'une autre procédure à part entière, la prise en charge anticipée des dispositifs médicaux numériques dite PECAN. Cette procédure est également soumise au contrôle de la CNEDiMTS.

Dès lors, à l'issue de l'évaluation de la demande au regard de ses principes, la Commission rend un avis éligible ou un avis non éligible. Cet avis est transmis aux ministres en charge de la santé et de la sécurité sociale. Ces derniers disposent d'un délai de 10 jours pour faire droit ou non à la demande.

En cas d'octroi de la PECT par les ministres, le demandeur est notifié de la décision de ces derniers. Ensuite, il doit proposer un montant maximal de la compensation qu'il revendique au regard de son produit ou de la prestation associée dans un délai de 10 jours. Cela posé, lorsque les ministres accusent réception de la décision de l'industriel, ils ont 45 jours pour accueillir ou rejeter le montant proposé. Ils peuvent également faire une contre-offre. Dans ce cas de figure, le demandeur bénéficie de 10 jours, à compter de la notification de la décision des ministres, pour consentir ou s'opposer au montant révisé. Dans l'hypothèse d'un refus, la demande de la PECT est réputée abandonnée. Dans le cas d'une réponse positive, un arrêté est publié.

Pour conclure, la PECT permet l'accès transitoire à des dispositifs innovants et certains dispositifs médicaux comportant une composante numérique. Dans le champ du numérique en santé, la voie privilégiée pour les dispositifs médicaux numériques reste la PECAN, toutefois, la PECT conserve un champ propre. Partant de là, le guide de la Haute Autorité de Santé contribue à clarifier les critères d'éligibilité et les exigences d'évaluation. Il traduit, pour les porteurs de projets, la volonté de la CNEDiMTS d'encadrer l'innovation numérique par un cadre juridique et scientifique rigoureux.

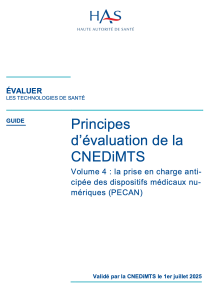
HAS, *Principes d'évaluation de la CNEDiMTS. Volume 3 : la prise en charge transitoire (PECT)*, 1er juillet 2025

GUIDE :

Principes d'évaluation de la CNEDiMTS
Volume 4 : la prise en charge anticipée des dispositifs médicaux numériques (PECAN)

par Mélanie SOUSA BARBEIRO

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Introduction

Le numérique occupe une place centrale dans le système de santé, et les dispositifs médicaux numériques (DMN), en particulier ceux intégrant de l'intelligence artificielle, connaissent un développement rapide. Pour accompagner ces innovations tout en garantissant un haut niveau d'exigence, le législateur a mis en place un dispositif d'accès précoce. Ce mécanisme permet la mise à disposition de technologies prometteuses avant l'achèvement complet de leur développement clinique, favorisant ainsi l'innovation tout en préservant la sécurité des patients.

Dans ce contexte, le document *« Principes d'évaluation de la CNEDiMTS (Volume 4) : Prise en charge anticipée (PECAN) »*, validé en juillet 2025 par la Haute Autorité de santé (HAS), présente les

critères et raisonnements utilisés par la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) pour formuler ses avis. En clair, il s'agit guide méthodologique ou d'une note de référence qui explicite les principes et critères d'évaluation de la CNEDiMTS pour les dispositifs médicaux numériques (DMN) dans le cadre de la prise en charge anticipée (PECAN).

Ce guide se concentre sur deux axes principaux : le cadre réglementaire de l'accès précoce et les critères d'éligibilité ainsi que les exigences méthodologiques applicables aux dispositifs médicaux numériques. L'idée est de comprendre les enjeux liés à l'évaluation anticipée et de clarifier les conditions dans lesquelles ces innovations peuvent être mises à disposition des patients.

I. ENCADREMENT JURIDIQUE ET PROCÉDURAL DE L'ACCÈS PRECOCE AUX DISPOSITIFS MÉDICAUX NUMÉRIQUES

Le document décrit d'abord les fondements juridiques et procéduraux de la PECAN **(A)**, avant de présenter la procédure d'évaluation structurée et transparente mise en place par la CNEDiMTS **(B)**.

A. Fondements légaux et cadre réglementaire de la prise en charge anticipée (PECAN)

Instaurée par l'article 58 de la loi de financement de la sécurité sociale pour 2022, la PECAN permet aux DMN d'accéder plus rapidement au remboursement, que ce soit pour un usage thérapeutique relevant de la LPPR ou pour des activités de télésurveillance relevant de la LATM. L'idée est d'offrir un accès anticipé à des innovations qui peuvent réellement apporter un bénéfice, sans sacrifier les standards scientifiques sur lesquels reposent les décisions de prise en charge. La CNEDiMTS intervient systématiquement pour éclairer ces décisions.

Le dispositif repose sur un équilibre précis : la prise en charge est temporaire, limitée à douze mois, et non renouvelable. L'entreprise doit ensuite déposer une demande d'inscription en droit commun dans un délai de six mois pour un produit destiné à la LPPR, ou de neuf mois pour un dispositif de télésurveillance. Certaines situations empêchent l'accès à la PECAN : il n'est ainsi pas possible d'obtenir deux prises en charge anticipées pour la même indication, ni de solliciter le dispositif en cas de suspension liée à un signalement de matériovigilance, ou lorsqu'un autre mode de financement est déjà mobilisé. Un nouveau dépôt n'est envisageable que si le précédent refus résulte exclusivement d'un manque de données en cours d'acquisition.

Par ailleurs, l'Agence du Numérique en Santé intervient lorsque la certification portant sur la protection des données personnelles, l'interopérabilité, la sécurité ou l'exportabilité est requise. Cette vérification, fondée sur l'article L.1470-5 du code de la santé publique, est cumulative à l'examen de la CNEDiMTS, notamment pour les DMN manipulant des données de santé ou connectés à des accessoires de collecte physiologique.

Ces bases juridiques et procédurales définissent le cadre, mais c'est la procédure d'évaluation qui garantit la rigueur scientifique et la transparence des décisions.

B. Organisation et déroulement de l'évaluation par la CNEDiMTS, garantissant rigueur et transparence

Le processus débute par le dépôt du dossier auprès des ministères, avec transmission simultanée à la CNEDiMTS. Une vérification de complétude est effectuée immédiatement : si des pièces manquent, le demandeur dispose de trente jours pour régulariser son dossier, sinon la demande est considérée comme abandonnée.

L'évaluation scientifique menée par la CNEDiMTS, sans phase contradictoire, doit aboutir à un avis dans un délai maximal de soixante jours. Les ministères disposent ensuite de trente jours supplémentaires pour arrêter la décision de prise en charge. Tous les avis sont publiés en ligne, favorables ou défavorables, afin de garantir lisibilité et transparence.

La CNEDiMTS peut faire appel à un expert externe, après validation de sa déclaration publique d'intérêts, pour compléter l'éclairage scientifique ou clinique. L'expert n'assiste ni à la délibération ni au vote, assurant une séparation claire entre expertise et décision. Les avis, même défavorables, sont conçus comme des outils d'amélioration : ils détaillent les points à renforcer et orientent les entreprises vers une stratégie plus solide, sans jamais remettre en cause l'intérêt intrinsèque du dispositif.

Avec ce cadre et cette procédure en place, l'attention se tourne maintenant vers les critères d'éligibilité et les exigences méthodologiques qui conditionnent l'accès des DMN à la PECAN.

II. CONDITIONS D'ÉLIGIBILITE ET EXIGENCES MÉTHODOLOGIQUES APPLICABLES AUX DISPOSITIFS MÉDICAUX NUMÉRIQUES

Le volume 4 des Principes d'évaluation de la CNEDiMTS précise les conditions d'éligibilité (A), puis les exigences méthodologiques (B) applicables aux dispositifs médicaux numériques, y compris pour les dispositifs intégrant de l'intelligence artificielle.

A. Les conditions d'accès nécessitant marquage CE, présomption d'innovation et cohérence du dossier

Plusieurs critères d'éligibilité sont applicables aux dispositifs médicaux numériques.

Le premier critère est la conformité du marquage CE, qui doit correspondre exactement à l'indication revendiquée. Toute discordance conduit automatiquement à un avis défavorable. Ce prérequis administratif est indispensable pour que la CNEDiMTS puisse examiner le dossier sur le plan scientifique.

Un autre critère est la présomption d'innovation. Cette dernière repose sur deux conditions. La première exige que le dispositif apporte un bénéfice clinique ou organisationnel, appuyé par des données initiales pertinentes : réduction des hospitalisations non programmées, amélioration de la qualité de vie, optimisation du parcours de soins, ou meilleure observance. Lorsque l'innovation concerne l'organisation, il faut démontrer qu'elle ne dégrade pas la qualité des soins, condition systématiquement vérifiée par la Commission.

La seconde condition concerne l'avancement des études : elles doivent être suffisamment avancées pour permettre une évaluation complète dans les six ou neuf mois suivant la décision PECAN. La méthodologie, la cohérence entre critères et bénéfices, le comparateur choisi, l'adéquation de la population et le réalisme du calendrier sont évalués. Les refus les plus fréquents concernent l'absence de données spécifiques, des protocoles peu solides, des critères inadaptés ou un désalignement entre l'étude et le dossier PECAN.

Enfin, le dossier doit être complet et structuré : description du DMN, mode d'action, estimation de la population cible, stratégie de référence, données de matériovigilance, premières preuves cliniques, protocoles finalisés, calendrier de résultats et pièces administratives. Si la PECAN accepte une part d'incertitude liée à l'innovation, elle n'admet pas l'insuffisance méthodologique ou des données imprécises.

Une fois ces conditions vérifiées, il reste à examiner la méthodologie et les exigences

spécifiques, particulièrement pour les DMN intégrant de l'intelligence artificielle.

B. Les exigences méthodologiques relatives aux DMN intégrant de l'intelligence artificielle

L'évaluation repose sur les guides méthodologiques de la HAS : développement clinique, DM connectés, études en vie réelle, évaluation organisationnelle et télésurveillance. L'objectif est d'isoler l'effet propre du dispositif, avec un comparateur pertinent, le contrôle des co-interventions, des critères liés aux bénéfices revendiqués et une population représentative. La transposabilité au système français est également importante, surtout pour des études internationales.

La distinction entre données spécifiques et non spécifiques se voit essentielle. Les données non spécifiques peuvent être utilisées si l'équivalence technique et fonctionnelle est démontrée, notamment pour des versions antérieures du DMN. À défaut, l'hétérogénéité ou l'absence de cohérence méthodologique entraîne souvent un refus, notamment pour des méta-analyses combinant des technologies trop différentes pour être extrapolées.

Pour les DMN intégrant un module d'intelligence artificielle, la documentation doit être particulièrement détaillée : modèle utilisé, données d'entraînement, méthodes de validation interne et externe, gestion des biais, mesures d'explicabilité, traçabilité des versions, performances attendues et stabilité en conditions réelles. Cette exigence vise à sécuriser l'usage clinique des algorithmes évolutifs et à garantir qu'ils n'affectent ni la pertinence des décisions médicales ni la sécurité des patients.

Conclusion

Le guide méthodologique de la CNEDiMTS relatif à la prise en charge anticipée des dispositifs médicaux numériques (PECAN) illustre l'équilibre délicat entre innovation et rigueur scientifique dans le système de santé français. En définissant clairement les fondements juridiques et procéduraux, la HAS offre un cadre structuré et transparent pour l'évaluation des DMN, tout en garantissant que les décisions reposent sur des données fiables et reproductibles.

Les critères d'éligibilité et les exigences méthodologiques détaillés dans le volume 4 permettent de sécuriser l'accès des innovations prometteuses, y compris celles intégrant de l'intelligence artificielle, tout en maintenant la sécurité et la qualité des soins. Ce dispositif d'accès précoce favorise ainsi l'adoption rapide de technologies utiles pour les patients, tout en fournissant aux entreprises un repère méthodologique précis pour renforcer la robustesse de leurs dossiers.

En définitive, la PECAN constitue un outil stratégique pour concilier innovation numérique, protection des patients et transparence dans la décision de prise en charge, renforçant la confiance des acteurs du système de santé et soutenant le développement responsable des DMN en France.

HAS, *Principes d'évaluation de la CNEDiMTS. Volume 4 : la prise en charge anticipée des dispositifs médicaux numériques (PECAN)*, 1er juillet 2025.

RÉFÉRENTIEL :

Harmonisation du bilan médicamenteux. **Recueil des besoins métiers en matière de bilan médicamenteux**

par Clarance JEAN-PIERRE

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole



Le référentiel d'harmonisation du bilan médicamenteux a été publié en juillet 2025 par la Haute Autorité de santé (HAS). Ce document fait suite à la saisine de la Délégation ministérielle au numérique en santé (DNS) et de la Direction générale de la santé (DGS). Il vise à définir un socle commun d'informations et de pratiques afin d'uniformiser la réalisation du bilan médicamenteux dans les différents secteurs de soins. Le document répond à un objectif de structuration des données et d'amélioration de leur partage entre professionnels de santé. Le référentiel indique que le bilan médicamenteux doit pouvoir être produit sous un format structuré compatible avec les systèmes d'information des professionnels de santé. Cette structuration est nécessaire pour permettre son dépôt dans le DMP. Le DMP est ainsi présenté comme un espace numérique destiné à recevoir et à rendre accessibles les informations issues du bilan, dans le cadre du parcours de soins du patient.

En outre, le référentiel définit un socle minimal d'informations devant figurer dans le bilan médicamenteux. Il comprend notamment l'identification du patient, la liste des traitements en cours, les éléments relatifs à l'observance, les informations issues de la conciliation médicamenteuse ainsi que les recommandations formulées par le professionnel. L'organisation de ces données sous une forme standardisée vise à garantir leur lisibilité et leur utilisation par d'autres professionnels de santé. Cette structuration conditionne également leur intégration correcte dans le DMP.

Par ailleurs, le document précise les exigences techniques nécessaires à cette intégration. En effet, le bilan médicamenteux doit pouvoir être exporté et transmis selon des formats compatibles avec les référentiels nationaux d'interopérabilité. Les logiciels métiers utilisés par les professionnels doivent être en mesure d'assurer le dépôt du document dans le DMP, dans des conditions conformes aux règles nationales applicables aux échanges de données de santé.

Le référentiel prévoit également des éléments assurant la traçabilité du bilan médicamenteux. Celui-ci doit mentionner la date de réalisation, l'identité du professionnel auteur ainsi que le contexte de production. Le bilan médicamenteux peut être mis à jour, et chaque version doit être clairement identifiée dans le DMP. Enfin, le texte rappelle que le dépôt et la consultation du bilan médicamenteux dans le DMP doivent respecter les règles applicables au DMP, notamment celles relatives à l'habilitation des professionnels et aux droits du patient en matière d'accès et de gestion de ses données de santé.

Ainsi, le référentiel organise non seulement le contenu du bilan médicamenteux, mais aussi les conditions de son intégration dans le DMP, en définissant les exigences de structuration, d'interopérabilité et de traçabilité nécessaires à son utilisation dans l'environnement numérique de santé.

HAS, *Harmonisation du bilan médicamenteux. Recueil des besoins métiers en matière de bilan médicamenteux,* 24 juillet 2025.

GUIDE :

Premières clefs d'usage de l'IA générative en santé

dans les secteurs sanitaire, social et médico-social

A.V.E.C : Avancer – **V**érifier – **E**stimer – **C**omprendre

par Maïlys CAPELL

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Éditorial

L'intelligence artificielle générative (IAG) en santé : un nouveau défi de responsabilité

En octobre 2025, la Haute Autorité de la Santé (HAS) a franchi une étape décisive dans l'encadrement des technologies numériques en publiant ses « Premières clefs d'usage de l'Intelligence Artificielle (IA) générative en santé ». Ce corpus documentaire, composé d'un guide pédagogique et d'un rapport d'élaboration approfondi, a été officiellement adopté comme Recommandations de Bonne Pratique (RBP) par le Collège de la HAS. Résultat d'une auto-saisine, ce travail a été piloté par la Mission numérique en santé (MNS), sous la conduite de Paul Valois, Julie Marc et Corinne Collignon. Ils ont produit une analyse critique de la littérature scientifique, mené des entretiens avec des experts de l'IA et ont consulté diverses associations de patients. L'objectif est clair : transformer ce qui n'est encore qu'un outil de curiosité en une pratique professionnelle sécurisée, éthique et juridiquement viable.

L'ensemble de ces travaux s'inscrit directement dans le cadre du projet stratégique 2025-2030 de la HAS, dont l'une des thématiques phares est le « Numérique et l'IA en santé ». En publiant ces RBP, la HAS ambitionne de construire un véritable cadre de confiance pour les usages de l'IA. L'enjeu est triple : accompagner les usages pertinents, améliorer les pratiques professionnelles et sécuriser le parcours de soin face à l'apparition des Large Language Models (LLM) dans les secteurs sanitaire, sociaux et médico- sociaux.

L'analyse de ces RBP doit être replacée dans un contexte légal européen en pleine effervescence. Si l'article 168 du TFUE fonde l'action de l'Union en complément des politiques nationales, l'IAG impose aujourd'hui un respect strict d'un corpus de normes complexe, produites à différents niveaux. Ces travaux de la HAS résonnent directement avec le Règlement (UE) 2024/1689 (IA Act) du 13 juin 2024, qui instaure une approche par les risques, et s'articulent avec les exigences de sécurité des Règlements (UE) 2017/745 et 2017/746 relatifs aux dispositifs médicaux. Ce cadre s'appuie également sur le Règlement (UE) 2025/327 relatif à l'Espace européen des données de santé et les garanties de l'article 22 du RGPD (complété par l'article 47 de la loi de 1978) pour encadrer les décisions individuelles automatisées. Enfin, la HAS s'appuie sur la Directive (UE) 2024/2853 sur la responsabilité du fait des produits défectueux pour protéger la liberté de décision des médecins. Face à des outils technologiques qui nous dépassent souvent, il est devenu indispensable de tenter de les maîtriser pour garantir, au final, la sécurité des patients

I. LA DISTINCTION ENTRE IAG « GRAND PUBLIC » ET IAG « MÉTIER »

Le rapport d'élaboration ne s'en cache pas : l'IA est déjà là. On observe un usage sauvage : des praticiens synthétisent des dossiers complexes ou rédigent des

comptes- rendus via des outils non sécurisés, souvent par nécessité, face à la surcharge administrative.

L'un des apports majeurs de l'argumentaire de la HAS est la distinction très nette entre les outils grand public (comme la version gratuite de ChatGPT) et les solutions dites « métier ».

Les IAG grand public sont des « boîtes noires » dont les processus d'entraînement sont opaques et dont les conditions d'utilisation permettent souvent la réutilisation des données communiquées par les utilisateurs pour améliorer le modèle. Pour la HAS, l'usage de ces outils en santé est hautement problématique : non seulement ils ne garantissent pas la confidentialité, mais ils sont sujets à un taux d'hallucination plus élevé. Contrairement aux outils professionnels qui s'appuient sur des bibliothèques de données scientifiques certifiées et des publications médicales relues par des experts, les IA grand public tirent leurs connaissances d'un mélange d'informations piochées partout sur le web. Elles n'ont pas été spécifiquement entraînées pour distinguer une information médicale fiable d'une rumeur ou d'une erreur trouvée sur un forum.

À l'inverse, l'IAG « métier » doit répondre à des exigences de documentation technique, de transparence algorithmique et bénéficier d'un marquage CE dispositif médical dès lors qu'elle intervient dans une finalité diagnostique ou thérapeutique. Le guide rappelle qu'un professionnel de santé ne devrait utiliser que des outils dont il peut identifier l'éditeur et en comprendre le périmètre de sécurité.

II. LA CERTIFICATION ET LE MARQUAGE CE : UN IMPÉRATIF DE SÉCURITE

Dans le secteur de la santé, l'innovation ne peut échapper aux règles de mise sur le marché. Le guide rappelle ainsi une distinction essentielle pour le professionnel de santé : l'outil est-il un simple assistant administratif ou un véritable Dispositif Médical ?

Dès lors qu'une IAG est utilisée dans une finalité médicale — qu'il s'agisse d'aide au diagnostic, de suggestion de traitement ou de surveillance de paramètres physiologiques — elle entre potentiellement dans le champ d'application du Règlement Européen 2017/745. Le marquage CE n'est pas un simple label de qualité, mais une attestation de conformité à des exigences de sécurité et de performance clinique.

Le rapport de la HAS est sans équivoque : si un professionnel utilise une IAG « grand public » dépourvue de marquage CE pour une décision de soin, il s'expose à un risque juridique majeur. En l'absence de certification, l'outil n'a pas été audité par un organisme notifié pour ses performances médicales. Utiliser une IA non certifiée pour interpréter des résultats de biologie ou pour établir un protocole thérapeutique revient, en droit, à utiliser un instrument non homologué.

Le guide engage donc les établissements de santé à une vigilance stricte :

a. **Vérifier la destination de l'outil :** L'éditeur revendique-t-il un usage médical ?

b. **Exiger la documentation technique :** Le professionnel doit avoir accès aux informations prouvant que l'outil a été testé sur des corpus de données cliniques pertinents.

c. **Refuser les « boîtes noires » non documentées :** Si l'éditeur ne garantit pas la traçabilité des sources et la gestion des risques d'erreurs, l'outil doit être cantonné à des tâches de secrétariat ou d'organisation administrative.

La HAS rappelle que le marquage CE est le garant de la « sécurité de résultat », même si la responsabilité finale de l'acte de soin reste humaine. C'est le point de jonction entre le droit des produits défectueux de santé et le droit de la responsabilité médicale.

III. L'ANALYSE JURIDIQUE DE LA MÉTHODE A.V.E.C.

Chaque pilier de la méthode redéfinit les contours de l'obligation de moyens renforcée du professionnel de santé.

a. APPRENDRE. La HAS insiste : on ne peut pas utiliser une IAG sans comprendre son fonctionnement. En droit européen, cela fait écho à l'AI Act qui impose une surveillance humaine. Ne pas se former aux limites de l'IA pourrait demain être qualifié de faute caractérisée en cas d'erreur de traitement.

b. VÉRIFIER. L'IAG peut halluciner, c'est-à-dire inventer des références bibliographiques ou encore des dosages médicamenteux. Le guide rappelle qu'un système d'IAG n'est pas un moteur de recherche. La HAS impose donc une relecture humaine systématique. Juridiquement, cela signifie que la preuve de l'erreur de l'IA ne sera jamais exonératoire d'une responsabilité médicale. La garantie humaine est le seul rempart qui assure que, derrière chaque ligne de code, existe une conscience capable de contredire la machine pour protéger le patient.

c. ESTIMER. Le rapport nous apprend qu'une simple requête consomme une quantité d'eau et d'électricité non négligeable pour refroidir les serveurs. La HAS demande donc aux soignants d'estimer si l'usage de l'IA est réellement nécessaire. Cette sobriété numérique se traduit par des conseils très concrets : supprimer les formules de politesse (bonjour, s'il te plaît) dans les échanges avec la machine afin de réduire la longueur du traitement algorithmique. Plus encore, elle alerte sur la perte de compétence : le risque est celui d'une dépendance cognitive où le praticien perdrait sa capacité d'analyse critique au profit d'une délégation totale à la machine. La recommandation de maintenir des séquences de travail « sans IA », et estimer quand l'IA est un réel gain de temps, est un cri d'alarme pour la préservation de l'intelligence humaine.

d. COMMUNIQUER. L'article L. 1111-4 du Code de la santé publique dispose que le patient doit recevoir une information loyale. La HAS va plus loin : si une IA a été utilisée pour aider au diagnostic ou à la rédaction du compte-rendu, le patient doit le savoir, et cela doit être mentionné dans son dossier médical, conformément à l'article L4001-3 du Code de Santé Publique.

IV. LE RISQUE DES BIAIS DISCRIMINATOIRES : UNE RESPONSABILITE EMERGENTE POUR LES PRATICIENS

Le rapport d'élaboration consacre une section essentielle aux biais algorithmiques. L'UE promeut des valeurs d'égalité et de non-discrimination. Cependant, les LLM sont entraînés sur des bases de données historiques qui reflètent les préjugés de notre société.

La HAS avertit : l'IAG peut reproduire, voire accentuer, des biais de genre, d'origine ou de classe sociale. Par exemple, une IA pourrait suggérer des protocoles de soins moins ambitieux pour certaines populations si les données d'entraînement sont déséquilibrées. Le guide impose donc au professionnel une posture de vigilance éthique. Il ne s'agit plus seulement de vérifier l'exactitude médicale d'une réponse, mais de s'assurer qu'elle ne contient pas une discrimination qui enfreindrait les principes fondamentaux du droit de la santé.

En publiant ces clefs d'usage, la HAS réalise une opération de transfert de responsabilité complexe. Si le guide sécurise les institutions, il place officiellement une charge de contrôle faramineuse sur les épaules du professionnel de santé.

On lui demande d'être, à la fois, médecin, informaticien capable de détecter des biais, et auditeur de conformité

réglementaire (avec la vérification du marquage CE). Est-il raisonnable de faire peser sur l'utilisateur final la responsabilité d'une « boîte noire » dont les mécanismes internes sont protégés, qui plus est, par le secret industriel ? Le guide prône la garantie humaine, mais cette garantie risque de devenir une fiction juridique si le professionnel n'a, ni le temps, ni les outils pour vérifier réellement les propositions de l'IA. Il existe un danger réel de voir apparaître une responsabilité sans faute, ou une obligation de sécurité de résultat déguisée, là où le médecin ne devait être tenu qu'à une obligation de moyens.

V. L'IMPACT SUR LES ÉTABLISSEMENTS SANITAIRES, SOCIAUX ET MÉDICO-SOCIAUX

Le déploiement de l'IAG n'est pas seulement un défi pour le praticien ; c'est un séisme organisationnel pour les Établissements Sanitaires, Sociaux et Médico-Sociaux. Le rapport d'élaboration de la HAS souligne que la mise en place de ces outils doit impérativement s'accompagner d'une réflexion institutionnelle profonde. On ne peut plus laisser l'usage de l'IAG au seul libre arbitre de l'agent.

L'un des points les plus sensibles du rapport d'élaboration concerne la protection des données de santé. En droit français, le secret médical est le socle de la confiance entre le soignant et le patient. La HAS est catégorique : il ne faut fournir aucune donnée identifiante (nom, prénom, NIR, date de naissance) dans une IAG non sécurisée. Le guide souligne que même une information partielle ou incomplète peut, par croisement de données, permettre une ré-identification. Le risque est double : d'une part, la violation du secret professionnel (sanctionnée pénalement) et, d'autre part, l'alimentation des bases de données des éditeurs par des cas cliniques réels, sans consentement des patients. La recommandation de la HAS de privilégier des environnements HDS (Hébergeur de Données de Santé) n'est donc pas une simple option technique, mais une condition de légalité. Pour garantir la sécurité des soins et la protection des données, la HAS préconise que le choix des outils soit centralisé au niveau de la gouvernance de l'établissement. La Direction des Systèmes d'Informations ne doit plus seulement être un support technique, mais un véritable garant de la conformité. C'est elle qui doit s'assurer que l'IAG utilisée est intégrée dans un environnement sécurisé, évitant ainsi l'usage d'outils personnels non autorisés qui expose l'établissement à des cyberattaques ou à des fuites de données massives.

En outre, l'intégration de l'IAG impose de repenser les processus de travail.

Le guide recommande aux établissements de définir des protocoles clairs : pour quelles tâches l'IA est-elle autorisée (rédaction de comptes-rendus, synthèse de littérature…) ? Le rapport précise que cette intégration doit faire l'objet d'un suivi via des indicateurs de performance et de qualité. En droit de la santé, cela renforce la responsabilité de l'établissement en cas de défaut d'organisation si aucun cadre n'a été fixé pour l'usage de ces technologies.

Enfin, la HAS insiste sur la nécessité d'un dialogue entre les directions, les représentants du personnel et les comités éthiques locaux. L'IAG modifie la valeur perçue du travail : si une tâche qui prenait deux heures est désormais réalisée en deux minutes, comment ce temps gagné est-il réalloué au bénéfice du patient ? La réussite organisationnelle réside dans la capacité de l'établissement à transformer ce gain de productivité en temps médical et soignant retrouvé, évitant ainsi que l'IA ne devienne un simple outil de rentabilité comptable au détriment de l'humanité des soins. Elle peut cependant absorber les tâches répétitives pour permettre au soignant de se concentrer sur l'essentiel : l'humain.

Conclusion

Le guide de la HAS d'octobre 2025 marque la fin de l'innocence numérique en matière d'utilisation de l'IA dans le milieu

sanitaire. Il ne s'agit plus de savoir si nous utiliserons l'IAG, mais plutôt de chercher comment tenter de rester maîtres de son usage. La HAS passe donc d'une posture de méfiance à une posture d'accompagnement. Elle ne cherche pas à interdire — ce qui serait illusoire — mais à normaliser. Ce passage vers le bon usage institutionnel implique que les établissements sanitaire, sociaux et médico- sociaux se saisissent de la gouvernance de ces outils. En effet, la responsabilité ne doit plus reposer uniquement sur l'utilisateur isolé, mais sur une stratégie collective de déploiement, qui pourrait passer notamment par la désignation d'un référent IA dans les établissements.

HAS, *Première clefs d'usage de l'IA générative en santé, dans les secteurs sanitaire, social et médico-social. A.V.E.C : Avance – Vérifier – Estimer – Communiquer*, 23 octobre 2025.

*La transformation numérique des établissements de santé se poursuit en 2026 à travers **deux initiatives majeures** : le lancement de la deuxième phase du programme HOP'EN (HOP'EN2) et le déploiement du programme HospiConnect, destiné à renforcer la sécurisation des accès aux systèmes d'information hospitaliers.*

Instruction n° DNS/2025/180 du 29 décembre 2025 relative au lancement de la deuxième phase du programme HOP'EN 2 pour soutenir la transformation numérique des établissements de santé, *BO* du 12/01/2026

Par une instruction du 29 décembre 2025, la Délégation au numérique en santé (DNS) a lancé la deuxième phase du programme HOP'EN (Hôpital numérique ouvert sur son environnement), destinée à poursuivre la transformation numérique des établissements de santé. Cette nouvelle étape vise à accompagner la montée en maturité des systèmes d'information hospitaliers, en favorisant notamment le déploiement de services numériques interopérables, le partage sécurisé des données de santé et la fluidification des parcours de soins**.** Le programme s'inscrit dans la continuité des actions engagées depuis 2019 pour moderniser les infrastructures numériques hospitalières et renforcer l'intégration des établissements dans l'écosystème numérique en santé.

Arrêté du 27 janvier 2026 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé – HospiConnect, *JORF* n° 0024 du 29 janvier 2026

L'arrêté du 27 janvier 2026 instaure le programme HospiConnect, un dispositif de financement destiné à renforcer la sécurité numérique des établissements de santé. Inscrit dans le cadre du programme CARE (Cybersécurité Accélération et Résilience des Établissements) et complémentaire du programme HOP'EN 2, il vise notamment à soutenir le déploiement de moyens d'identification électronique conformes au référentiel national d'identification électronique, afin de sécuriser l'accès aux systèmes d'information hospitaliers et aux données de santé. Le programme accompagne plus largement le développement de mécanismes d'authentification forte, de gestion des identités et des accès numériques, dans un contexte de renforcement des exigences de cybersécurité et de protection des données au sein du secteur hospitalier.

REPÈRES

Jusqu'en 2022, la télésurveillance médicale était principalement financée dans le cadre de l'expérimentation **ETAPES** (Expérimentations de télémédecine pour l'amélioration des parcours en santé). La loi de financement de la sécurité sociale (**LFSS**) pour 2022 a instauré un cadre pérenne de prise en charge des activités de télésurveillance médicale, codifié à l'**article L. 162-52 du code de la sécurité sociale**. Ce dispositif repose sur une liste des activités de télésurveillance prises en charge par l'Assurance maladie, complétée progressivement par voie réglementaire, ainsi que sur des forfaits destinés à financer leur mise en œuvre.

PRISE EN CHARGE DES ACTIVITÉS DE TÉLÉSURVEILLANCE MÉDICALE

La télésurveillance médicale poursuit son intégration dans le droit commun de l'Assurance maladie. Plusieurs textes publiés en 2025 et 2026 étendent ou adaptent les modalités de prise en charge applicables à différentes pathologies, contribuant ainsi à la diversification progressive des activités de télésurveillance prises en charge.



TÉLÉSURVEILLANCE DU DIABÈTE GESTATIONNEL

Renouvellement de la prise en charge du DMN MYDIABBY jusqu'en 2028

- Arrêté du 27 mars 2026 portant renouvellement d'inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° L 0077 du 31 mars 2026

TÉLÉSURVEILLANCE DES PORTEURS DE MONITEURS CARDIAQUES IMPLANTÉS

Inscription du dispositif CARELINK (Medtronic)

- Arrêté du 24 juillet 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025
- Arrêté du 24 juillet 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0182 du 7 août 2025

Inscription du dispositif HOME MONITORING SERVICE CENTER (Biotronik)

- Arrêté du 23 juin 2025 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0149 du 28 juin 2025
- Arrêté du 23 juin 2025 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0147 du 26 juin 2026

Inscription du dispositif LATITUDE CLARITY (Boston Scientific)

- Arrêté du 3 mars 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026
- Arrêté du 3 mars 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0055 du 5 mars 2026

Inscription du dispositif IMPLICITY IM009 (Implicity)

- Arrêté du 20 mai 2026 portant inscription d'activité de télésurveillance médicale sur la liste prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n° 0119 du 22 mai 2026
- Arrêté du 20 mai 2026 fixant le montant d'un forfait technique applicable à une activité de télésurveillance inscrite sur la liste des activités de télésurveillance médicale prévue à l'article L. 162-52 du code de la sécurité sociale, *JORF* n°0119 du 22 mai 2026



GUIDE DE LA CONSULTATION, « Comment consulter les documents de Mon espace santé »

par Lukas MARA

Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Le guide *« Mon espace santé/DMP »* est intéressant pour comprendre les évolutions actuelles du numérique en santé en France. Il présente principalement les nouvelles modalités d'accès aux données médicales et leur gestion par les professionnels de santé et les patients. Ainsi, le guide ne se limite pas à une simple présentation technique de la plateforme. Il expose des enjeux juridiques, organisationnels et éthiques liés à la circulation des données de santé dans un système de soins de plus en plus numérisé.

Le guide rappelle que le vieillissement de la population, l'augmentation des maladies chroniques et la complexification des parcours de soins rendent indispensable une meilleure coordination entre les professionnels de santé. Le numérique apparaît alors comme une réponse à ces difficultés, notamment grâce à la centralisation et au partage sécurisé des données médicales. Mon espace santé est un outil destiné à fluidifier les échanges d'informations entre les acteurs du soin tout en renforçant la place du patient dans la gestion de sa santé. En effet, Mon espace santé succède au Dossier Médical Partagé (DMP), créé initialement en 2004 mais dont le déploiement a longtemps été considéré comme un échec. Il y avait plusieurs difficultés qui empêchaient son adoption massive : les dossiers n'étaient pas créés automatiquement, les professionnels de santé ne les alimentaient pas régulièrement et les logiciels utilisés n'étaient pas suffisamment interopérables. Afin de remédier à ces limites, la loi de 2019 instaure un système d'opt-out avec la création automatique d'un profil pour chaque assuré social, sauf opposition de sa part. Mon espace santé est ensuite généralisé en 2022 comme nouvelle version du DMP, avec une logique davantage centrée sur le patient.

Mon espace santé ne doit plus être perçu comme un simple dossier médical numérique. Le guide insiste au contraire sur le fait qu'il s'agit d'un véritable *« compagnon de santé »*. La plateforme permet notamment au patient d'accéder à ses antécédents médicaux, à ses ordonnances, à ses comptes rendus d'hospitalisation, à ses résultats de biologie ou encore à ses vaccinations. Elle comprend également une messagerie sécurisée, un agenda médical et différents outils de prévention. Cette évolution traduit une volonté claire des pouvoirs publics de mettre en avant un patient acteur, plus autonome dans son parcours de soins.

De surcroît, le guide met en avant le renforcement des droits des patients sur leurs données de santé. En effet, contrairement à l'ancien DMP, certaines informations n'étaient pas nécessairement accessibles au patient. Désormais, le principe repose sur la transparence puisque l'usager peut consulter les données présentes dans son espace santé. Le patient peut consulter l'historique des accès à son dossier, recevoir des notifications lorsqu'un professionnel consulte ses données et masquer certains documents s'il le souhaite. Cette logique rejoint les principes du RGPD et de la protection des données personnelles, particulièrement

importantes lorsqu'il s'agit de données sensibles.

Ensuite, le guide présente les différentes situations dans lesquelles les professionnels de santé utilisent Mon espace santé. Ils peuvent s'en servir avant une consultation, pendant une hospitalisation, aux urgences ou après une prise en charge pour assurer le suivi du patient. Il met aussi en avant plusieurs avantages concrets comme le gain de temps, la réduction des examens réalisés plusieurs fois, une meilleure connaissance des antécédents du patient et une meilleure coordination entre les professionnels. Le développement du numérique en santé répond donc à des besoins concrets pour améliorer l'efficacité des soins.

Le cœur juridique du guide repose sur le mécanisme appelé « **DICAH** », qui correspond aux cinq conditions cumulatives nécessaires pour accéder aux données de santé d'un patient. Ce système est particulièrement intéressant car il illustre la manière dont les exigences juridiques sont traduites techniquement dans les outils numériques de santé.

1. La première condition est la **D**isponibilité du profil Mon espace santé du patient. Le guide précise qu'environ 68 millions de profils ont déjà été créés automatiquement pour les assurés sociaux.
2. La deuxième condition concerne l'**I**dentité Nationale de Santé (INS), présentée comme un identifiant numérique sécurisé permettant de garantir l'identification correcte du patient. Cette identification est importante car elle permet d'éviter les erreurs médicales liées à une confusion entre patients.
3. La troisième condition est le **C**onsentement du patient. Les professionnels de santé ne peuvent accéder qu'aux informations nécessaires à la prise en charge du patient. Celui-ci doit être informé et donner son accord, afin de garantir le respect de sa vie privée et du secret médical. Le guide prévoit également des règles particulières pour les mineurs avec un système de *« connexion secrète »* permettant de protéger certaines informations médicales sensibles. Cela montre l'importance accordée à la confidentialité des données de santé. De plus, en cas d'urgence, un accès exceptionnel appelé *« bris de glace »* est possible lorsque le patient ne peut pas donner son consentement et que sa vie est en danger. Cet accès reste toutefois strictement encadré et doit être justifié.
4. La quatrième condition concerne l'**A**uthentification du professionnel de santé. Le professionnel doit se connecter de manière sécurisée afin de protéger les données médicales du patient.
5. Enfin, la cinquième condition est l'**H**abilitation du professionnel. L'accès aux documents médicaux dépend de la profession du soignant et de son rôle dans la prise en charge du patient, notamment grâce à des outils sécurisés comme la carte CPS ou ProSanté Connect.

Ainsi, le guide montre que Mon espace santé s'inscrit dans une stratégie plus globale de transformation numérique du système de santé français. Les années 2026 et 2027 doivent permettre une intégration encore plus poussée dans les logiciels hospitaliers et les outils métiers des professionnels de santé. L'objectif est de rendre l'accès aux données médicales plus fluide et plus automatique afin d'améliorer la continuité des soins. Ce guide présente donc un intérêt majeur pour comprendre les mutations actuelles du droit du numérique en santé. Il illustre concrètement la manière dont les outils numériques modifient les relations entre patients, professionnels et établissements de santé. Il montre également que le développement du partage des données de santé nécessite un équilibre constant entre efficacité des soins, protection de la vie privée, cybersécurité et

respect des droits fondamentaux des patients.

ANS, *Guide professionnel de santé – Consultation Mon espace santé/DMP*, septembre 2025.

Actualisation des critères de référencement des services et outils numériques dans Mon espace santé

L'arrêté du 19 juin 2025 met à jour les critères applicables au référencement des services et outils numériques au sein du catalogue de Mon espace santé. Il remplace le référentiel de référencement précédemment en vigueur par une nouvelle version destinée à adapter les exigences applicables aux solutions numériques intégrées à l'espace numérique de santé. Cette évolution vise notamment à renforcer les garanties en matière de sécurité, d'interopérabilité, de protection des données et de qualité des services proposés aux usagers.

Arrêté du 19 juin 2025 modifiant l'arrêté du 20 novembre 2023 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé, JORF n° 0147 du 26 juin 2025.

Approbation du référentiel d'utilisation de l'application carte Vitale comme moyen d'identification à distance

L'arrêté du 5 février 2026 approuve le référentiel fixant les critères applicables à l'utilisation de l'application carte Vitale comme moyen d'identification à distance des usagers. Ce référentiel définit les exigences techniques, organisationnelles et de sécurité auxquelles doivent satisfaire les services souhaitant recourir à ce dispositif. Il vise à garantir un niveau élevé de confiance dans les procédures d'identification numérique tout en assurant la protection des données personnelles et la sécurisation des échanges dématérialisés.

Arrêté du 5 février 2026 approuvant le référentiel fixant les critères applicables en vue de la délivrance de l'autorisation d'utilisation de la carte Vitale sous forme d'application mobile comme moyen d'identification à distance des utilisateurs, *JORF* n° 0034 du 10/02/2026.



L'APPLICATION CARTE VITALE COMME MOYEN D'AUTHENTIFICATION À DISTANCE

L'application carte Vitale (apCV) ne constitue plus seulement une version dématérialisée de la carte Vitale. Elle a vocation à devenir un véritable outil d'identification numérique. Des services autorisés pourront ainsi s'appuyer sur l'application pour vérifier à distance l'identité d'un usager lors de démarches en ligne, sans présence physique. Le référentiel approuvé par l'arrêté fixe les garanties de sécurité, d'authentification et de protection des données applicables à cette utilisation.

SANTEXPO 2026

60ème édition

« L'excellence en santé : un engagement pour toutes les générations »

Le numérique en santé

Synthèse

Droit du numérique en santé

Thomas BOUDON
Étudiant en Master Droit de la santé
École de droit de Toulouse, Université Toulouse Capitole

D'après les notes du salon des 19, 20 et 21 mai 2026
Paris Expo, Porte de Versailles • Salon organisé par la Fédération hospitalière de France

GLOSSAIRE DES ABREVIATIONS

Les sigles et acronymes employés dans la synthèse sont rassemblés ci-dessous. Ils sont utilisés de manière uniforme dans le corps du texte, après une première mention développée lorsque la clarté l'exige.

Sigle	Signification
CE	conformité européenne (marquage)
CHU	centre hospitalier universitaire
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (loi américaine de 2018)
CNIL	Commission nationale de l'informatique et des libertés
CRA	règlement sur la cyberrésilience (Cyber Resilience Act)
DPO	délégué à la protection des données (data protection officer)
EDS	entrepôt de données de santé
EHDS	espace européen des données de santé (European Health Data Space)
FHIR	standard d'interopérabilité en santé (Fast Healthcare Interoperability Resources)
HDS	hébergeur de données de santé (certification)
IA	intelligence artificielle
MDR	règlement européen sur les dispositifs médicaux (Medical Device Regulation)
NIS 2	directive « Network and Information Security » 2
OpenEHR	standard ouvert de modélisation et de stockage du dossier de santé
RGPD	règlement général sur la protection des données
SecNumCloud	visa de sécurité national pour les services d'informatique en nuage (« cloud de confiance »)
TFUE	Traité sur le fonctionnement de l'Union européenne
UGAP	Union des groupements d'achats publics
UniHA	réseau coopératif des achats hospitaliers

AVANT-PROPOS

Du 19 au 21 mai 2026 s'est tenue, à Paris Expo – Porte de Versailles, la 60e édition du salon SANTEXPO, organisé par la Fédération hospitalière de France[196]. Placée sous le thème de **« l'excellence en santé »**, cette édition anniversaire a consacré plus de la moitié de sa programmation au numérique en santé, réunissant près de 36 000 participants, quelque 700 exposants et plus de 550 intervenants[197]. C'est à partir des notes prises au fil de ces trois journées, en représentation de l'Université Toulouse Capitole, qu'a été bâtie la présente synthèse.

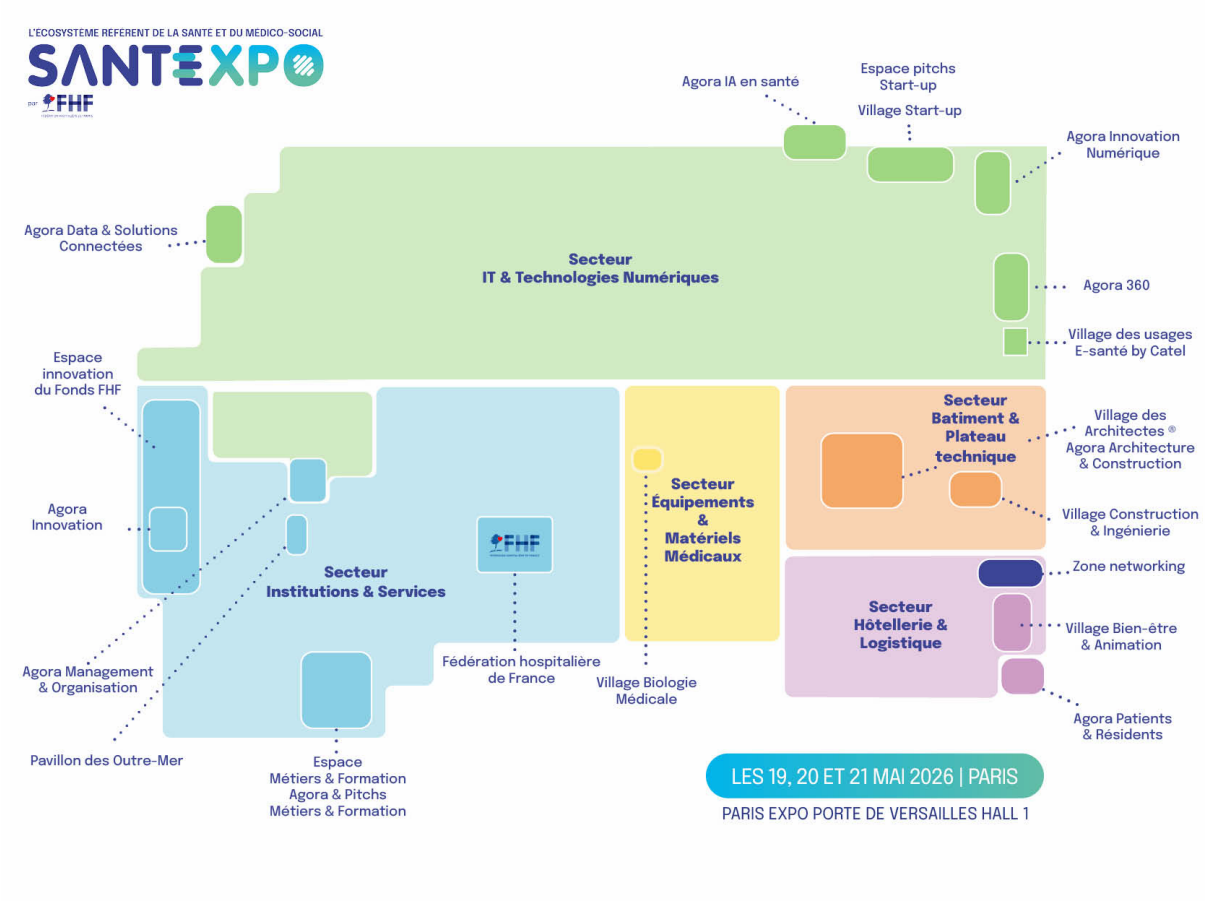


Figure — SANTEXPO 2026 — Plan su salon.

Le présent document n'est pas une restitution exhaustive du salon (objet d'une trace écrite distincte) mais un **exercice de synthèse** répondant à la méthodologie de la dissertation : amorce, délimitation du sujet, intérêt, problématisation, problématique et annonce de plan en introduction ; développement en trois parties articulées par de brèves transitions ; conclusion ouverte. La matière première demeure les notes du salon, mais le propos a été enrichi des enseignements du Master Droit de la Santé et du diplôme d'université *Digital Health Law*, ainsi que de recherches complémentaires. L'appareil de référencement en notes adopte le format de la bibliothèque de l'Université Toulouse Capitole.

Avertissement. La synthèse s'appuie sur des propos d'intervenants rapportés de mémoire et de notes personnelles ; ils n'engagent ni leurs auteurs, ni les organisations citées. Les chiffres et exemples issus du salon sont reproduits à titre documentaire, et les mentions de solutions ou d'éditeurs le sont à titre purement informatif. L'analyse, les rapprochements et les éventuelles erreurs n'engagent que l

eur auteur.

[196] Fédération Hospitalière de France, *SantExpo 2026* (consulté le 30/05/2026).
[197] APMnews, « L'excellence en santé, fil rouge de l'édition 2026 de Santexpo » [en ligne], 5 mai 2026 (consulté le 30/05/2026).

INTRODUCTION

Le 11 février 2024, peu après deux heures du matin, les imprimantes du centre hospitalier d'Armentières se sont mises à cracher une demande de rançon ; quatre-vingt-quinze pour cent du réseau était déjà chiffré, les urgences ont fermé soixante-douze heures, et l'établissement est revenu au papier. Quelques mois plus tard, lors de la soixantième édition du salon SANTEXPO, en mai 2026, un intervenant résumait l'épisode d'une formule qui a fait mouche : *« ce n'est pas un sujet informatique, c'est un sujet de soins »*. La phrase dit l'essentiel. Le numérique a cessé d'être un outil périphérique de l'hôpital pour en devenir le système nerveux, au point qu'une défaillance technique se traduit aujourd'hui en pertes de chances pour le patient, voire en décès.

Cette bascule est l'objet de la présente synthèse. Par « numérique en santé », on entend l'ensemble des technologies (dossiers patients informatisés, entrepôts de données, dispositifs médicaux logiciels, systèmes d'intelligence artificielle, infrastructures d'hébergement) qui transforment la production, la circulation et l'exploitation de l'information de santé. Le champ couvert dépasse le seul hôpital : il embrasse les trois composantes du système de santé français, le secteur sanitaire, le secteur social et le secteur médico-social[198], dont la réunion sous une même bannière demeure, du reste, davantage un horizon qu'une réalité homogène. Sur ce terrain mouvant s'est invité, en quelques années, un corpus de textes européens d'une densité inédite : règlement sur l'espace européen des données de santé (EHDS), règlement sur l'intelligence artificielle (IA), directive « NIS 2 », règlement sur la cyberrésilience (CRA), sans compter le socle que constituent le règlement général sur la protection des données (RGPD) et le règlement relatif aux dispositifs médicaux (MDR).

L'intérêt du sujet tient précisément à cette concomitance. Jamais le législateur de l'Union n'a, en si peu de temps, autant encadré un secteur ; et jamais le calendrier ne s'est fait aussi pressant, l'EHDS devant produire ses principaux effets dès 2029[199]. Or cette pression réglementaire rencontre un système de santé fragile : infrastructures héritées et cloisonnées, établissements publics corsetés par leur statut, financements contraints, disparités territoriales criantes, le tout dans un marché du numérique de santé encore neuf mais déjà férocement disputé, où les solutions les plus performantes sont souvent américaines. La transition n'est donc ni un simple projet de modernisation, ni une affaire de pure conformité : elle est le point de rencontre d'une contrainte juridique exogène, d'une nécessité opérationnelle endogène et d'une vulnérabilité structurelle.

De là naît une tension que les trois jours du salon n'ont cessé d'illustrer. D'un côté, une transformation imposée par le droit de l'Union et aspirée par un marché qui n'attend pas ; de l'autre, un appareil de soins inégalement préparé, dont les acteurs publics doivent composer avec des règles, qu'il s'agisse de la commande publique, de la fonction publique ou du principe de spécialité, pensées pour un autre temps. Entre les deux, des principes que nul ne saurait sacrifier : la souveraineté sur les données, la sécurité des systèmes, le respect des droits des patients.

Dans quelle mesure le système de santé français, dans ses composantes sanitaire, sociale et médico-sociale, est-il juridiquement et structurellement prêt à absorber une transition numérique imposée par le droit de l'Union et portée par un marché concurrentiel, sans sacrifier la

[198] *SantExpo 2026*, préc.

[199] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé, *JOUE* [en ligne], 5 mars 2025 ; entrée en vigueur le 26 mars 2025, application progressive (usage primaire en 2027, usage secondaire en 2029, catégories étendues en 2031) (consulté le 30/05/2026).

souveraineté, la sécurité ni les droits des patients ?

Répondre suppose d'abord de mesurer la force qui pousse à la transformation : une transition à marche forcée, sous la double aiguillon du droit européen et des nécessités du soin (I). Il faut ensuite confronter cet élan à la réalité d'un système inégalement armé pour l'absorber, où la maturité numérique des secteurs le dispute aux contraintes propres à l'acteur public (**II**). Il s'agira enfin de dégager les voies d'un équilibre juridique soutenable, à même de réconcilier souveraineté, performance, sécurité et droits des patients (**III**).

I. Une transition numérique à marche forcée

A. Une contrainte exogène : le droit de l'Union comme moteur

1. L'EHDS et la circulation des données de santé

Au sommet de l'édifice trône le règlement du 11 février 2025 relatif à l'EHDS[200]. Le choix de sa base juridique mérite qu'on s'y arrête, car il est révélateur : l'Union s'est fondée sur l'article 114 du Traité sur le fonctionnement de l'Union européenne (TFUE), relatif au marché intérieur, plutôt que sur l'article 168, qui ne lui reconnaît qu'une compétence d'appui en matière de santé[201]. Autrement dit, c'est par la logique du marché unique, et non par celle de la santé publique, que la Commission européenne a pu imposer un cadre contraignant. La donnée de santé devient une marchandise circulant librement. Et cette qualification commande tout le reste.

Deux usages structurent le règlement. D'abord, l'usage primaire consacre des droits nouveaux au bénéfice du patient : accès à ses données, portabilité, échange transfrontalier de son dossier et de ses prescriptions électroniques, le tout adossé à un format européen reposant sur le standard FHIR[202]. Ensuite, l'usage secondaire ouvre la réutilisation des données à des fins de recherche, d'innovation ou de pilotage des politiques publiques, via un guichet géré par un organisme responsable de l'accès aux données et soumis à autorisation. Son entrée en application est progressive : 2027 pour l'usage primaire, 2029 pour l'essentiel de l'usage secondaire, 2031 pour les catégories étendues[203]. L'échéance, elle, est désormais inscrite dans le marbre. Pour les établissements, le message est clair : l'interopérabilité n'est plus une option mais une obligation, et la certification des plateformes deviendra la condition même de l'accès au réseau européen. On comprend qu'au centre hospitalier universitaire (CHU) de Toulouse, les responsables avouaient se préparer « un peu à l'aveugle », faute d'actes d'exécution encore stabilisés.

2. L'IA Act et le MDR : la régulation des systèmes et des dispositifs

Adopté le 13 juin 2024, le règlement sur l'IA procède d'une tout autre méthode : horizontale, graduée selon le risque, et résolument extraterritoriale[204]. En santé, la plupart des systèmes déployés (aide au diagnostic, tri des patients, codage) basculent dans la catégorie à haut risque de l'annexe III, ce qui emporte des obligations lourdes de documentation, de transparence et de surveillance. Certes, le calendrier de ces obligations a été assoupli, le « Digital

---

[200] Règlement (UE) 2025/327 (EHDS), préc.

[201] *Traité sur le fonctionnement de l'Union européenne*, art. 114 (rapprochement des législations, marché intérieur), retenu comme base juridique du règlement EHDS de préférence à l'art. 168 (compétence d'appui en matière de santé publique).

[202] HL7 International, *HL7 FHIR, Fast Healthcare Interoperability Resources* [en ligne] (consulté le 30/05/2026).

[203] Règlement (UE) 2025/327 (EHDS), préc.

[204] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'IA), *JOUE* [en ligne], 12 juillet 2024 ; v. not. l'annexe III (systèmes à haut risque) et l'art. 40 (normes harmonisées) (consulté le 30/05/2026).

Omnibus » de novembre 2025 ayant repoussé certaines échéances[205], mais la direction ne fait pas de doute.

À ce premier texte se superpose le règlement de 2017 sur les dispositifs médicaux[206]. Dès lors qu'un logiciel poursuit une finalité médicale, il est un dispositif médical, soumis à une classification par niveau de risque et au marquage CE délivré sous le contrôle d'organismes notifiés. Ainsi, la solution d'aide à la décision présentée au salon était marquée CE en classe IIa, ses éditeurs devant articuler conformité au règlement sur les dispositifs et exigences à venir du règlement sur l'IA. Pareille double conformité n'a rien d'académique : un acteur étranger jugé non conforme, OpenEvidence, n'était à la date du salon accessible ni dans l'Union, ni au Royaume-Uni. La régulation produit donc déjà des effets de marché. Elle s'adosse d'ailleurs largement à la normalisation technique : les normes harmonisées, au sens de l'article 40 du règlement sur l'IA, valent présomption de conformité, déplaçant une part du pouvoir normatif vers des organismes privés[207].

3. NIS 2 et le Cyber Resilience Act : la cybersécurité érigée en obligation

Longtemps affaire de bonnes pratiques, la sécurité numérique est devenue une obligation juridique sanctionnée. Promulguée le 14 décembre 2022, la directive « NIS 2 » range la santé parmi les secteurs hautement critiques et classe les établissements, selon leur taille et leur nature, en entités essentielles ou importantes[208]. Trois obligations en découlent : s'enregistrer auprès de l'autorité compétente, notifier les incidents significatifs, et déployer des mesures de gestion des risques déclinées par le référentiel cyber national, qui fixe une vingtaine d'objectifs de sécurité[209]. Quant au CRA, entré en vigueur fin 2024 et applicable par paliers jusqu'en 2027, il complète le dispositif en imposant une sécurité « dès la conception » aux fabricants de produits comportant des éléments numériques, tout au long de leur cycle de vie[210].

Quelques chiffres disent l'urgence. En 2024, les établissements de santé ont déclaré quelque sept cent cinquante incidents, en hausse de près de trente pour cent[211], et l'on a observé une augmentation de cent treize pour cent des accidents vasculaires cérébraux mal pris en charge dans les hôpitaux victimes d'une attaque. La cybersécurité a quitté le champ technique pour entrer dans celui de la sécurité des soins.

---

[205] Commission européenne, *Digital Omnibus*, proposition de simplification du cadre numérique de l'Union [en ligne], 19 novembre 2025 (consulté le 30/05/2026).

[206] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (MDR), *JOUE* [en ligne], n° L 117, 5 mai 2017 (consulté le 30/05/2026).

[207] Organisation internationale de normalisation, *NF EN ISO/IEC 27001:2023, Systèmes de management de la sécurité de l'information* [en ligne] (consulté le 30/05/2026).

[208] 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 (directive NIS 2), *JOUE* [en ligne], n° L 333, 27 décembre 2022 (consulté le 30/05/2026).

[209] Agence nationale de la sécurité des systèmes d'information, *Référentiel cyber France (ReCyF)* [en ligne], 2026 (consulté le 30/05/2026).

[210] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences horizontales de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act), *JOUE* [en ligne], 20 novembre 2024 ; entré en vigueur le 10 décembre 2024, application par paliers jusqu'en décembre 2027 (consulté le 30/05/2026).

[211] Agence du numérique en santé / CERT Santé, *Observatoire des signalements d'incidents de sécurité des SI pour le secteur santé, bilan 2025* [en ligne], 2026 (consulté le 30/05/2026).

B. Une nécessité endogène : efficience, qualité et attractivité

1. Désenclaver et structurer des données silotées

Si le droit pousse, le besoin tire. Producteur de données massives, l'hôpital français les enferme pourtant. Un établissement compte couramment des centaines de logiciels qui ne se parlent pas ; tel centre exploitait encore en 2024 un dossier patient mis en service en 1999. Faute d'urbanisation d'ensemble, les systèmes se sont empilés par strates successives. Sur le remède, le consensus est large : une logique d'interopérabilité « par les interfaces » et un entrepôt de données de santé (EDS) capable de centraliser, d'historiser et d'exposer l'information. Encore faut-il ne pas confondre les fonctions, que se partagent plusieurs familles de standards. Pour l'échange entre systèmes, le pivot s'appelle FHIR[212] : il fait circuler la donnée d'un logiciel à l'autre. Pour le stockage, deux standards complémentaires coexistent : OpenEHR[213], qui modélise et conserve le dossier clinique au fil du soin, et OMOP[214], modèle commun qui range et harmonise la donnée dans l'entrepôt, en vue de l'analyse et de la réutilisation. Les uns communiquent, les autres structurent ; c'est leur articulation qui fait la cohérence de l'ensemble. Et le constat, partout au salon, était le même : sans interopérabilité, l'IA reste inopérante, car un modèle n'a de valeur qu'adossé à des données fiables, structurées et croisées. Recueillie au plus près du soin, la qualité de la donnée conditionne tout l'édifice.

2. Libérer du temps soignant et fluidifier le parcours patient

Vient ensuite l'argument du temps. Près de quatre dixièmes du temps de travail hospitalier seraient absorbés par des tâches répétitives ou administratives. Sur ce point, les promesses de gains sont considérables : comptes rendus et lettres de liaison rédigés par assistance vocale, codage des séjours accéléré, synthèse automatique du dossier. Un centre hospitalier avançait une diminution de quarante pour cent du temps de ses agents administratifs ; un acteur du médico-social, une baisse de soixante pour cent du temps de saisie grâce à la dictée. Au-delà de l'efficience, c'est l'attractivité qui est en jeu : recentrer le soignant sur la relation au patient, dans un contexte de pénurie, constitue un argument de recrutement. Même logique pour la fluidification du parcours (télésurveillance des patients chroniques, anticipation des flux aux urgences, coordination ville-hôpital), à la condition expresse que l'humain conserve la décision finale.

3. Se positionner dans un marché neuf et concurrentiel

Une dernière force, plus diffuse, achève d'entraîner le mouvement : la pression du marché. Jeune mais foisonnant, le numérique de santé voit coexister éditeurs historiques convertis à l'IA, plateformes intégrées et myriade de jeunes pousses. En 2024, la France comptait plusieurs centaines d'entreprises de santé numérique, dont près de deux cents pour la seule Occitanie[215]. Une solution française d'IA médicale (MedGPT) revendiquait sept cent mille connexions mensuelles. Dans ce contexte, ne pas se doter d'outils numériques, c'est risquer de décrocher, et ce sur deux plans. Verticalement (micro-vertical), dans la relation au patient : recourant aux assistants conversationnels grand public, celui-ci en vient à interroger son médecin, qui doit à son tour disposer d'outils spécialisés et fiables. Horizontalement (méso-horizontal), entre acteurs de santé : dans des parcours toujours

---

[212] HL7 International, *HL7 FHIR*, préc.

[213] openEHR International, *openEHR Specifications* [en ligne]. Standard ouvert de modélisation et de persistance du dossier de santé (consulté le 30/05/2026).

[214] Observational Health Data Sciences and Informatics, *OMOP Common Data Model* [en ligne] (consulté le 30/05/2026).

[215] APMnews, art. préc.

plus coordonnés, l'établissement ou le professionnel qui n'échange pas ses données se marginalise, sort des circuits d'adressage et se fait contourner par ceux qui, eux, savent se connecter. Le décrochage n'est donc pas seulement commercial, il est relationnel : rester dans le jeu suppose de rester interopérable. Se positionner devient ainsi un impératif de survie autant qu'un choix de gestion : l'image de l'établissement, sa place dans les réseaux de soins et sa capacité à fidéliser les compétences en dépendent. Sa face sombre, la concentration entre quelques mains étrangères, n'apparaîtra qu'au stade des contraintes. À ces deux échelles s'en ajoute une troisième, plus vaste : celle de la France et de l'Union européenne face à la concurrence internationale. Mais à ce niveau, le numérique cesse d'être un simple atout concurrentiel pour devenir une question de souveraineté, dont la face sombre, la concentration du marché entre quelques mains étrangères, n'apparaîtra qu'au stade des contraintes.

Ces forces convergentes, à savoir l'obligation venue de la Commission européenne, la quête d'efficience et la concurrence, dessinent une dynamique puissante. Encore faut-il que le système soit en état d'en soutenir le choc. Or rien n'est moins sûr : la maturité numérique reste très inégale d'un secteur à l'autre, et l'acteur public se heurte à des contraintes que le marché ignore.

II. UN SYSTÈME INÉGALEMENT ARMÉ POUR L'ABSORBER

A. Une maturité numérique différenciée selon les secteurs

1. Le sanitaire : richesse des données, faiblesse des infrastructures

Côté sanitaire, le paradoxe est saisissant. Les données y sont d'une richesse rare : l'Assistance publique-Hôpitaux de Paris suit huit millions de patients par an, et certains centres disposent de quarante années d'historique exploitable. Mais les infrastructures peinent à suivre. Huit cents applications cohabitent parfois au sein d'un même groupe, le dossier patient demeure peu structuré, et certains progiciels de référence, anciens et éprouvés, n'évoluent plus qu'à grand-peine. On dénombrait cent vingt-cinq EDS autorisés par la Commission nationale de l'informatique et des libertés (CNIL), signe d'une dynamique réelle ; mais le pays ne disposait que de trois supercalculateurs publics, ce qui borne sa capacité d'entraînement de modèles. Richesse de la matière première, pauvreté de l'outillage : le contraste est frappant.

2. Le social et le médico-social : un retard préoccupant

Dès que l'on quitte l'hôpital, le tableau s'assombrit. Le social et le médico-social accusent un retard de numérisation préoccupant, que traduit le déploiement encore embryonnaire du dossier usager informatisé. Quant au programme national de cybersécurité, il ne s'y est ouvert que tardivement : l'appel à projets dédié aux établissements et services sociaux et médico-sociaux n'a été lancé, sous forme expérimentale, qu'en mars 2026, pour une vingtaine de lauréats et moins de deux millions d'euros[216]. Pourtant, les usages prometteurs ne manquent pas (robotique sociale, exosquelettes de prévention des troubles musculo-squelettiques, réalité

[216] Agence du numérique en santé, *Programme CaRE : cybersécurité, accélération et résilience des établissements* [en ligne] (consulté le 30/05/2026).

virtuelle apaisante pour les résidents atteints de troubles cognitifs), mais ils se déploient sur un socle fragile, où la maturité cybersécuritaire reste faible et la mobilisation des acteurs encore timide. Ici, le défi est moins technologique qu'organisationnel et financier.

3. La ville et la coordination des parcours : l'enjeu de la responsabilité populationnelle

Entre l'hôpital et le domicile, la ville constitue le maillon le plus difficile à intégrer. Souvent prisonnières des cabinets libéraux, les données y restent dispersées, ce qui contraint à bâtir des passerelles spécifiques. Or l'enjeu dépasse la seule technique : il s'agit d'assumer une responsabilité populationnelle, c'est-à-dire de penser la santé d'un territoire entier, en stratifiant la population par niveau de risque et en réunissant un consortium ville-hôpital. Déployée dans plusieurs milliers de pharmacies, la téléconsultation assistée répond directement aux déserts médicaux ; la directive de 2011 sur les soins transfrontaliers[217] avait, dès avant l'EHDS, posé les jalons d'une mobilité du patient. Mais la coordination suppose une information fiable, disponible au bon moment et à la bonne personne : exactement ce que le morcellement actuel rend malaisé.

B. Des acteurs publics juridiquement et économiquement contraints

1. Le statut public : commande publique et fonction publique hospitalière

C'est ici que le juriste retrouve son terrain. Établissement public, l'hôpital est un pouvoir adjudicateur, soumis au Code de la commande publique et à ses principes cardinaux : liberté d'accès, égalité de traitement des candidats, transparence des procédures[218]. Dès 2003, le Conseil constitutionnel leur a reconnu valeur constitutionnelle[219]. Ces garanties, précieuses pour le bon emploi des deniers publics, ont un revers : la lenteur. Là où le marché du numérique se renouvelle en quelques mois, la passation d'un marché public s'étire, impose la rédaction de clauses techniques exigeantes (en lien avec le responsable de la sécurité et le délégué à la protection des données, le DPO) et se heurte aux conditions générales d'utilisation, non négociables, des grands fournisseurs. D'où un risque, maintes fois souligné au salon : que « les bonnes solutions arrivent trop tard ».

Pour desserrer cet étau, les établissements peuvent passer par une centrale d'achat. En se fournissant auprès de l'UGAP, établissement public industriel et commercial, ou d'un réseau coopératif hospitalier comme UniHA, qui s'interposent entre les EPS et les industriels, l'acheteur s'épargne sa propre procédure : la mise en concurrence a déjà été faite en amont[220]. Le gain de temps est réel, mais il a une contrepartie. La centrale prélève une commission, et surtout l'établissement choisit dans un catalogue déjà référencé : son éventail se réduit aux solutions retenues par l'opérateur. Le contournement de la lenteur se paie ainsi d'un libre choix plus étroit, et la commodité tend à orienter l'achat autant que le besoin propre de l'établissement. La centrale est donc une réponse ambivalente, dont on retrouvera le versant vertueux, la mutualisation, au stade des solutions.

À la rigidité de l'achat s'ajoute celle de l'emploi. Avec son recrutement par concours et ses grilles, la fonction publique

---

[217] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* [en ligne], n° L 88, 4 avril 2011 (consulté le 30/05/2026).

[218] *Code de la commande publique*, art. L. 3 (principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures, garants de l'efficacité de la commande publique et de la bonne utilisation des deniers publics).

[219] Conseil constitutionnel, décision n° 2003-473 DC du 26 juin 2003 (consécration de la valeur constitutionnelle des principes fondamentaux de la commande publique).

[220] *Code de la commande publique*, art. L. 2113-2 et s. (centrales d'achat).

hospitalière peine à attirer des compétences rares, ingénieurs en données ou spécialistes de la sécurité, que le privé surpaye. Vieillissement des effectifs, dont un tiers a passé la cinquantaine, et débat récurrent sur le poids des fonctions administratives compliquent encore l'équation. Le facteur humain, en définitive, pèse autant que le facteur technique.

2. Des financements et un retour sur investissement incertains, sur fond de disparités territoriales

L'argent commande, et il manque. Contraints, les budgets hospitaliers le sont à l'heure où le retour sur investissement des projets d'IA demeure difficile à objectiver : il faut le mesurer sur quatre registres (opérationnel, économique, qualité des soins et gouvernance) sans se contenter d'une démonstration de laboratoire. Des financements fléchés existent, du programme de cybersécurité doté de sept cent cinquante millions d'euros[221] au volet numérique du Ségur de la santé[222] ; mais un projet pilote réussi ne préjuge en rien d'un passage à l'échelle, lequel coûte cher et tarde à produire ses fruits. Surtout, ces moyens se répartissent inégalement. Un grand CHU et un petit hôpital de proximité ne disposent ni des mêmes équipes, ni de la même capacité d'investissement : la fracture numérique épouse la fracture territoriale, et la première creuse la seconde.

3. Une dépendance technologique extra-européenne : la souveraineté entre impératif et surcoût

C'est alors que réapparaît le marché, sous son visage inquiétant. Près des deux tiers du marché mondial du cloud sont contrôlés par trois acteurs américains, et l'écrasante majorité des grands modèles d'IA sont conçus hors d'Europe. Or le droit américain, par le CLOUD Act de 2018, autorise un accès extraterritorial aux données hébergées par ces entreprises[223]. La souveraineté numérique, c'est-à-dire la localisation des données dans l'Union, leur traitement depuis l'Union, le contrôle opérationnel et la maîtrise contractuelle, n'est donc pas un slogan, mais une réponse à une vulnérabilité juridique réelle, que la loi visant à sécuriser et réguler l'espace numérique a entendu renforcer[224]. Le hic est son coût. Choisir la souveraineté, c'est souvent renoncer aux solutions les plus performantes, et payer plus cher : l'arbitrage se joue entre fiabilité, coût et souveraineté, et il pèse d'autant plus lourd que l'établissement est modeste. La boucle se referme ainsi sur les disparités territoriales.

Le diagnostic est posé : une transition irrésistible se heurte à un système inégalement préparé et à un acteur public bridé. Plutôt que d'y voir une impasse, le droit offre les instruments d'un équilibre, à condition de concilier ce qui paraît d'abord inconciliable : la souveraineté et la performance, puis la valorisation des données, leur sécurité et les droits des patients.

III. UN ÉQUILIBRE JURIDIQUE À CONSTRUIRE POUR UNE TRANSITION SOUTENABLE

A. Concilier souveraineté et performance

1. La maîtrise de l'hébergement et des données

Un premier levier est juridico-technique. En santé, l'exigence portant sur l'hébergement est doublement justifiée. La donnée est sensible, d'abord, au sens où sa divulgation porte gravement atteinte à la vie

[221] Agence du numérique en santé, *Programme CaRE*, préc.
[222] Agence du numérique en santé, *Ségur du numérique en santé* [en ligne] (consulté le 30/05/2026).
[223] États-Unis, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. n° 115-141, 23 mars 2018.
[224] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *JORF* [en ligne], n° 0119, 22 mai 2024 (consulté le 30/05/2026).

privée de la personne[225] ; mais elle est aussi engagée dans le soin, car elle nourrit le diagnostic et la décision thérapeutique. Ce n'est donc pas seulement sa confidentialité qu'il faut garantir, c'est aussi son intégrité et sa disponibilité, dont dépend directement la sécurité du patient. Voilà pourquoi tout hébergement de données de santé est subordonné à la certification HDS[226], à laquelle s'ajoute, pour les usages les plus sensibles, le référentiel SecNumCloud de l'agence nationale de la sécurité des systèmes d'information, qui qualifie le « cloud de confiance »[227]. Le panel s'est étoffé : cloud public souverain, cloud privé régulé (où l'hébergeur s'interdit l'accès aux données et où l'établissement conserve les clés de chiffrement), architectures hybrides. D'ailleurs, la pratique a trouvé un compromis astucieux : tester et entraîner les modèles sur un cloud public, plus rapide et moins onéreux, puis déployer en local la solution retenue, au plus près des données sensibles. Au fond, la souveraineté n'exige pas de renoncer à toute performance ; elle commande de cartographier, pour chaque usage, le niveau de protection juridiquement adéquat.

2. La mutualisation comme réponse

Plus organisationnel, le second levier répond directement aux contraintes du statut public. Rendus obligatoires par la loi de modernisation de notre système de santé de 2016, les groupements hospitaliers de territoire imposent une convergence des systèmes d'information qui mutualise compétences et investissements[228]. Cette logique se prolonge dans les centrales d'achat : l'Union des groupements d'achats publics, établissement public industriel et commercial, et le réseau coopératif hospitalier UniHA jouent le rôle de tiers de confiance entre les établissements et les industriels, et dispensent l'acheteur d'une partie du formalisme[229]. À l'échelle supérieure, le partage de l'innovation entre établissements publics (« briques » réplicables, infrastructures de calcul communes à plusieurs centres universitaires) permet de répartir le coût de la souveraineté et d'atténuer les disparités territoriales. Ce que la rigidité de la commande publique freine d'un côté, la mutualisation le débloque de l'autre.

B. Concilier valorisation, sécurité et droits des patients

1. Une valorisation encadrée et non lucrative de la donnée

Réelle, la valeur des données françaises découle d'un trait que l'on ne soupçonne pas toujours : l'égalité d'accès aux soins produit des jeux de données diversifiés, donc fiables, là où des systèmes plus inégalitaires les biaisent. Encore faut-il valoriser sans dénaturer. À cette fin, le régime de l'usage secondaire de l'EHDS recourt à un système de redevances dont la finalité n'est pas lucrative : on ne vend pas la donnée, on facture un appui méthodologique[230]. En droit interne, l'architecture est connue : Système national des données de santé[231],

---

[225] Règlement (UE) 2016/679 (RGPD), art. 9 (interdiction de principe et protection renforcée du traitement des catégories particulières de données, dont les données concernant la santé).

[226] Ministère chargé de la santé / Agence du numérique en santé, *Certification des hébergeurs de données de santé (HDS)* [en ligne] (consulté le 30/05/2026).

[227] Agence nationale de la sécurité des systèmes d'information, *SecNumCloud : référentiel d'exigences pour les prestataires de services d'informatique en nuage* [en ligne] (consulté le 30/05/2026).

[228] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* [en ligne], n° 0022, 27 janvier 2016 (groupements hospitaliers de territoire, art. L. 6132-1 du *Code de la santé publique*) (consulté le 30/05/2026).

[229] *Code de la commande publique*, art. L. 2113-2 et s. (centrales d'achat). L'Union des groupements d'achats publics (UGAP), établissement public à caractère industriel et commercial, et le réseau coopératif hospitalier UniHA agissent comme centrales d'achat au service des acheteurs publics de santé.

[230] Règlement (UE) 2025/327 (EHDS), préc.

[231] Commission nationale de l'informatique et des libertés, *Le Système national des données de santé (SNDS)* [en ligne] (consulté le 30/05/2026).

Health Data Hub comme guichet[232], réseau régional d'entrepôts. Et la stratégie nationale de réutilisation pour 2025-2028, issue d'un rapport de 2023, en a fait sa boussole, plaçant la confiance au cœur du dispositif[233]. Soulignée par les praticiens du salon, la frontière juridique est nette : une exploitation lucrative ne se conçoit que sur des données anonymisées, sorties du champ du RGPD[234] ; jamais sur des données simplement pseudonymisées. La CNIL, devenue accompagnatrice plus que gendarme, y veille par ses méthodologies de référence, dans la logique de responsabilisation des acteurs.

2. La cybersécurité, condition de la continuité des soins

Certaines exigences ne se négocient pas, et la première est la sécurité informatique. Longtemps réduite à une affaire d'informaticiens, elle se laisse aujourd'hui saisir par une grille à quatre exigences, résumées par l'acronyme DICP : la disponibilité de la donnée, son intégrité, sa confidentialité et la preuve, c'est-à-dire la traçabilité des accès. Ces quatre propriétés ne protègent pas seulement un patrimoine informationnel ; elles conditionnent la possibilité même de soigner. Une donnée indisponible au moment du diagnostic, ou silencieusement altérée, se paie en perte de chances pour le patient. Voilà pourquoi le programme national de cybersécurité ne se contente plus de prévenir l'attaque : il impose d'organiser la survie du SI. Mise en place d'une gouvernance cybersécurité, construction et test d'un plan de continuité et de reprise d'activité, volet numérique du plan blanc, bilans d'impact sur l'activité destinés à identifier les fonctions vitales à rétablir en priorité : l'établissement doit désormais penser le fonctionnement en mode dégradé[235]. L'épisode du centre hospitalier d'Armentières, contraint de revenir au papier durant des semaines, a montré que la question n'est pas de savoir si la panne surviendra, mais comment continuer à soigner lorsqu'elle survient. La cybersécurité a ainsi cessé d'être un sujet technique pour devenir une dimension de la sécurité des soins.

3. Les droits du patient et l'éthique, socle intangible

Reste le ou un socle primordial, celui que nulle promesse d'efficience ne saurait entamer : les droits de la personne et les principes éthiques. Le secret médical, consacré par le Code de la santé publique et réaffirmé par la loi du 4 mars 2002[236], l'information claire, loyale et appropriée, ainsi que le consentement, explicite pour les données sensibles et écrit pour les données génétiques en droit français[237], encadrent strictement la circulation de l'information. Mais le numérique déplace la difficulté : il ne suffit plus de protéger la donnée, il faut garder la maîtrise de la décision qu'elle nourrit. C'est tout le sens de la garantie humaine du recours à l'IA, codifiée à l'article L. 4001-3 du Code de la santé publique depuis la loi de bioéthique de 2021, qui impose information, traçabilité et maintien d'un contrôle humain[238]. La réflexion éthique avait préparé le terrain :

---

[232] Plateforme des données de santé (*Health Data Hub*), *Missions et projet HealthData@EU Pilot* [en ligne] (consulté le 30/05/2026).

[233] MARCHAND-ARVIER (J.), *Faire de la France un pays pionnier de la réutilisation des données de santé*, rapport [en ligne], 2023, fondant la stratégie nationale de réutilisation des données de santé 2025-2028 (consulté le 30/05/2026).

[234] 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 (RGPD), *JOUE* [en ligne], n° L 119, 4 mai 2016 (consulté le 30/05/2026).

[235] Agence du numérique en santé, *Programme CaRE*, préc.

[236] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* [en ligne], 5 mars 2002 ; v. égal. *Code de la santé publique*, art. L. 1110-4 (secret médical).

[237] Règlement (UE) 2016/679 (RGPD), art. 9 (traitement portant sur des catégories particulières de données, dont les données concernant la santé et les données génétiques).

[238] *Code de la santé publique*, art. L. 4001-3 (garantie humaine du recours aux dispositifs médicaux recourant à l'intelligence artificielle), issu

dans leur avis commun de 2022 sur le diagnostic médical et l'IA, le Comité consultatif national d'éthique et le Comité national pilote d'éthique du numérique mettaient en garde contre toute logique de substitution à l'humain et prônaient l'explicabilité des résultats comme la collégialité du regard[239]. Ces exigences prolongent les quatre principes cardinaux de la bioéthique, à savoir l'autonomie, la bienfaisance, la non-malfaisance et la justice, qui en numérique se traduisent en transparence, loyauté et qualité. Encore faut-il les faire vivre : comités d'éthique, coordinateurs de la donnée distincts du DPO, cartographie des usages pour endiguer l'« IA de l'ombre », et surtout formation des professionnels, l'agence nationale estimant que près des trois quarts des incidents seraient évitables par une sensibilisation adéquate. Comme le résumait un dirigeant hospitalier, la sagesse de l'IA vient par la méthode.

CONCLUSION

Le système de santé français n'est pas prêt ; mais il se prépare, et c'est précisément la contrainte européenne qui l'y force. Tel est le paradoxe que révèle SANTEXPO 2026 : le foisonnement normatif de l'Union, souvent vécu comme un fardeau, agit en réalité comme un double ressort. D'un côté, un accélérateur qui impose l'interopérabilité, la sécurité et la traçabilité ; de l'autre, un garde-fou qui hisse les données françaises au rang d'actif de confiance, plus diversifié et mieux protégé que ceux des grands marchés concurrents. La transition est imposée et nécessaire ; le système est inégalement armé, l'acteur public plus contraint que tout autre ; et l'équilibre, lorsqu'il s'esquisse, repose moins sur la technique que sur le droit : souveraineté arbitrée plutôt que proclamée, mutualisation contre fragmentation, valorisation encadrée, sécurité et droits érigés en limites intangibles.

L'horizon, toutefois, demeure incertain. En 2029 puis 2031, les échéances de l'EHDS mettront à l'épreuve la capacité réelle des établissements à tenir le calendrier. L'essor de l'IA agentique, conjugué à la hausse continue de son coût, rouvrira la question de la dépendance technologique et du risque de décrochage européen. Quant au mouvement de simplification amorcé par le « Digital Omnibus », il dira si l'Union sait alléger sa propre charge sans renier ses ambitions. Au-delà des textes et des infrastructures, c'est peut-être la relation entre le patient et le soignant qui sera le plus sûr révélateur de la transition : selon que l'outil numérique libère du temps pour le soin ou s'interpose dans le colloque singulier, il l'aura confortée ou appauvrie. Une certitude demeure : dans un domaine où une panne se mesure en pertes de chances pour le patient, le droit n'est pas l'ennemi de l'innovation, mais la condition de la confiance sans laquelle aucune transition numérique de la santé ne sera humainement et socialement acceptable.

de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

[239] Comité consultatif national d'éthique et Comité national pilote d'éthique du numérique, Avis n° 141 du CCNE et n° 4 du CNPEN, « Diagnostic médical et intelligence artificielle : enjeux éthiques » [en ligne], novembre 2022 (consulté le 30/05/2026).

BIBLIOGRAPHIE

Sont recensées ci-dessous les sources citées en notes de bas de page, classées par nature et présentées selon les conventions de la bibliothèque de l'Université Toulouse Capitole.

I. Textes de l'Union européenne

Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé, *JOUE* [en ligne], 5 mars 2025 ; entrée en vigueur le 26 mars 2025, application progressive (usage primaire en 2027, usage secondaire en 2029, catégories étendues en 2031) (consulté le 30/05/2026).

Traité sur le fonctionnement de l'Union européenne, art. 114 (rapprochement des législations, marché intérieur), retenu comme base juridique du règlement EHDS de préférence à l'art. 168 (compétence d'appui en matière de santé publique).

Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* [en ligne], n° L 88, 4 avril 2011 (consulté le 30/05/2026).

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 (RGPD), *JOUE* [en ligne], n° L 119, 4 mai 2016 (consulté le 30/05/2026).

Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (MDR), *JOUE* [en ligne], n° L 117, 5 mai 2017 (consulté le 30/05/2026).

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'IA), *JOUE* [en ligne], 12 juillet 2024 ; v. not. l'annexe III (systèmes à haut risque) et l'art. 40 (normes harmonisées) (consulté le 30/05/2026).

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 (directive NIS 2), *JOUE* [en ligne], n° L 333, 27 décembre 2022 (consulté le 30/05/2026).

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences horizontales de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act), *JOUE* [en ligne], 20 novembre 2024 ; entré en vigueur le 10 décembre 2024, application par paliers jusqu'en décembre 2027 (consulté le 30/05/2026).

Commission européenne, *Digital Omnibus*, proposition de simplification du cadre numérique de l'Union [en ligne], 19 novembre 2025 (consulté le 30/05/2026).

II. Textes nationaux et droit étranger

Code de la commande publique, art. L. 3 (principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures, garants de l'efficacité de la commande publique et de la bonne utilisation des deniers publics).

Conseil constitutionnel, décision n° 2003-473 DC du 26 juin 2003 (consécration de la valeur constitutionnelle des principes fondamentaux de la commande publique).

Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* [en ligne], n° 0022, 27 janvier 2016 (groupements hospitaliers de territoire, art. L. 6132-1 du *Code de la santé publique*) (consulté le 30/05/2026).

Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* [en ligne], 5 mars 2002 ; v. égal. *Code de la santé publique*, art. L. 1110-4 (secret médical) (consulté le 30/05/2026).

Code de la santé publique, art. L. 4001-3 (garantie humaine du recours aux dispositifs médicaux recourant à l'intelligence artificielle), issu de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique.

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *JORF* [en ligne], n° 0119, 22 mai 2024 (consulté le 30/05/2026).

Code de la commande publique, art. L. 2113-2 et s. (centrales d'achat). L'Union des groupements d'achats publics (UGAP), établissement public à caractère industriel et commercial, et le réseau coopératif hospitalier UniHA agissent comme centrales d'achat au service des acheteurs publics de santé.

États-Unis, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. n° 115-141, 23 mars 2018.

III. Rapports, doctrine et sources institutionnelles

Fédération Hospitalière de France, *SantExpo 2026* [en ligne] (consulté le 30/05/2026).

APMnews, « L'excellence en santé, fil rouge de l'édition 2026 de Santexpo » [en ligne], 5 mai 2026 (consulté le 30/05/2026).

Agence du numérique en santé, *Programme CaRE : cybersécurité, accélération et résilience des établissements* [en ligne] (consulté le 30/05/2026).

Agence du numérique en santé / CERT Santé, *Observatoire des signalements d'incidents de sécurité des SI pour le secteur santé, bilan 2025* [en ligne], 2026 (consulté le 30/05/2026).

MARCHAND-ARVIER (J.), *Faire de la France un pays pionnier de la réutilisation des données de santé*, rapport [en ligne], 2023, fondant la stratégie nationale de réutilisation des données de santé 2025-2028 (consulté le 30/05/2026).

Commission nationale de l'informatique et des libertés, *Le Système national des données de santé (SNDS)* [en ligne] (consulté le 30/05/2026).

Plateforme des données de santé (*Health Data Hub), Missions et projet HealthData@EU Pilot* [en ligne] (consulté le 30/05/2026).

Ministère chargé de la santé / Agence du numérique en santé, *Certification des hébergeurs de données de santé (HDS)* [en ligne] (consulté le 30/05/2026).

Agence nationale de la sécurité des systèmes d'information, *SecNumCloud : référentiel d'exigences pour les prestataires de services d'informatique en nuage* [en ligne] (consulté le 30/05/2026).

Agence du numérique en santé, *Ségur du numérique en santé* [en ligne] (consulté le 30/05/2026).

Agence nationale de la sécurité des systèmes d'information, *Référentiel cyber France (ReCyF)* [en ligne], 2026 (consulté le 30/05/2026).

Comité consultatif national d'éthique et Comité national pilote d'éthique du numérique, *Avis n° 141 du CCNE et n° 4 du CNPEN, « Diagnostic médical et intelligence artificielle : enjeux éthiques »* [en ligne], novembre 2022 (consulté le 30/05/2026).

IV. Normes et standards techniques

HL7 International, *HL7 FHIR, Fast Healthcare Interoperability Resources* [en ligne] (consulté le 30/05/2026).

Observational Health Data Sciences and Informatics, *OMOP Common Data Model* [en ligne] (consulté le 30/05/2026).

OpenEHR International, *openEHR Specifications* [en ligne]. Standard ouvert de modélisation et de persistance du dossier de santé (consulté le 30/05/2026).

Organisation internationale de normalisation, *NF EN ISO/IEC 27001:2023, Systèmes de management de la sécurité de l'information* [en ligne] (consulté le 30/05/2026).

Droit belge

Soutien financier à l'utilisation de la télématique et des dossiers médicaux électroniques par les médecins

L'arrêté royal du 25 juillet 2025 modifie le régime applicable à l'intervention financière accordée aux médecins pour l'utilisation de la télématique et la gestion électronique des dossiers médicaux. Il actualise plusieurs critères conditionnant l'octroi de cette intervention, notamment en lien avec l'utilisation effective des outils numériques de santé, de la facturation électronique, des services MyCareNet ainsi que du partage sécurisé des données de santé. Le dispositif s'inscrit dans la politique de numérisation des pratiques médicales et de renforcement de l'interopérabilité des systèmes d'information en santé.

Arrêté royal modifiant l'arrêté royal du 30 juin 2017 fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux médecins pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux, *M.B* du 25/07/2025.

Extension du soutien financier aux sage-femmes pour l'utilisation de la télématique

L'arrêté royal du 30 octobre 2025 fixe les conditions dans lesquelles les sage-femmes peuvent bénéficier d'une intervention financière de l'INAMI pour l'utilisation de la télématique et la gestion électronique des dossiers des patientes. Le dispositif est subordonné à plusieurs conditions relatives à l'activité professionnelle, à l'adhésion à la convention nationale ainsi qu'à l'utilisation effective d'outils numériques et de la facturation électronique. Cette mesure participe à l'intégration des sage-femmes dans la stratégie de numérisation des soins et au développement des usages numériques au sein des professions de santé.

Arrêté royal fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux sage-femmes pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux en 2025, *M.B* du 30/10/2025.

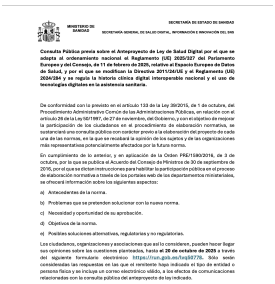
Droit espagnol

Resolución de 1 de diciembre de 2025, de la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, por la que se publica el Convenio con la Sociedad Española de Informática de la Salud, para impulsar la transformación digital del Sistema Nacional de Salud, « BOE » núm. 294, de 08/12/2025

Cette résolution, publiée au Bulletin officiel du 8 décembre 2025, rend publique une convention de coopération conclue entre la Direction générale de la santé numérique et des systèmes d'information du Système national de santé espagnol et la Société espagnole d'informatique de santé (SEIS). L'accord vise à soutenir la transformation numérique du système de santé espagnol au moyen d'actions conjointes de réflexion, d'expertise, de formation et de diffusion des connaissances. Il porte notamment sur l'interopérabilité des systèmes d'information, la gouvernance des données de santé, l'intelligence artificielle, la cybersécurité et les services numériques de santé.

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (SEIS)

Fondée en 1977, la Société espagnole d'informatique de santé (SEIS) est une association scientifique et professionnelle dédiée au développement du numérique en santé en Espagne. Elle réunit des professionnels de santé, experts en systèmes d'information, chercheurs, administrations publiques et entreprises du secteur afin de promouvoir l'innovation, l'interopérabilité et la transformation numérique du système de santé.



MINISTERIO DE SANIDAD

SECRETARÍA DE ESTADO DE SANIDAD

SECRETARÍA GENERAL DE SALUD DIGITAL, INFORMACIÓN E INNOVACIÓN DEL SNS

Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

De conformidad con lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en relación con el artículo 26 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y con el objetivo de mejorar la participación de los ciudadanos en el procedimiento de elaboración normativa, se sustanciará una consulta pública con carácter previo a la elaboración del proyecto de cada una de las normas, en la que se recabará la opinión de los sujetos y de las organizaciones más representativas potencialmente afectados por la futura norma.

En cumplimiento de lo anterior, y en aplicación de la Orden PRE/1590/2016, de 3 de octubre, por la que se publica el Acuerdo del Consejo de Ministros de 30 de septiembre de 2016, por el que se dictan instrucciones para habilitar la participación pública en el proceso de elaboración normativa a través de los portales web de los departamentos ministeriales, se ofrecerá información sobre los siguientes aspectos:

a) Antecedentes de la norma.

b) Problemas que se pretenden solucionar con la nueva norma.

c) Necesidad y oportunidad de su aprobación.

d) Objetivos de la norma.

e) Posibles soluciones alternativas, regulatorias y no regulatorias.

Los ciudadanos, organizaciones y asociaciones que así lo consideren, pueden hacer llegar sus opiniones sobre las cuestiones planteadas, hasta **el 20 de octubre de 2025** a través del siguiente formulario electrónico https://sun.gob.es/bsg59776. Solo serán consideradas las respuestas en las que el remitente haya indicado el tipo de entidad o persona física y en incluya un correo electrónico válido, a los efectos de comunicaciones relacionadas con la consulta pública del anteproyecto de ley indicado.

Consultation publique sur l'avant-projet de loi relatif à la santé numérique

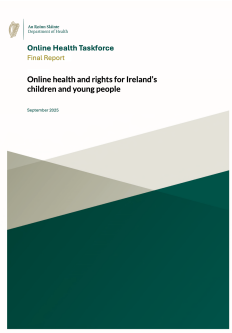
Le ministère espagnol de la Santé lance une consultation publique en vue de l'élaboration d'un avant-projet de loi destiné à adapter le droit espagnol au règlement (UE) 2025/327 relatif à l'Espace européen des données de santé (EHDS). Le texte ne se limite toutefois pas à cette adaptation. Il poursuit plus largement l'objectif de consolider le cadre juridique espagnol en matière de santé numérique et de l'articuler avec les nouvelles exigences européennes. **La consultation publique s'est déroulée du 22 septembre au 20 octobre 2025**.

L'avant-projet prévoit notamment :

- le renforcement de l'interopérabilité de l' « histoire clinique numérique » (« *historia clínica digital interoperable* ») ;
- l'amélioration de l'accès et du contrôle des patients sur leurs données de santé électroniques ;
- l'organisation d'une gouvernance nationale et régionale des données de santé ;
- l'intégration de l'Espagne aux infrastructures européennes prévues par l'EHDS ;
- l'encadrement de l'utilisation des technologies numériques dans le domaine sanitaire, notamment l'intelligence artificielle, la biométrie et les neurotechnologies.

Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

Droit irlandais



Department of Health (An Roinn Sláinte), *Online Health Taskforce. Final Report : Online health and rights for Ireland's children and young people*, September 2025

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Instituée en septembre 2024 par le ministère de la Santé irlandais (*Department of Health*) et présidée par l'ancienne sénatrice Jillian van Turnhout, l'Online Health Taskforce (ci-après « OHT ») a remis un rapport final daté de septembre 2025, que la ministre de la Santé Jennifer Carroll MacNeill a rendu public le 12 décembre 2025[240]. Ce rapport propose, dans une perspective de santé publique, une réponse aux défis auxquels sont confrontés les enfants et les jeunes dans l'environnement numérique. Les travaux se sont appuyés sur une *National Youth Assembly on Youth Online Health* tenue le 9 juillet 2025, sur une consultation des parties prenantes qui a recueilli 86 contributions, sur un rapport de l'*Institute of Public Health* consacré à l'exposition des enfants au marketing en ligne de produits nocifs pour la santé,

Established in September 2024 by the Department of Health (*An Roinn Sláinte*) and chaired by former Senator Jillian van Turnhout, the Online Health Taskforce (hereinafter 'OHT') delivered a final report dated September 2025, which the Minister for Health, Jennifer Carroll MacNeill, made public on 12 December 2025[249]. The report sets out, from a public health perspective, a response to the challenges facing children and young people in the digital environment. The work drew upon a *National Youth Assembly on Youth Online Health* held on 9 July 2025, a stakeholder consultation which received 86 submissions, a report by the *Institute of Public Health* on children's exposure to the online marketing of health-harming products, and a review of the international scientific literature. The whole is structured around four

[240] Online Kealth Taskforce, Final Report: Online health and rights for Ireland's children and young people, Department of Health, sept. 2025; Jennifer Carroll MacNeill (ministre de la Santé), communiqué de presse, gov.ie, 12 déc. 2025.

[249] Online Health Taskforce, *Final Report: Online Health and Rights for Ireland's Children and Young People* (Department of Health 2025); Jennifer Carroll MacNeill (Minister for Health), press release (gov.ie, 12 December 2025).

ainsi que sur une revue de la littérature scientifique internationale. L'ensemble s'articule autour de quatre principes fondateurs et de dix recommandations opérationnelles.

I. LES PRINCIPES FONDATEURS : LES DROITS DE L'ENFANT COMME BOUSSOLE

Des droits équivalents en ligne et hors ligne. Le premier principe repose sur une évidence qui reste largement à concrétiser. Dans l'environnement numérique, les enfants et les jeunes doivent bénéficier des mêmes droits que dans le monde physique : santé, vie privée, sécurité, participation, liberté d'expression, accès à l'information et à l'éducation, protection contre les préjudices. Le rapport se réclame ici directement de l'Observation générale n° 25 (2021) du Comité des droits de l'enfant des Nations Unies[241], laquelle avait fixé le cadre.

Cohérence, coopération, agilité. Les trois autres principes prolongent cette exigence. Il est demandé au gouvernement d'assurer une cohérence entre stratégies publiques, cadres législatifs et mécanismes de financement, afin que les espaces en ligne comme hors ligne offrent aux mineurs les conditions de leur épanouissement. Le rapport appelle par ailleurs l'Irlande à porter ces enjeux au niveau international. Enfin, la Taskforce insiste sur la nécessité d'une recherche suffisamment agile pour suivre le rythme des évolutions technologiques.

Les dix recommandations opérationnelles qui suivent se répartissent en cinq domaines d'action.

Le premier insiste sur la nécessité d'une approche fondée sur les droits des enfants et des jeunes, supposant en particulier une co-construction des

foundational principles and ten operational recommendations.

I. THE FOUNDATIONAL PRINCIPLES : CHILDREN'S RIGHTS AS GUIDING COMPASS

Equivalent rights online and offline. The first principle rests on a proposition that remains largely to be put into practice. In the digital environment, children and young people should enjoy the same rights as those afforded to them in the physical world: health, privacy, safety, participation, freedom of expression, access to information and education, as well as protection from harm. The report draws here directly on General Comment No. 25 (2021) of the UN Committee on the Rights of the Child[250], which had set the framework.

Coherence, cooperation, agility. The three other principles take this requirement further. Government is required to ensure coherence across public strategies, legislative frameworks and funding mechanisms, so that both online and offline spaces offer minors the conditions for their development. The report also calls on Ireland to champion these issues at the international level. Finally, the Taskforce insists on the need for a research agenda capable of keeping pace with the speed of technological change.

The ten operational recommendations that follow fall within five areas of action.

The first stresses the need for a children's and young people's rights-based approach, which supposes in particular that solutions be co-designed with minors themselves. The second concerns safety by design, coupled with the introduction of a legally binding age-

[241] Comité des droits de l'enfant des Nations Unies, Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique, CRC/C/GC/25, 2 mars 2021.
[250] UN Committee on the Rights of the Child, 'General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment' UN Doc CRC/C/GC/25 (2 March 2021).

solutions avec les mineurs eux-mêmes. Le deuxième concerne la sécurité dès la conception (*Safety by Design*), qu'accompagne la mise en place d'un système de classification par âge juridiquement contraignant. Le troisième porte sur la littératie numérique critique, que le rapport entend déployer dans l'ensemble du système éducatif. Le quatrième, consacré à l'application effective du droit et à la responsabilité, cible spécifiquement les systèmes de recommandation algorithmique. Quant au cinquième, il traite de l'articulation avec la réglementation européenne et nationale.

II. L'ARTICULATION AVEC LE DROIT DE L'UNION EUROPEENNE

A. Le DSA comme socle, le Digital Fairness Act comme perspective

Le règlement n° 2022/2065/UE du 19 octobre 2022 relatif au marché unique des services numériques[242] (ci-après « DSA »), applicable en Irlande depuis février 2024, constitue le socle du raisonnement. La recommandation n° 3 invite l'Irlande à plaider, à l'échelle européenne, pour que les fournisseurs de produits et services numériques intègrent les principes de *Child Rights by Design* dans la conception de leurs services et algorithmes. Sont visées ici les lignes directrices adoptées par la Commission européenne en juillet 2025 sur le fondement de l'article 28 du DSA, lequel est consacré à la protection des mineurs en ligne[243].

La question des systèmes de recommandation algorithmique est au

classification system. The third addresses critical digital literacy, which the report proposes to roll out across the entire education system. The fourth, devoted to enforcement and accountability, specifically targets recommender systems. As for the fifth, it concerns the articulation between EU and national regulation.

II. ARTICULATION WITH EU LAW

A. The DSA as foundation, the Digital Fairness Act as horizon

Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services[251] (hereinafter 'DSA'), in force in Ireland since February 2024, forms the starting point of the reasoning. Recommendation 3 calls on Ireland to advocate, at European level, for all providers of digital products and services to embed Child Rights by Design principles into the design of their services and algorithms. The intended reference point here is the guidance adopted by the European Commission in July 2025 on the basis of Article 28 of the DSA, which addresses the protection of minors online[252].

The question of recommender systems lies at the heart of Recommendation 6, which calls on platforms to put in place effective risk-mitigation measures, and on regulators to enforce the obligations arising under the DSA, particularly as regards the swift removal of illegal content. The Taskforce goes one step further: should platforms fail to comply with both the DSA and the *Online Safety and Media Regulation Act 2022* (OSMRA), the liability exemption

[242] 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 n° 2000/31/CE (règlement sur les services numériques), *JOUE* n° L 277 du 27/10/2022.
[243] Commission européenne, G*uidelines on the protection of minors online under Article 28(1) of the Digital Services Act*, *C(2025)* 4613 final, 14 juillet 2025.
[251] Regulation n° 2022/2065/EU of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] *OJ* L277/1.
[252] European Commission, 'Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act' *C(2025)* 4613 final (14 July 2025).

cœur de la recommandation n° 6, qui appelle les plateformes à mettre en œuvre des mesures effectives d'atténuation des risques, et les régulateurs à faire respecter le DSA, notamment s'agissant du retrait rapide des contenus illicites. La Taskforce pousse le raisonnement un cran plus loin : à défaut pour les plateformes de respecter le DSA et l'*Online Safety and Media Regulation Act 2022* (OSMRA), l'exonération de responsabilité dont elles bénéficient pour les contenus préjudiciables mais légaux mériterait, selon lui, d'être reconsidérée. La prise de position n'est pas anodine. Elle traduit une forme de tension entre l'approche européenne, largement centrée sur les obligations de transparence et d'évaluation des risques systémiques qui pèsent sur les très grandes plateformes (*VLOPs*/*VLOSEs*), et l'ambition irlandaise d'aller au-delà de la seule modération de contenu, pour s'attaquer à la conception même des services. L'Organisation mondiale de la santé (OMS) avait d'ailleurs, dans ses travaux de 2025 consacrés aux déterminants numériques de la santé mentale des jeunes[244], noté cette inflexion, relevant que l'Irlande s'intéressait désormais aux « *addictive design features* » [« caractéristiques de conception addictive »] des plateformes.

La présidence irlandaise du Conseil et le Digital Fairness Act. Le rapport ne se limite pas à une lecture du droit en vigueur. Par sa recommandation n° 9, il exhorte le gouvernement irlandais à se saisir de la présidence du Conseil de l'Union européenne, qui débutera en juillet 2026, pour favoriser une convergence des politiques nationales en la matière. La recommandation n° 10, enfin, soutient le projet de *Digital Fairness Act* (DFA), qui vise à combler les lacunes du droit de la consommation

they benefit from for harmful but legal content ought, in its view, to be reconsidered. That position is a significant one. It reflects a genuine tension between the European approach, which is largely built around transparency obligations and systemic risk assessments imposed on very large platforms (*VLOPs*/*VLOSEs*), and the Irish ambition to move beyond content moderation alone and address the very design of the services themselves. The World Health Organization, in its 2025 work on the digital determinants of youth mental health[253], had already noted this shift, observing that Ireland was now turning its attention to the 'addictive design features' of platforms.

The Irish Presidency of the Council and the Digital Fairness Act. The report does not confine itself to a reading of the existing law. Through Recommendation 9, it urges the Irish Government to seize upon its forthcoming Presidency of the Council of the European Union, which will begin in July 2026, as an opportunity to foster convergence among national policies in this field. Recommendation 10, for its part, supports the *Digital Fairness Act* (DFA) project, which aims to close the gaps left by existing consumer law in tackling online commercial practices. Ireland advocates an ambitious reading: a self-standing regulation conceived as the 'digital twin' of the Unfair Commercial Practices Directive, carrying a general prohibition on unfair digital commercial practices as well as an explicit ban on targeted advertising directed at minors on the basis of sensitive data within the meaning of Article 9 of the GDPR. The report thereby draws, once again, a bridge between consumer protection, personal-data protection and the protection of minors.

[244] Organisation mondiale de la santé (Bureau régional de l'Europe), *Commercial determinants of youth mental health: a policy brief*, OMS, 2025.
[253] World Health Organization Regional Office for Europe, *Commercial Determinants of Youth Mental Health: A Policy Brief* (WHO 2025)

face aux pratiques commerciales en ligne. L'Irlande y défend une lecture ambitieuse : un règlement autonome, conçu comme le « jumeau numérique » de la directive sur les pratiques commerciales déloyales, qui prohiberait les pratiques numériques déloyales et interdirait expressément la publicité ciblée adressée aux mineurs sur la base de données sensibles au sens de l'article 9 du RGPD. Voilà qui fait le pont, déjà esquissé ailleurs dans le texte, entre protection des consommateurs, protection des données à caractère personnel et protection des mineurs.

B. Les convergences avec le règlement européen sur l'IA

Bien que le rapport ne se présente pas comme un texte de transposition du règlement n° 2024/1689/UE du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle[245] (ci-après « RIA » ou « AI Act »), il en croise nettement les préoccupations. Les systèmes de recommandation algorithmique y sont traités comme l'une des sources majeures de risques pour les mineurs : le rapport les définit comme des systèmes d'IA qui profilent le comportement des individus pour déterminer les contenus qui leur sont présentés, afin de maximiser leur engagement. Or cette qualification fonctionnelle n'est pas sans effet au regard du RIA. Appliqués à des enfants, de tels systèmes peuvent basculer dans la catégorie des pratiques manipulatoires prohibées par l'article 5 ; à défaut, ils relèveront au minimum des systèmes à haut risque, avec évaluation de conformité associée.

Le rapport accorde à l'IA générative une attention particulière en relevant la multiplication des contenus d'abus

B. Convergences with the EU AI Regulation

Although the report does not present itself as a text of transposition of Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence[254] (hereinafter 'AI Act'), it clearly intersects with the European legislator's concerns. Recommender systems are treated as one of the main sources of risk to minors: the report defines them as AI systems that profile individuals' behaviour in order to determine what content is shown to them, with a view to maximising engagement. Now that functional classification is not without consequence under the AI Act. When applied to children, such systems may fall within the category of manipulative practices prohibited by Article 5; failing that, they will qualify, at the very least, as high-risk systems subject to conformity assessment.

Generative AI receives particular attention from the report, which notes the rise in AI-generated child sexual abuse material, as well as the emergence of *chatbots* that form pseudo-relationships with children, sometimes of a sexual nature, and give them misleading advice, including in the field of mental health. The *National Youth Assembly* calls, in that context, for the creation and distribution of *deepfakes* to be banned. That request aligns with the transparency obligations which Article 50 of the AI Act now imposes on systems generating synthetic content. Departing from the established instruments, the report finally suggests an original avenue: that of a Digital Child Safety Certification, inspired by the CE marking applied to physical toys[255]. Such a scheme could, in time, dovetail with the conformity

[245] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, *JOUE* n° L 2024/1689, 12 juill. 2024.
[254] Regulation n° 2024/1689/EU of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] *OJ* L2024/1689
[255] Council Directive 88/378/EEC of 3 May 1988 on the approximation of the laws of the Member States concerning the safety of toys [1988] OJ L187/1; Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] *OJ* L170/1.

sexuels sur mineurs générés par IA, ainsi que le développement de *chatbots* qui nouent avec les enfants de fausses relations, parfois à dimension sexuelle, et leur prodiguent des conseils erronés, y compris dans le champ de la santé mentale. La *National Youth Assembly* demande, dans ce contexte, que soit prohibée la création et la diffusion de *deepfakes* ; l'exigence converge avec les obligations de transparence que l'article 50 du RIA impose désormais aux systèmes générant des contenus synthétiques. À rebours des textes existants, le rapport propose enfin une piste originale : celle d'une *Digitale Child Safety Certification*, inspirée du marquage CE applicable aux jouets physiques[246]. Ce dispositif pourrait, à terme, entrer en dialogue avec les procédures d'évaluation de conformité que le RIA prévoit pour les systèmes à haut risque, et ouvrir la voie à une certification intégrée des produits numériques destinés aux mineurs.

C. Le cadre national et le rôle du Coimisiún na Meán

L'Irlande n'est pas démunie face à ces enjeux. L'OSMRA[247] avait déjà, en 2022, institué le Coimisiún na Meán en tant que régulateur de la sécurité en ligne, et introduit un *Online Safety Code* imposant certaines obligations aux plateformes de partage de vidéos établies sur le territoire, particulièrement en matière de vérification d'âge. Plusieurs limites sont cependant pointées du doigt par le rapport. Le champ d'application du dispositif, d'abord, reste étroit et ne couvre qu'une catégorie restreinte de services numériques. La marge d'appréciation laissée aux plateformes, ensuite, apparaît excessive.

Renforcer les moyens et les pouvoirs du Coimisiún na Meán. La

assessment procedures that the AI Act provides for high-risk systems and pave the way for integrated certification of digital products designed for minors.

C. The national framework and the role of Coimisiún na Meán

Ireland is not ill-equipped when it comes to these issues. The OSMRA[256] had already, in 2022, established Coimisiún na Meán as the online safety regulator, and introduced an *Online Safety Code* imposing certain obligations on video-sharing platforms established in Ireland, particularly in relation to age verification. Several shortcomings are nevertheless identified by the report. The scope of the framework, first, remains narrow and covers only a limited category of digital services. The margin of appreciation left to platforms, further, appears excessive.

Strengthening the resources and powers of Coimisiún na Meán. Recommendation 7 calls for the regulator to be given adequate resources, both financial and human. It further suggests conferring upon it broader powers. Among those envisaged are the possibility of geo-blocking online services and VPNs, the option to conditionally disable recommender algorithms as regards minors, and the implementation of robust age verification at the national level, in cooperation with other European regulators and the Commission.

A personal liability for directors and officers. Recommendation 8 is more ambitious still. Drawing inspiration from the precedent set by the *Data Protection Act 2018*[257] in the field of data protection, it proposes amending the OSMRA in order to introduce personal liability for directors and officers of companies

[246] Directive n° 88/378/CEE du Conseil du 3 mai 1988 concernant le rapprochement des législations des États membres relatives à la sécurité des jouets, *JOUE* n° L 187 du 16/07/1988 ; Directive n° 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets, *JOUE* n° L 170 du 30/06/2009.
[247] Irlande, *Online Safety and Media Regulation Act 2022*, Act n° 41 of 2022, promulguée le 10 décembre 2022.
[256] Online Safety and Media Regulation Act 2022.
[257] Data Protection Act 2018, ss 146 and 149.

recommandation n° 7 appelle à doter le régulateur de ressources adéquates, financières comme humaines. Elle suggère également de lui conférer des pouvoirs élargis. Sont notamment visés la possibilité de procéder au géo-blocage de services en ligne et de VPN, celle de désactiver conditionnellement les algorithmes de recommandation à l'égard des mineurs, ou encore la mise en œuvre d'une vérification d'âge robuste au niveau national, en coopération avec les autres régulateurs européens et la Commission.

Une responsabilité personnelle des dirigeants. La recommandation n° 8 est plus audacieuse encore. S'inspirant du précédent établi par le *Data Protection Act 2018*[248] en matière de données, elle propose de modifier l'OSMRA pour instituer une responsabilité personnelle des dirigeants et administrateurs d'entreprises fournissant des produits et services numériques, en cas de manquement aux réglementations de sécurité en ligne affectant la santé, la sécurité ou le bien-être des enfants et des jeunes. La proposition prend place dans un débat européen plus vaste sur la responsabilisation des décideurs au sein des entreprises technologiques.

III. PORTEE DU RAPPORT

Le rapport de l'OHT se distingue par son parti pris : aborder la sécurité en ligne comme une question de santé publique, et non comme un simple problème de régulation des contenus. Il prend d'ailleurs expressément ses distances avec l'idée d'une interdiction générale des smartphones pour les enfants, jugée « trop grossière comme instrument ». Le modèle qu'il propose combine au contraire régulation structurelle des plateformes, littératie numérique et autonomisation des mineurs.

providing digital products and services, where their undertaking breaches online safety regulations affecting the health, safety and wellbeing of children and young people. The proposal fits into the broader European debate on the accountability of decision-makers within technology companies.

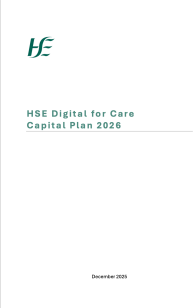
III. SCOPE OF THE REPORT

What sets the OHT report apart is its approach: to treat online safety as a public health issue rather than a narrow problem of content regulation. It explicitly distances itself from the idea of a blanket ban on smartphones for children, deemed 'too blunt an instrument'. The model it puts forward combines instead the structural regulation of platforms, digital literacy and the empowerment of minors.

This report thus illustrates in a remarkable way how a Member State transposes and extends, through soft law instruments, the requirements of the DSA, the GDPR and the AI Act. The recommendations it sets out moreover foreshadow the debates of the forthcoming Irish Presidency of the Council of the European Union (commencing in July 2026), which could thereby elevate the digital health of minors to the status of a European political priority. The digital safety certification of children and the conditional disabling of recommendation algorithms already provide a number of illustrations of this.

[248] Irlande, *Data Protection Act 2018*, Act n° 7 of 2018, sections 146 et 149 (responsabilité personnelle des dirigeants en cas de manquement commis avec leur consentement, leur complicité ou imputable à leur négligence).

Ce rapport montre ainsi de façon remarquable comment un État membre transpose et prolonge, au moyen d'instruments de soft law, les exigences du DSA, du RGPD et du RIA. Les recommandations formulées préfigurent par ailleurs les débats de la prochaine présidence irlandaise du Conseil de l'Union européenne (à compter de juillet 2026), laquelle pourrait ainsi élever la santé numérique des mineurs au rang de priorité politique européenne. La certification de sécurité numérique des enfants ou la désactivation conditionnelle des algorithmes de recommandation en offrent déjà quelques illustrations.





Health Service Executive (HSE), *Digital for Care Capital Plan 2026*, December 2025
et
Department of Health (An Roinn Sláinte), *National Development Plan Review 2025 – Sectoral Investment Plan : Department of Health 2026–2030*, July 2025

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

En l'espace de quelques mois, la santé numérique irlandaise s'est dotée de deux instruments de planification complémentaires qu'il convient de lire ensemble. L'un fixe l'enveloppe de l'année 2026. L'autre en trace la trajectoire pluriannuelle.

Le plan annuel pour 2026. Publié par le *Health Service Executive* (HSE) en décembre 2025, le *Digital for Care Capital Plan 2026* est l'instrument annuel d'investissement numérique en santé. Il découle directement de la stratégie-cadre *Digital for Care: A Digital Health Framework for Ireland 2024–2030*[258], approuvée par le gouvernement et intégrée à la réforme *Sláintecare*. L'enveloppe prévue pour 2026 s'élève à 263 millions d'euros (contre 190 M€ en 2025), dont 70 % fléchés vers les projets de transformation.

Parmi ces projets, plusieurs méritent l'attention. Le dossier patient électronique national (*HSE One Health Record – NEHR*, 36 M€) en constitue le premier poste d'investissement, en vue d'un déploiement dans les six régions sanitaires. On peut citer également l'application mobile *HSE Health App* (mise à disposition du public depuis février 2025), laquelle intègre un

Within the space of a few months, Irish digital health has been equipped with two complementary planning instruments which should be read together. The first sets the financial envelope for 2026. The second maps out its multiannual trajectory.

The annual plan for 2026. Published by the *Health Service Executive* (HSE) in December 2025, the *Digital for Care Capital Plan 2026* is the annual instrument of digital investment in health. It flows directly from the overarching strategy *Digital for Care: A Digital Health Framework for Ireland 2024–2030*[262], which was approved by Government and is integrated into the *Sláintecare* reform. The envelope provided for 2026 comes to €263 million (as against €190 million for 2025), of which 70 percent is earmarked for transformation projects.

Among those projects, several deserve attention. The national electronic patient record (*HSE One Health Record – NEHR*, €36 million) constitutes its leading investment line, with a view to deployment across the six health regions. Mention may also be made of the *HSE Health App* mobile application (made available to the public from February 2025), which carries an explicit

[258] Department of health (Irlande), Digital for Care: A Digital Health Framework for Ireland 2024–2030, Department of Health, May 2024.
[262] Department of Health, *Digital for Care: A Digital Health Framework for Ireland 2024–2030* (Department of Health 2024).

engagement explicite en matière d'obligations européennes (MyHealth@EU/EEDS). S'y ajoutent le dossier de soins partagé (*Shared Care Record*), la prescription électronique (*ePrescribing*), les soins virtuels et le télésuivi, le déploiement de solutions d'IA conformes à la stratégie *AI for Care* (identification d'AVC, radiologie, échocardiogrammes), ainsi qu'un volet cybersécurité adossé à la directive NIS 2[259].

Ce plan illustre bien la dynamique d'intégration du système de santé irlandais dans l'architecture européenne. La référence à MyHealth@EU rattache en effet l'Irlande au dispositif de l'espace européen des données de santé[260] (EEDS). L'*Individual Health Identifier* (IHI) institué par le *Health Identifiers Act 2014* anticipe, de son côté, les exigences d'identification transfrontalière posées par le règlement EEDS. Le volet cybersécurité prolonge enfin cette même dynamique du côté de la protection des systèmes d'information.

La trajectoire pluriannuelle à horizon 2030. Ce plan annuel ne prend tout son sens qu'à la lecture du plan sectoriel de santé publié en juillet 2025 dans le cadre de la révision du *National Development Plan* (NDP). Celui-ci alloue une enveloppe de 9,25 milliards d'euros aux infrastructures de santé et à la numérisation pour la période 2026–2030. Jamais l'État irlandais n'avait consenti un tel investissement en infrastructures de santé publique.
La section 3.3 du plan, intitulée « *Digital for Care* », décline les six principes de la

commitment in relation to European obligations (MyHealth@EU/EHDS). Added to this are the *Shared Care Record*, *ePrescribing*, virtual care and remote monitoring, the deployment of AI solutions aligned with the *AI for Care* strategy (stroke identification, radiology, echocardiograms), and a cybersecurity strand anchored on the NIS 2 Directive[263].

This plan illustrates the gradual integration of the Irish health system into the European digital health architecture. The reference to MyHealth@EU does in fact anchor Ireland within the apparatus of the European Health Data Space[264] (EHDS). The *Individual Health Identifier* (IHI) established by the *Health Identifiers Act 2014*, for its part, anticipates the cross-border identification requirements laid down by the EHDS Regulation. The cybersecurity strand, finally, extends the same dynamic on the side of information-system protection.

The multiannual trajectory to 2030. This annual plan only takes on its full meaning when read against the health sectoral plan published in July 2025 as part of the revision of the *National Development Plan* (NDP). The latter allocates an envelope of €9.25 billion to health infrastructure and digitalisation for the period 2026–2030. Never before has the Irish State committed such an investment in public health infrastructure.
Section 3.3 of the plan, entitled '*Digital for Care*', sets out the six principles of the overarching strategy adopted in May 2024: the patient as empowered partner, digital modernisation of the workplace, digitally connected care, data-driven services, the digital-health innovation

[259] Directive n° 2022/2555/UE 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 (directive NIS 2), *JOUE* n° L 333 du 27/12/2022.
[260] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive n° 2011/24/UE et le règlement (UE) 2024/2847, *JOUE* n° L 2025/327 du 5/03/2025.
[263] Directive n° 2022/2555/EU of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [2022] *OJ* L333/80
[264] Regulation n° 2025/327/EU of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] *OJ* L2025/327

stratégie-cadre adoptée en mai 2024 : le patient responsable de sa santé, la modernisation numérique du milieu de travail, les soins connectés, les services fondés sur les données, l'écosystème d'innovation en santé numérique et les fondations sécurisées. Le programme *Digitally Enabled and Connected Care*, qui concentre les financements dans le dossier de santé électronique national, la prescription électronique, le *National Shared Care Record* et les soins virtuels, est doté à lui seul d'une enveloppe supérieure à un milliard d'euros. Le volet *Secure Foundations & Digital Enablers* bénéficie quant à lui d'un investissement compris entre 500 millions et un milliard.

Sont identifiés expressément, comme moteurs réglementaires de cette transformation, les obligations découlant du règlement EEDS, de la directive NIS 2, du RIA et du *Health Information Act 2026*. Le plan est clair sur ce point : tout retard dans ces investissements exposerait l'Irlande à des risques de non-conformité. On mentionnera enfin l'ouverture, en 2026, du *National Children's Hospital Ireland* (NCHI), pensé comme le premier hôpital public entièrement numérique du pays : un jalon emblématique de la stratégie.

L'ampleur de l'effort consenti apparaît toutefois à la mesure du retard accumulé. Selon l'indicateur de la Décennie numérique 2025 relatif à l'accès aux dossiers de santé électroniques[261], l'Irlande occupe la dernière place (25 %) parmi les vingt-neuf pays évalués, loin de la moyenne européenne (83 %) et des 100 % atteints par l'Estonie, dont l'infrastructure X-Road est pourtant opérationnelle depuis 2001. Ce n'est donc pas tant d'un rattrapage qu'il s'agit que d'un démarrage, certes intensif.

ecosystem, and secure foundations. The *Digitally Enabled and Connected Care* programme, which funds the national electronic health record, ePrescribing, the *National Shared Care Record* and virtual care, is alone provided with an envelope exceeding one billion euros. The *Secure Foundations & Digital Enablers* strand, for its part, benefits from an investment of between €500 million and €1 billion.

The plan expressly identifies, as regulatory drivers of this transformation, the obligations flowing from the EHDS Regulation, the NIS 2 Directive, the AI Act and the *Health Information Act 2026*. The plan is unambiguous on this point: any delay in these investments would expose Ireland to non-compliance risks. Mention should finally be made of the opening, in 2026, of the *National Children's Hospital Ireland* (NCHI), conceived as the first fully digital public hospital in the country: an emblematic milestone within the strategy.

The scale of the commitment made is, however, commensurate with the scale of the lag accumulated. According to the Digital Decade 2025 indicator on access to electronic health records[265], Ireland occupies last place (with a score of 25 percent) among the twenty-nine countries assessed, a considerable distance from the European average (83 percent) and from the 100 percent reached by Estonia, whose X-Road infrastructure has nonetheless been operational since 2001. It is therefore less a matter of catching up than of a belated start, albeit one now pursued intensively.

[261] Communication de la Commission européenne sur l'état d'avancement de la décennie numérique, *COM(2025)*290 final du 16/06/2025.
[265] European Commission, 'Digital Decade Report 2025' SWD(2025) 290 (June,16 2025)/


Number 10 of 2026
Health Information Act 2026

Health Information Act 2026, No. 10 of 2026, signed into law by the President of Ireland on 30 April 2026

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Déposé en juillet 2024 par le *Ministère de la Santé* devant le *Dáil Éireann*, le *Health Information Bill 2024* (ci-après « HIA » ou « la loi ») a été longuement débattu et amendé, puis adopté en première lecture par le *Dáil Éireann* le 19 novembre 2025, avant d'être transmis devant le *Seanad Éireann*. Après examen et amendements, le texte a finalement été adopté par les deux chambres et promulgué par le Président de la République le 30 avril 2026 sous le titre de Health Information Act 2026 (n° 10 of 2026)[266].

La loi porte une ambition considérable. Elle se veut l'instrument par lequel l'Irlande donne effet, dans son ordre juridique interne, au règlement n° 2025/327/UE relatif à l'espace européen des données de santé (ci-après « EEDS » ou « règlement EHDS »). Le texte s'inscrit par ailleurs dans le prolongement du *Health Identifiers Act 2014*[267] et de la réforme *Sláintecare*, et confère au *Health Service Executive* (Direction des services de santé ; ci-après « HSE ») un rôle pivot dans l'architecture nationale de gestion des données de santé électroniques.

Introduced in July 2024 by the *Department of Health* to *Dáil Éireann*, the *Health Information Bill 2024* (hereinafter 'HIA' or 'the Act') was debated at length and amended, then passed at first reading by *Dáil Éireann* on 19 November 2025, before being referred to the *Seanad Éireann*. Following examination and amendments, the text was finally passed by both Houses and signed into law by the President of Ireland on 30 April 2026 under the title of Health Information Act 2026 (No. 10 of 2026)[273].

The Act carries considerable ambition. It is intended as the instrument by which Ireland gives effect, in its domestic legal order, to Regulation (EU) 2025/327 on the European Health Data Space (hereinafter 'EHDS' or 'EHDS Regulation'). The Act also fits within the line of the *Health Identifiers Act 2014*[274] and of the *Sláintecare* reform, and confers on the *Health Service Executive* (hereinafter 'HSE') a pivotal role in the national architecture governing electronic health data.

[266] Irlande, *Health Information Act 2026*, n° 10 of 2026 ; Bill n° 61 of 2024 déposé le 19 juill. 2024 devant le Dáil Éireann ; texte adopté en première lecture le 19 nov. 2025 et transmis devant le Seanad Éireann, promulgué par le Président de la République d'Irlande le 30 avril 2026.
[267] Irlande, *Health Identifiers Act 2014*, Act n° 15 of 2014.
[273] Health Information Act 2026 (No 10 of 2026); originating as the Health Information Bill 2024 (Bill No 61 of 2024) introduced on 19 July 2024 before Dáil Éireann; passed First Stage on 19 November 2025 and referred to Seanad Éireann; signed into law by the President of Ireland on 30 April 2026.
[274] Health Identifiers Act 2014.

I. L'OBLIGATION DE PARTAGE DES DONNEES DE SANTE (PARTIE 2)

La Partie 2 de la loi pose le principe d'un *duty to share* [« devoir de partage »] entre prestataires de soins. Aux termes de la section 7, tout prestataire qui assure le soin d'un patient est tenu de transmettre à ses confrères intervenant dans la même prise en charge les données de santé personnelles pertinentes, nécessaires et proportionnées, dans un format numérique conforme aux lignes directrices d'interopérabilité fixées par le HSE.

On reconnaîtra ici l'esprit du chapitre II du règlement EHDS, qui régit l'utilisation primaire des données de santé électroniques. Le droit du patient vient compléter le dispositif : la section 8 lui permet d'exiger le transfert gratuit de ses données vers un autre prestataire, dans un délai d'un mois. Ce délai s'aligne expressément sur celui de l'article 15 du RGPD[268] pour l'exercice du droit d'accès, et de l'article 20 du RGPD[269] pour l'exercice du droit à la portabilité. Des mesures de sauvegarde sont enfin prévues à la section 9 en cas de cessation d'activité d'un prestataire.

II. LE DOSSIER DE SANTE ELECTRONIQUE NATIONAL (PARTIE 3)

La Partie 3 constitue le cœur du dispositif de transposition. La section 10 habilite le HSE à créer, pour chaque patient, un dossier de santé électronique national (*Electronic Health Record*, ci-après « EHR »), après analyse d'impact relative à la protection des données (*data*

I. THE DUTY TO SHARE PERSONAL HEALTH DATA (PART 2)

Part 2 of the Act establishes the principle of a 'duty to share' among healthcare providers. Pursuant to section 7, any healthcare services provider responsible for the care of a patient is required to transmit to other providers involved in the patient's treatment the relevant, necessary and proportionate personal health data, in a digital format compliant with the interoperability guidelines laid down by the HSE.

The provision echoes the approach of Chapter II of the EHDS Regulation, which governs the primary use of electronic health data. The patient's own right completes the mechanism: section 8 allows the patient to request the free-of-charge transfer of their data to another provider, within one month. That timeframe expressly mirrors the one laid down by Article 15 of the GDPR[275] for the exercise of the right of access, and by Article 20 of the GDPR[276] for the axercise of the right to data portability. Finally, section 9 provides for safeguarding measures in the event of the cessation of activity of a provider.

II. THE NATIONAL ELECTRONIC HEALTH RECORD (PART 3)

Part 3 constitutes the core of the transposition framework. Section 10 empowers the HSE to create, for each patient, a national Electronic Health Record (hereinafter 'EHR'), following a data protection impact assessment conducted in consultation with the *Data Protection Commission* (DPC). Section

[268] 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 (règlement général sur la protection des données), *JOUE* n° L 119 du 4/05/2016.
[269] *Ibid*.
[275] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] *OJ* L119/1
[276] *ibid*

protection impact assessment) réalisée en concertation avec la *Data Protection Commission* (DPC). La section 10(3) apporte une précision importante : aucun patient ne pourra se voir refuser un service de santé au motif qu'il ne dispose pas d'un EHR. On retrouve ici la logique de l'article 3, paragraphe 10, du règlement EHDS, qui prohibe toute discrimination fondée sur l'exercice des droits relatifs aux données de santé.

Contenu du dossier de santé électronique (EHR). La section 11 dresse la liste des catégories de données appelées à figurer dans l'EHR. On y retrouve sans surprise les rubriques énumérées à l'article 14 et à l'annexe I du règlement EHDS : résumé patient, prescriptions, dispensations, imagerie médicale, résultats de laboratoire et lettres de sortie. Le législateur irlandais est cependant allé plus loin que le texte européen. Trois catégories supplémentaires sont expressément mentionnées : les données relatives aux maladies rares (intégration aux Réseaux européens de références[270]), celles qui portent sur le statut fonctionnel du patient, et celles que ce dernier fournit lui-même. Cet ajout anticipe les catégories prioritaires que le règlement EHDS prévoit de rendre accessibles à terme dans le cadre de MyHealth@EU.

Identification du patient. Elle repose sur le *personal public service number* (PPSN), numéro d'identification personnel utilisé par l'administration irlandaise. La section 12 impose son enregistrement par tout prestataire de santé, mais prohibe simultanément le refus de soins en cas d'absence de PPSN. Le mécanisme est destiné à assurer la liaison avec l'*Individual Health Identifier* (IHI) institué par le *Health Identifiers Act 2014*, dans la perspective des exigences d'identification

10(3) contains an important refinement: no patient may be refused a health service on the ground that they do not hold an EHR. One finds here the logic of Article 3(10) of the EHDS Regulation, which prohibits any discrimination based on the exercise of rights in relation to health data.

Content of the EHR. Section 11 lists the categories of data intended to be recorded in the EHR. One recognises here, unsurprisingly, the headings enumerated in Article 14 and Annex I of the EHDS Regulation: patient summary, e-prescriptions, e-dispensations, medical imaging, laboratory results, and discharge reports. The Irish legislator has, however, gone further than the European text. Three additional categories are expressly referred to: data relating to rare diseases (integrating European reference networks[277]), data concerning the functional status of the patient, and data provided by the patient themselves. That addition anticipates the priority categories that the EHDS Regulation is to make accessible in due course through MyHealth@EU.

Patient identification. It rests upon the Personal Public Service Number (PPSN), the personal identification number used by the Irish public administration. Section 12 requires its recording by every healthcare services provider while, at the same time, prohibiting the refusal of care in cases where no PPSN is available. The mechanism is intended to ensure articulation with the *Individual Health Identifier* (IHI) established by the *Health Identifiers Act 2014*, with a view to the cross-border identification requirements set down by the EHDS Regulation.

[270] Directive n° 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JOUE* n° L 88 du 4/04/2011, art. 12.
[277] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] *OJ* L88/45, art 12.

transfrontalière posées par le règlement EHDS.

III. L'ACCES AU DOSSIER ET LES DROITS DU PATIENT (SECTIONS 13 A 16)

Le régime d'accès à l'EHR a été pensé autour de quatre catégories de bénéficiaires : le patient lui-même ; une « personne appropriée » qui agit pour son compte (parent, tuteur, ou encore représentant décisionnel au sens de l'*Assisted Decision-Making (Capacity) Act 2015*[271]) ; le prestataire de soins, aux fins du traitement en cours ; enfin les agents du HSE (Health Service Executive ; Direction des services de santé), à des fins de maintenance technique.

La section 14 reconnaît au patient un droit de restreindre l'accès à tout ou partie de son EHR, à la condition qu'il ait reçu un avertissement explicite sur les conséquences potentielles de cette restriction sur sa prise en charge. Il s'agit d'un mécanisme d'*opt-out* qui reprend la logique de l'article 8 du règlement EHDS. Une exception a néanmoins été prévue : la section 14(4) permet l'accès aux données restreintes lorsque les intérêts vitaux du patient l'exigent, avec traçabilité et notification en retour. Soulignons enfin la mise en place, à la section 15, d'une notification automatique et en temps réel de tout accès à l'EHR, conformément à l'exigence de transparence portée par l'article 9, du règlement EHDS.

IV. L'UTILISATION PRIMAIRE ET SECONDAIRE DES DONNEES DE SANTE ELECTRONIQUE

La section 18 autorise le HSE à conclure des accords réciproques avec des prestataires établis dans des pays tiers, pour l'échange sécurisé d'informations contenues dans l'EHR, après consultation de la DPC (Data

III. ACCESS TO THE RECORD AND THE RIGHTS OF THE PATIENT (SECTIONS 13 TO 16)

The regime of access to the EHR has been designed around four categories of beneficiaries: the patient themselves; an 'appropriate person' acting on the patient's behalf (parent, guardian, or decision-making representative within the meaning of the *Assisted Decision-Making (Capacity) Act 2015*[278]); the healthcare services provider, for the purposes of the treatment in progress; and, finally, HSE personnel, for purposes of technical maintenance.

Section 14 recognises the patient's right to restrict access to all or part of their EHR, on condition that they have received an explicit warning as to the potential consequences of such restriction for their treatment. The mechanism is one of opt-out, which takes up the logic of Article 8 of the EHDS Regulation. An exception has nonetheless been provided for: section 14(4) permits access to restricted data where the patient's vital interests so require, with traceability and notification back to the patient. One should further underline the arrangement put in place at section 15, which provides for automatic, real-time notification of any access to the EHR, in line with the transparency requirement laid down by Article 9 of the EHDS Regulation.

IV. THE PRIMARY AND SECONDARY USE OF ELECTRONIC HEALTH DATA

Section 18 authorises the HSE to conclude reciprocal agreements with third-country healthcare providers for the secure exchange of information contained in the EHR, following consultation with the DPC. Here lies a

[271] Irlande, *Assisted Decision-Making (Capacity) Act 2015*, Act n° 64 of 2015.
[278] Assisted Decision-Making (Capacity) Act 2015.

Protection Commission ; Commission de protection des données). Voici une amélioration notable : l'Irlande prépare ainsi le terrain à une interconnexion avec MyHealth@EU qui pourrait, à terme, dépasser le seul cadre des États membres. La disposition vient compléter, de ce point de vue, l'article 14 du règlement EHDS sur l'accès transfrontalier.

La Partie 4 et l'utilisation secondaire. C'est le deuxième pan du dispositif. La Partie 4 de la loi encadre la collecte d'informations de santé par le HSE auprès de « personnes pertinentes », à des fins d'intérêt public : santé publique, planification des services et statistiques. Plusieurs garanties balisent le dispositif. Le texte exige en particulier une évaluation préalable de la nécessité de recourir à des données personnelles plutôt qu'anonymisées (section 22(4)), une analyse d'impact, une pseudonymisation, des mesures de limitation d'accès, ainsi qu'une formation ciblée des agents amenés à manipuler ces données. On notera, à cet égard, qu'au stade du Seanad le texte initial a été amendé pour supprimer la condition de subsidiarité qui imposait au HSE de démontrer, préalablement à toute demande, que les données ne pouvaient être obtenues par d'autres moyens en temps utile et de manière effective. La suppression de cette condition élargit sensiblement les pouvoirs de collecte du HSE à des fins secondaires et mérite d'être signalée. La définition de la « health information » à la section 2 a, dans le même mouvement, été étendue aux informations relatives à la fourniture et à l'évaluation des services de santé. Par ailleurs, les finalités d'utilisation secondaire visées aux sections 17(b)(ii) et 22(2) ont été élargies pour inclure « la planification intégrée des services, la gestion des performances et l'utilisation efficiente et efficace des ressources dans le domaine de la santé » ; ce dernier ajout n'étant pas neutre au regard des exigences de proportionnalité posées par l'article 9 du RGPD.

significant avenue: Ireland is in this way preparing the ground for an interconnection with MyHealth@EU that may, in time, extend beyond the sole framework of the Member States. The provision thus complements Article 14 of the EHDS Regulation on cross-border access.

Part 4 and secondary use. This is the second strand of the framework. Part 4 of the Act governs the collection of health information by the HSE from 'relevant persons', for public-interest purposes: public health, service planning, and statistics. Several safeguards frame the mechanism. The Act requires, in particular, a prior assessment of the necessity of resorting to personal data rather than anonymised data (section 22(4)), an impact assessment, pseudonymisation, access-restriction measures, and targeted training for officers who come to handle such data. It should be noted, in this regard, that at the Seanad stage the original text was amended so as to remove the subsidiarity-type condition which had required the HSE to demonstrate, prior to any request, that the data could not be obtained 'by alternative means in a timely and effective manner'. The removal of that condition appreciably widens the HSE's collection powers for secondary purposes, and deserves to be flagged. The definition of 'health information' at section 2 has, in the same vein, been extended to encompass information relating to the provision and evaluation of health services; and the secondary-use purposes referred to in sections 17(b)(ii) and 22(2) have been broadened to include 'integrated service planning, performance management and the efficient and effective use of resources in the area of health' — the latter addition not being a neutral one when measured against the proportionality requirements laid down by Article 9 of the GDPR.

The HSE may not, under any circumstances, re-identify the patients whose data have been collected (section 24(2)), and is to publish, every eighteen

Le HSE ne peut en aucun cas ré-identifier les patients dont les données ont été collectées (section 24(2)), et doit publier tous les dix-huit mois un rapport sur l'utilisation des données obtenues. On retrouve, en filigrane, les grandes lignes du chapitre IV du règlement EHDS consacré à l'utilisation secondaire, appuyées sur les bases juridiques nationales de traitement des données sensibles au sens de l'article 9, paragraphe 2, points g), h) et i), du RGPD.

On signalera enfin que la section 21, qui régit l'élaboration par le HSE des lignes directrices d'application de la loi, intègre désormais la *Health Information and Quality Authority* (HIQA) parmi les autorités obligatoirement consultées. L'ajout fait écho au rôle reconnu à la HIQA dans la stratégie *AI for Care* commentée infra, en particulier dans la préparation du *National Guidance for the Responsible and Safe Use of AI in Health and Social Care*.

On retiendra surtout de cette loi qu'elle place l'Irlande parmi les premiers États membres à avoir mené à terme un processus législatif formel de « mise en œuvre » du règlement EHDS, avant même l'expiration du délai d'application. L'utilisation primaire et l'utilisation secondaire des données de santé y sont articulées dans un cadre juridique unifié, qui tente de concilier les exigences d'interopérabilité européenne et les spécificités institutionnelles irlandaises, notamment le rôle pivot du HSE et l'ancrage sur le PPSN.

L'adoption définitive du texte clôt la trajectoire législative, mais ouvre celle, plus délicate encore, de la mise en œuvre. L'enjeu n'est pas mince : compte tenu du retard de l'Irlande déjà mesuré par l'indicateur de la Décennie numérique 2025 (v. supra)[272], l'ambition législative portée par la loi ne se traduira dans les faits qu'à la faveur d'un effort

months, a report on the use made of the data obtained. One recognises, in outline, the broad lines of Chapter IV of the EHDS Regulation concerning secondary use, supported by the national legal bases for the processing of sensitive data within the meaning of Article 9(2)(g), (h) and (i) of the GDPR.

It should finally be noted that section 21, which governs the elaboration by the HSE of the guidelines giving effect to the Act, now includes the *Health Information and Quality Authority* (HIQA) among the bodies that must be consulted. The addition echoes the role conferred on HIQA in the *AI for Care* strategy discussed below, in particular as regards the preparation of the *National Guidance for the Responsible and Safe Use of AI in Health and Social Care*.

Most notably, the Act places Ireland among the first Member States to have brought to completion a formal legislative process for the transposition of the EHDS Regulation, even before the expiry of the implementation deadline. Primary and secondary use of health data are articulated there within a unified legal framework, which seeks to reconcile the European interoperability requirements with the institutional specificities of Ireland, notably the pivotal role of the HSE and the reliance on the PPSN.

The final adoption of the text closes the legislative trajectory but opens the more delicate one of implementation. The stakes are not minor: given Ireland's considerable lag, as already measured by the 2025 Digital Decade indicator (see above)[279], the legislative ambition carried by the Act will only bear fruit in practice were accompanied by a technical implementation effort and a level of citizen take-up of an entirely different order.

[272] Commission européenne, *COM(2025)* 290 final, *préc.* ; *v. supra*, « Infrastructures numériques de santé ».
[279] European Commission, 'Digital Decade Report 2025' (n 13); *see further the discussion under 'Digital Health Infrastructure' above.*

d'implémentation technique et d'appropriation citoyenne d'une toute autre ampleur.



Department of Health (An Roinn Sláinte) & Health Service Executive (HSE), *AI for Care – The Artificial Intelligence (AI) Strategy for Healthcare in Ireland 2026–2030*, March 2026

par Thomas BOUDON

Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Fruit d'une commande conjointe du ministère de la Santé (*Department of Health*, ci-après « DoH ») et du HSE, la stratégie *AI for Care* est la toute première stratégie nationale irlandaise dédiée à l'intégration de l'intelligence artificielle dans le système de santé. Publiée en 2025 pour la période 2026–2030, elle donne corps à un engagement inscrit au *Programme for Government 2025*[280], lequel prévoyait l'élaboration d'une telle stratégie en cohérence avec le cadre *Digital for Care 2024–2030* et avec la réforme *Sláintecare*. Un *AI Implementation Framework* élaboré par le HSE, qui détaille les modalités opérationnelles de déploiement, vient compléter l'ensemble. Il s'agit de l'un des premiers exercices systématiques, par un État membre, d'articulation entre une politique sectorielle d'IA en santé et les exigences du RIA.

I. LES PRINCIPES DIRECTEURS : LA CONVERGENCE AVEC LE CADRE EUROPEEN

La vision affichée par *AI for Care* consiste à « exploiter l'IA de manière sûre et responsable pour transformer la manière dont nous dispensons des soins efficients et innovants ». Cette vision est étayée par six principes directeurs dont la convergence avec le RIA et, plus largement, l'approche européenne de l'IA digne de confiance est notable.

Jointly commissioned by the Department of Health (*An Roinn Sláinte*, hereinafter 'DoH') and the HSE, the *AI for Care* strategy is the very first national Irish strategy dedicated to the integration of artificial intelligence into the healthcare system. Published in 2025 for the period 2026–2030, it gives substance to a commitment inscribed in the *Programme for Government 2025*[284], which had provided for the development of such a strategy in alignment with the *Digital for Care 2024–2030* framework and with the *Sláintecare* reform. An *AI Implementation Framework* prepared by the HSE, setting out the operational arrangements for deployment, completes the package. This represents one of the first systematic exercises, by a Member State, in aligning a sectoral AI policy in healthcare with the requirements of the AI Act.

I. THE GUIDING PRINCIPLES : CONVERGENCE WITH THE EUROPEAN FRAMEWORK

The vision set out by *AI for Care* is to 'harness AI safely and responsibly to transform how we deliver efficient and innovative healthcare for patients and professionals'. That vision is underpinned by six guiding principles whose convergence with the AI Act and,

[280] Gouvernement d'Irlande, *Programme for Government: Securing Ireland's Future*, janvier 2025.
[284] *Programme for Government: Securing Ireland's Future* (Government of Ireland 2025.

Le principe *Person-Centred place* les résultats de santé et les besoins du public au cœur des décisions relatives à l'adoption de l'IA, tout en postulant un partenariat continu avec les patients. Le principe *Transparent and Trustworthy* fait directement écho aux obligations de transparence posées par les articles 13 et 14 du RIA pour les systèmes à haut risque. Le principe *Human in the Loop*, sans doute le plus significatif du point de vue juridique, emprunte la terminologie même du RIA, dont l'article 14 impose un contrôle humain effectif pour tout système à haut risque. Aussi la stratégie précise que l'IA doit « soutenir les professionnels de santé dans leur prise de décision médicale tout en gardant toujours le praticien au centre des soins au patient » : l'exigence juridique d'un contrôle humain adéquat se voit ainsi traduite dans le langage de la politique de santé.

Deux autres principes viennent prolonger cet alignement. Le principe *Governance and Safety* exige la conformité aux législations nationale et européenne applicables, RIA inclus. Quant au principe *Proven Benefit*, il engage à une évaluation continue des résultats mesurables de l'IA déployée. La stratégie rejoint ainsi l'exigence de surveillance post-commercialisation prévue à l'article 72 du RIA. La référence complémentaire aux principes éthiques de l'OMS[281] relatifs à l'IA pour la santé achève d'inscrire la démarche dans un cadre de gouvernance à plusieurs niveaux : national, européen et international.

more broadly, with the European approach to trustworthy AI, is striking.

The *Person-Centred* principle places health outcomes and the needs of the public at the heart of decisions relating to AI adoption, while postulating continuous partnership with patients. The *Transparent and Trustworthy* principle directly echoes the transparency obligations laid down by Articles 13 and 14 of the AI Act for high-risk systems. The *Human in the Loop* principle, doubtless the most significant from a legal standpoint, borrows the very terminology of the AI Act, Article 14 of which imposes effective human oversight for every high-risk system. The strategy accordingly specifies that AI must 'support clinicians in their clinical decision-making while keeping the clinician at the centre of patient care': the legal requirement of adequate human oversight is thus translated into the language of health policy.

Two further principles carry this alignment forward. The *Governance and Safety* principle demands compliance with applicable national and European legislation, the AI Act included. As for the *Proven Benefit* principle, it commits to ongoing assessment of the measurable outcomes of AI once deployed. The strategy thus meets the post-market monitoring requirement provided for at Article 72 of the AI Act. The complementary reference to the WHO's ethical principles[285] on AI for health completes the inscription of the endeavour within a layered governance framework: national, European and international.

[281] Organisation mondiale de la santé, Ethics and governance of artificial intelligence for health, OMS, Juin 2021 ; mis à jour en oct. 2023 pour intégrer les grands modèles multimodaux.
[285] World Health Organization, Ethics and Governance of Artificial Intelligence for Health (WHO 2021, updated October 2023).

II. QUATRE PILIERS STRATEGIQUES A LA LUMIERE DU RIA

A. AI for Clinical Care

C'est le pilier aux enjeux juridiques les plus denses. Il englobe l'imagerie médicale assistée par IA (détection de fractures, d'AVC, de tumeurs), l'aide à la décision clinique et la documentation clinique automatisée. La stratégie reconnaît expressément que bon nombre de ces solutions sont qualifiées d'« IA en tant que dispositif médical » (*AI-as-a-medical-device*) au titre du règlement n° 2017/745/UE[282] et qu'elles sont, à ce titre, traitées comme des systèmes à haut risque au sens de l'article 6, paragraphe 1, du RIA lu conjointement avec l'annexe I.

Les conséquences sont considérables. Ces solutions sont soumises aux obligations du chapitre III, section 2, du RIA. La gestion des risques (article 9) doit être établie et documentée. La gouvernance des données est encadrée à l'article 10. La documentation technique (article 11), la traçabilité des opérations (article 12), la transparence (article 13), le contrôle humain (article 14) et les exigences de robustesse, de précision et de cybersécurité (article 15) viennent compléter le dispositif. La stratégie mentionne par ailleurs les analyses d'impact sur les droits fondamentaux prévues à l'article 27 du RIA, ainsi que l'inscription des projets sur les registres d'IA visés à l'article 49.

Le rapport illustre sa démarche par une étude de cas intéressante : le déploiement de l'IA en radiologie, dans un hôpital universitaire irlandais, pour la détection de caillots sanguins et de fractures. Les résultats cités font état d'une amélioration du taux de détection des caillots de 100 %, le système opérant

II. FOUR STRATEGIC PILLARS IN LIGHT OF THE AI ACT

A. AI for Clinical Care

This is the pillar whose legal stakes run deepest. It encompasses AI-assisted medical imaging (detection of fractures, strokes, and tumours), clinical decision support, and automated clinical documentation. The strategy expressly acknowledges that a number of these clinical solutions qualify as 'AI-as-a-medical-device' within the meaning of Regulation (EU) 2017/745[286] and are, on that account, treated as high-risk systems within the meaning of Article 6(1) of the AI Act read in conjunction with Annex I.

The consequences are considerable. Those solutions are made subject to the obligations of Chapter III, Section 2, of the AI Act. A risk-management system must be established and documented (Article 9). Data and data governance are regulated at Article 10. Technical documentation (Article 11), record-keeping (Article 12), transparency (Article 13), human oversight (Article 14) and the requirements of accuracy, robustness and cybersecurity (Article 15) complete the framework. The strategy also refers to the fundamental rights impact assessments provided for at Article 27 of the AI Act, together with registration of projects in the EU database of AI systems referred to at Article 49.

The strategy illustrates its approach through an instructive case study: the deployment of AI in radiology, in an Irish teaching hospital, for the detection of blood clots and fractures. The figures cited report an improvement in the clot detection rate of 100 percent, the system operating in support of the radiologist rather than autonomously.

---

[282] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, *JOUE* n° L 117 du 5/05/2017.

[286] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] *OJ* L117/1.

toutefois en appui du radiologue et non de manière autonome.

B. AI for Operations

Ce pilier concerne l'amélioration de l'efficience opérationnelle du système. Sont envisagées l'automatisation des fonctions support (ressources humaines, finances, chaîne d'approvisionnement), la gestion prédictive de la demande et des capacités, l'automatisation des centres de contact, ou encore l'accélération du déploiement du dossier de santé électronique. À première vue, le profil de risque apparaît moindre que pour les applications cliniques. Il convient cependant de ne pas s'y méprendre. Certains usages (gestion prédictive du flux de patients, allocation automatisée des lits) sont susceptibles de relever de l'annexe III, point 5, du RIA relative aux systèmes à haut risque en matière de santé, dès lors qu'ils influent sur l'accès aux soins ou l'allocation des ressources.

C. AI for Research & Innovation

Le troisième pilier porte sur la mobilisation de l'IA pour accélérer la recherche médicale, optimiser les essais cliniques et améliorer l'audit clinique. Il soulève des questions juridiques spécifiques, notamment quant à l'articulation entre le RIA et le cadre de protection des données. L'utilisation de l'IA pour l'analyse de grands volumes de données de santé ou pour le recrutement automatisé de patients implique en effet, par hypothèse, un traitement au sens de l'article 9 du RGPD. La stratégie prévoit d'ailleurs une rationalisation des procédures de conformité, la préparation des analyses d'impact relatives à la protection des données (AIPD, *DPIA*) figurant parmi les actions prioritaires, ce qui ouvre un champ d'articulation avec le chapitre IV du règlement EHDS relatif à l'utilisation secondaire des données de santé.

B. AI for Operations

This pillar concerns the improvement of the operational efficiency of the system. It contemplates the automation of support functions (human resources, finance, supply chain), predictive management of demand and capacity, the automation of contact centres, and the acceleration of the roll-out of the electronic health record. At first sight, the risk profile appears lower than that of clinical applications. It is advisable, however, not to be misled. Certain uses (predictive management of patient flow, automated bed allocation) are liable to fall within Annex III, point 5, of the AI Act concerning high-risk systems in the health domain, where they influence access to care or the allocation of resources.

C. AI for Research & Innovation

The third pillar concerns the mobilisation of AI to accelerate medical research, optimise clinical trials, and improve clinical audit. It raises legal issues that are specific to it, notably as regards the articulation between the AI Act and the data-protection framework. The use of AI for the analysis of large volumes of health data or for the automated recruitment of patients necessarily implies, by hypothesis, a processing of data within the meaning of Article 9 of the GDPR. The strategy does indeed provide for a streamlining of compliance procedures, the preparation of data protection impact assessments (DPIAs) being among the priority actions, opening up a field of articulation with Chapter IV of the EHDS Regulation on the secondary use of health data.

D. *AI for Public Health*

The fourth and final pillar aspires to integrate AI into population-level screening programmes, epidemiological surveillance, and the formulation of evidence-based public health policies. The strategy cites, by way of example, a Swedish study from 2023 in which AI-

D. AI for Public Health

Le quatrième et dernier pilier ambitionne d'intégrer l'IA dans les programmes de dépistage populationnel, la surveillance épidémiologique et la formulation de politiques de santé publique fondées sur les preuves. La stratégie cite, à titre d'exemple, une étude suédoise réalisée en 2023 dans laquelle le dépistage du cancer du sein assisté par IA aurait permis une hausse de 29 % du taux de détection tout en réduisant de 44 % la charge de travail des radiologues[283]. On voit bien l'intérêt de la méthode. Son application à grande échelle soulève cependant des enjeux considérables en matière d'équité algorithmique et de non-discrimination, lesquels sont au cœur du RIA (considérant 27 et article 10, paragraphe 2, relatif à la prévention des biais).

III. UNE FEUILLE DE ROUTE DANS LE TEMPO DU RIA

La stratégie déploie une feuille de route à trois horizons : « *Now* » (année 1), « *Next* » (années 2–3) et « *Future* » (années 4–5). Elle identifie vingt-six opportunités prioritaires de déploiement de l'IA. Cette séquence mérite d'être mise en regard du calendrier d'application du RIA. Les systèmes à haut risque, qui recouvrent la plupart des applications cliniques du premier pilier, seront soumis aux obligations du chapitre III à compter du 2 août 2026, soit la première année d'exécution de la feuille de route *AI for Care*. La coïncidence temporelle implique que les preuves de concept et les projets pilotes de l'horizon « *Now* » devront intégrer dès leur conception les exigences du RIA en matière de gestion des risques, de qualité des données et de documentation technique.

supported breast cancer screening reportedly enabled a 29 percent increase in the cancer detection rate while reducing the radiologists' workload by 44 percent[287]. One readily appreciates the interest of the method. Its application at scale nevertheless raises considerable issues in terms of algorithmic fairness and non-discrimination, matters which lie at the heart of the AI Act (recital 27 and Article 10(2) on the prevention of bias).

III. A ROADMAP IN STEP WITH THE AI ACT TIMELINE

The strategy deploys a roadmap with three horizons: '*Now*' (year 1), '*Next*' (years 2–3) and '*Future*' (years 4–5). It identifies twenty-six priority opportunities for the deployment of AI. That sequencing deserves to be read against the timeline for the application of the AI Act. High-risk systems, which cover the bulk of the clinical applications of the first pillar, will be subject to the obligations of Chapter III from 2 August 2026, namely the first year of execution of the *AI for Care* roadmap. The temporal coincidence means that the proofs of concept and pilot projects of the '*Now*' horizon will have to incorporate, from the design stage, the AI Act requirements in terms of risk management, data quality and technical documentation.

The *AI Implementation Framework* developed by the HSE sets out the mechanisms of governance, approval and monitoring. It provides, in particular, for the creation of an *AI & Automation Centre of Excellence*, tasked with recording AI projects in a national registry (as required, moreover, by the AI Act) and with ensuring compliance with the guidelines of the Health Information and Quality Authority (HIQA) and of the Department of Public Expenditure,

[283] LANG M. et *al.*, « Artificial intelligence-supported screen reading versus standard double reading in the Mammography Screening with Artificial Intelligence trial (MASAI) », *The Lancet Digital Health*, 2023.
[287] K LANG and others, 'Artificial Intelligence-Supported Screen Reading versus Standard Double Reading in the Mammography Screening with Artificial Intelligence Trial (MASAI)' (2023) *The Lancet Digital Health.*

L'*AI Implementation Framework* développé par le HSE décline les mécanismes de gouvernance, d'approbation et de suivi. Il prévoit notamment la création d'un Centre d'excellence en IA et automatisation (*AI & Automation Centre of Excellence*), chargé d'enregistrer les projets d'IA sur un registre national (ce qu'impose par ailleurs le RIA) et d'assurer la conformité aux lignes directrices de la *Health Information and Quality Authority* (HIQA) et du *Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation* (DPER).

Sont visées, à cet égard, les *Guidelines for the Responsible Use of AI in the Public Service* publiées par le DPER ainsi que le *National Guidance for the Responsible and Safe Use of AI in Health and Social Care* en cours de préparation à la HIQA, lequel doit accompagner la mise en conformité avec le RIA. Le rôle de la HIQA dans cet écosystème se trouve d'ailleurs conforté par la section 21 du *Health Information Act 2026*, qui impose désormais au HSE de la consulter pour l'élaboration de ses lignes directrices (v. *supra*). Une remarque conclusive mérite d'être soulignée : la stratégie reconnaît elle-même la nécessité de demeurer agile face à l'évolution des cadres européens. L'observation n'est pas anodine dès lors que la Commission doit adopter, dans les mois à venir, plusieurs règlements d'exécution précisant les exigences techniques applicables aux systèmes d'IA à haut risque dans le domaine de la santé.

IV. PORTEE DE LA STRATEGIE

La démarche irlandaise appelle plusieurs remarques. En premier lieu, elle témoigne d'une anticipation sectorielle du RIA qui mérite l'attention. Loin de traiter ce texte comme une contrainte, la stratégie en fait un cadre structurant, intégré dès la conception des projets (*compliance by design*). La

Infrastructure, Public Service Reform and Digitalisation (DPER).

Particular reference is made to the *Guidelines for the Responsible Use of AI in the Public Service* issued by the DPER and to the forthcoming *National Guidance for the Responsible and Safe Use of AI in Health and Social Care* being prepared at HIQA, which is to accompany compliance with the AI Act. The role of HIQA in this ecosystem is, moreover, reinforced by section 21 of the *Health Information Act 2026*, which now requires the HSE to consult HIQA in the elaboration of its guidelines (see above). One concluding remark deserves to be underlined: the strategy itself acknowledges the need to remain agile in the face of the evolution of European frameworks. The observation is not trivial, inasmuch as the Commission is required, in the months ahead, to adopt a number of implementing regulations specifying the technical requirements applicable to high-risk AI systems in the health domain.

IV. SCOPE OF THE STRATEGY

The Irish approach calls for a number of comments. First, it bears witness to a sectoral anticipation of the AI Act that commands attention. Far from treating the text as a constraint, the strategy makes of it a structuring framework, embedded from the design stage of projects (*compliance by design*). The approach contrasts with certain more defensive stances, in which compliance with the AI Act is apprehended as a retrospective exercise of adapting existing systems.

Second, the strategy puts in evidence a point of articulation still left unresolved: that between conformity assessment under the Medical Devices Regulation and that required by the AI Act. The category of 'AI-as-a-medical-device' systems is certainly identified, and their classification as high-risk systems under the AI Act is explicitly acknowledged. The practical arrangements for the articulation of the two regimes remain, however, largely

démarche contraste avec certaines approches plus défensives, où la conformité au RIA est appréhendée comme un exercice rétrospectif d'adaptation de systèmes existants.

En second lieu, la stratégie laisse entrevoir un point d'articulation encore en suspens : celui entre l'évaluation de conformité au titre du règlement sur les dispositifs médicaux et celle requise par le RIA. La catégorie des systèmes d'« IA en tant que dispositif médical » est certes identifiée, et leur classification comme systèmes à haut risque au titre du RIA est explicitement reconnue. Les modalités pratiques d'articulation des deux régimes restent cependant largement renvoyées à l'*AI Implementation Framework*. Voilà assurément l'un des enjeux déterminants de la mise en œuvre effective du texte.

La stratégie s'inscrit enfin dans un écosystème réglementaire plus large. Le *Health Information Act 2026* analysé ci-dessus en constitue l'autre jalon majeur, qu'une stratégie nationale de données du HSE, encore à venir, viendra compléter. Qu'observe-t-on ? La stratégie reconnaît explicitement que la donnée constitue le « fondement de l'adoption de l'IA » et établit un lien bidirectionnel entre qualité des données et efficacité des systèmes. Ce faisant, elle trace un pont direct avec le règlement EHDS, dont le chapitre IV organise précisément l'accès à des données de santé de qualité à des fins de recherche, d'innovation et d'élaboration de politiques. À l'approche de la présidence irlandaise du Conseil de l'Union européenne, en juillet 2026, cet ancrage pourrait bien offrir à l'Irlande un socle cohérent pour porter ces sujets au niveau européen.

deferred to the *AI Implementation Framework*. It is, without doubt, one of the determining questions for the effective implementation of the text.

The strategy finally takes its place within a wider regulatory ecosystem. The *Health Information Act 2026* analysed above constitutes its other major milestone, which a forthcoming HSE data strategy will, in due course, complete. What does this reveal? The strategy explicitly acknowledges that data constitutes the 'foundation of AI adoption', and establishes a bidirectional link between data quality and the effectiveness of systems. In so doing, it draws a direct bridge with the EHDS Regulation, whose Chapter IV organises precisely the access to quality health data for the purposes of research, innovation and policymaking. As the Irish Presidency of the Council of the European Union draws near, in July 2026, that anchoring may yet offer Ireland a coherent platform from which to carry these matters at European level.

Droit italien

Direttiva generale per l'attività amministrativa e la gestione, Anno 2026 (Directive générale pour l'activité administrative et la gestion), 2026.

par Maddalena DE CARLO
Etudiante en Master 2 Droit international et comparé, École de droit de Toulouse, Université Toulouse Capitole

Aperçu général de la directive

La directive générale du Ministère italien de la Santé, adoptée en vertu des articles 4 et 14 du décret législatif n° 165/2001, constitue le document stratégique annuel qui structure les priorités de la gestion du Service National de Santé (SSN) pour l'année en cours. Elle établit les orientations globales en matière de santé publique, d'organisation des services, de ressources humaines et de modernisation des infrastructures sanitaires.

Ce document encadre les actions des administrations centrales, des Régions et des Provinces autonomes dans l'exécution de leurs missions, en tenant compte des engagements européens et des financements du PNRR (Piano Nazionale di Ripresa e Resilienza)[288].

Après un "contexte institutionnel" (p. 11) qui rappelle le cadre juridique fondamental, incluant le decreto legge 300/1999, la legge 172/2009 et autres textes de référence, le cœur du document réside dans l'intitulé 2 « Priorité de l'action administrative et de la gestion » (v. p. 12 et s.), lequel repose sur treize objectifs stratégiques majeures présentées de manière fluide et hiérarchisée.

On retiendra plus particulièrement les points suivants :

- **2.1.** « Renforcement des mesures de prévention » (p. 17) (vise à protéger les groupes vulnérables pour un bien-être équitable) ;
- **2.2.** « Promotion de politiques de santé axées sur l'innovation » (p. 17) (renforce les réseaux de recherche et le transfert technologique) ;
- **2.3.** « Renforcement des capacités de surveillance épidémiologique » (p. 18) (améliore la gestion des urgences sanitaires) ;
- **2.4.** « Réduction des inégalités entre les régions » (pp. 19-26)[289]

[288] PNRR -désigne le plan italien de relance et de résilience financé par NextGenerationEU pour répondre aux exigences d'interopérabilité de l'EHDS.

[289] 2.4. Incluant dix-sept sous-points, il aborde la garantie des niveaux essentiels d'assistance (LEA) à travers l'intégration hôpital-territoire, les interventions PNRR, la réduction des listes d'attente et l'utilisation de l'IA dans des conditions de non-discrimination et d'information des patients - en incluant des aspects tels que :
2.4.1 Programmation sanitaire nationale
2.4.4 Rischio Clinico ("Risque clinique")

Sont aussi à relever les sections suivantes :

- **2.5.** « Valoriser les professionnels de santé » (p. 27) (met l'accent sur la reconnaissance des médecins urgentistes) ;
- **2.6.** « Favoriser l'innovation technologique dans les dispositifs médicaux » (p. 30) (modernise les essais cliniques).
- **2.7.** « Simplifier l'accès aux services de santé et renforcer les interventions en santé numérique » (p. 33) (constitue un élément central de la directive dans le domaine de la digitalisation, structurant les priorités stratégiques de modernisation du SSN)[290].

Le document se poursuit avec les priorités restantes de l'intitulé 2 (pp. 37-44), qui couvrent :

- **2.8.** « Implémentation de l'efficacité organisationnel du ministère » ;
- **2.9.** « Sensibilisation des usagers à la santé publique » ;
- **2.10.** « Promotion des modes de vie sains et de la santé mentale » ;
- **2.11.** « Sécurité alimentaire » ;
- **2.12.** « Santé publique vétérinaire », et enfin ;
- **2.13.** « Renforcement du rôle international de l'Italie en matière de politique sanitaire ».

La directive se clôt par une synthèse des objectifs stratégiques :

3. « Synthèse des objectifs stratégiques ;

4. « Destinataires et attribution des ressources adressée aux Centri di responsabilità amministrativa (CRA) » (p. 46) ;

5. « Ressources financières et humaines » (p. 47) ;

6. « Systèmes de monitoring informatisé » (p. 47) ;

7. « Bilan de réalisation des objectifs 2025 » (p. 48) ; et enfin

8. « Dispositions finales » (p. 52), complétés par quatre annexes : tableau récapitulatif des objectifs (Allegato 1, p. 54), effectifs au 1er janvier 2026 (Allegato 2, p. 61), modèles et fiches détaillées d'objectifs (Allegati 3-4, pp. 64-67).

Les orientations stratégiques de la directive en matière de santé numérique

Dans le domaine de la digitalisation, la directive identifie des actions stratégiques précises. Elle énonce clairement que la section 2.7 vise à simplifier l'accès aux services de santé et à renforcer la santé numérique par trois axes prioritaires (p. 33).

1. En développant l'écosystème des données de santé (EDS) en créant un outil centralisé (plateforme) de collecte, d'analyse et de valorisation des données sanitaires au service des professionnels de la santé et du public ;
2. En exploitant le potentiel d'information du dossier de santé électronique (FSE) en tant que système d'alimentation du SDE et d'accès aux services de santé numérique ;

2.4.5 Farmacia dei servizi (" Pharmacie des services").
2.4.10 Numero europeo 116117 ("Numéro européen pour soins non urgents") ou encore,
2.4.11 SiVeAS (système de vérification nationale).

[290] Cette section se déploie en points précis :
2.7.1 « Renforcement du Dossier Médical Électronique » (p. 34) ;
2.7.2 « Mise en œuvre de l'Écosystème des Données Sanitaires " (p. 34) ;
2.7.3 « Renforcement des capacités de collecte, d'analyse et de diffusion des données + soutien à la télémédecine » (p. 35) ;
2.7.4 « Santé numérique et échange de données sanitaires dans le cadre européen » (p. 36) ; 2.7.5 Sunshine Act (p. 36) ;
2.7.6 « Élévation des niveaux de cybersécurité » (p. 37) ;
2.7.7 « Rapport sur l'état sanitaire du pays 2022-2024 » (p. 37). Aspects qui seront développés plus en détail (v. p. 3).

3. En développant les services de télémédecine afin d'accroître l'offre de prestations sanitaires de plus en plus efficaces et rapides, avec une attention particulière accordée aux sujets atteints de pathologies chroniques, y compris par la mise en œuvre de la plateforme nationale.

Le Ministère de la Santé entend poursuivre le renforcement de l'infrastructure numérique du Service National de Santé (SSN) en cohérence avec les investissements PNRR en cours, et dans le but de la mise en œuvre de l'Espace européen des données de santé (EEDS) conformément au Règlement UE 2025/327, entré en vigueur le 26 mars 2025.

« *Fascicolo Sanitario Elettronico*[291] (FSE) »

La directive annonce d'abord que l'Italie doit se doter d'un cadre de gouvernance national pour l'usage des données de santé et distingue, conformément au Règlement sur l'EEDS, l'utilisation primaire[292] et l'utilisation secondaire[293]. Ce cadre doit être aligné sur l'objectif européen de la « décennie digitale 2020-2030[294] », qui vise à garantir à toutes les personnes l'accès à leurs données de santé d'ici 2030.

Dans cette perspective, la directive rattache les objectifs de l' EEDS au PNRR, en particulier à l'Investissement 1.3 « *Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione* » (*Missione 6, Componente 2*). Le Ministère de la Santé y est désigné comme entité chargée de la mise en œuvre, en collaboration avec le Département pour la transformation digitale, notamment pour renforcer le FSE à travers de nouveaux décrets prévus par l'article 12, alinéa 7, du décret-loi n° 179/2012.

La directive prévoit aussi la mise en place d'un cadre juridique spécifique pour la télémédecine, qui doit couvrir à la fois les règles de traitement des données de santé et les modalités de tarification des actes de télémédecine, en coopération étroite avec AGENAS (Agence nationale de santé numérique). L'idée est de sécuriser juridiquement ces pratiques tout en les intégrant dans le financement ordinaire du système. L'ensemble de ces "sous-investissements" a un double objectif : d'un côté, moderniser l'infrastructure technologique du Ministère pour supporter de nouvelles applications numériques ; de l'autre, améliorer la rapidité, l'exhaustivité et la qualité des données, qu'elles soient cliniques ou issues du *Nuovo Sistema Informativo Sanitario* (NSIS[295]) utilisé pour la programmation, le suivi et le pilotage administratif. D'ailleurs, la directive explique que, pour la digitalisation, elle se concentre sur le renforcement du *Fascicolo Sanitario Elettronico* (FSE). Elle rappelle que la numérisation des systèmes de santé est considérée par la Commission

[291] Il s'agit de l'équivalent du Dossier de santé électronique.

[292] Art. 2 p.1 let. d) du Règlement (UE) 2025/327 « utilisation primaire : le traitement de données de santé électroniques pour la fourniture de soins de santé en vue d'évaluer, de maintenir ou de 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 sociaux, administratifs ou de remboursement pertinents ».

[293] Art. 2 p. 1 let. e) « utilisation secondaire », le traitement de données de santé électroniques aux fins énoncées au chapitre IV du présent règlement, autres que les finalités initiales pour lesquelles ces données ont été collectées ou produites »
Chapitre 4, Art. 53 désigne le traitement des données de santé pour des finalités autres que les soins individuels (art. 53). Elle est autorisée pour : a) santé publique ; b) politiques sanitaires ; c) statistiques officielles ; d) formation ; e) recherche scientifique et innovation (IA, dispositifs médicaux) ; f) optimisation des soins.

[294] Décision (UE) 2022/2481 du Parlement européen et du Conseil du 14 décembre 2022 établissant le programme d'action pour la décennie numérique à l'horizon 2030.

[295] NSIS - Nouveau système d'information sanitaire

européenne comme un élément central pour responsabiliser les citoyens et construire une société plus saine, les données étant vues comme un facteur clé de la transformation numérique et devant être accessibles et partageables dans toute l'UE.

Conformément à la stratégie de la Commission européenne, les données de santé sont présentées comme essentielles non seulement pour la prise en charge individuelle (prévention et soins personnalisés) dans le cadre de leur utilisation primaire, mais aussi pour la recherche, la prévention des maladies et le recours à des outils numériques centrés sur le patient (utilisation secondaire). L'objectif opérationnel du Ministère italien est donc d'étendre et d'uniformiser au niveau national le contenu des documents numériques de santé, leurs fonctionnalités, ainsi que les modalités de consultation par les professionnels du SSN.

La directive insiste sur le fait que cette transformation sera progressive, organisée en plusieurs phases liées entre elles, et que le Ministère jouera un rôle de coordination entre toutes les institutions concernées. De façon plus précise, il lui revient de fixer les fondements juridiques et d'adopter des lignes directrices techniques (règles, guides, codifications, classifications, standards) pour la collecte, la conservation, la consultation et l'échange de données entre Régions et Provinces autonomes, avec l'appui d'AGENAS et du Département pour la transformation digitale.

« Ecosistema dei dati sanitari[296] (EDS) »

La directive présente ensuite l'Écosystème des Données Sanitaires (EDS) comme l'instrument nécessaire pour parfaire l'architecture du FSE, en fournissant des services d'élaboration et de consultation des données extraites des documents du FSE, tant pour l'usage primaire (prévention, diagnostic, soins) que secondaire (programmation, gouvernement, recherche) (p. 34).



Dans le cadre de la directive, l'EDS assure deux fonctions fondamentales : coordination informatique nationale et prestation de services homogènes sur tout le territoire (services aux patients, professionnels, administrateurs, chercheurs). L'objectif est d'optimiser l'utilisation des données pour une assistance plus efficace, appropriée et rapide, tout en offrant aux citoyens une visibilité claire et immédiate de leurs informations sanitaires, dans le plein respect de la confidentialité, de la cybersécurité et de la protection des données personnelles (p. 35).

La directive précise que l'EDS, conformément à l'article 12, alinéa 15-quater du décret-loi n° 179/2012, sera réalisé en collaboration avec le Département pour la Transformation Digitale (DTD) et AGENAS, et intégrera les données alimentant le système FSE provenant de toutes les structures sanitaires et médico-sociales publiques et privées, des entités du Service National de Santé, des professionnels de santé et du système Tessera Sanitaria[297].

Ces données EDS seront validées et extraites par les solutions technologiques identifiées afin d'offrir des services à l'ensemble des opérateurs du SSN et aux patients, principalement pour les finalités de soins et de prévention, mais aussi pour la prophylaxie internationale, le gouvernement et la recherche.

L'EDS est explicitement présenté comme la base nationale de départ pour la mise en œuvre du Règlement UE 2025/327 établissant l'Espace européen des données de santé, dont les objectifs consistent à permettre aux personnes un meilleur contrôle sur leurs données sanitaires, à faciliter une meilleure continuité des soins

[296] Espace européen des données de santé (EEDS).

[297] Système équivalent à celui des services sanitaires à partir de la Carte Vitale.

transfrontières au sein de l'UE, à encourager un marché unique des services et produits de santé numérique, et à garantir un cadre cohérent pour la réutilisation des données pour la recherche, l'innovation, les politiques sanitaires et les activités règlementaires.

Pour atteindre ces objectifs, la directive prévoit la mise en œuvre de règles communes pour les données personnelles, l'identification de standards et formats assurant l'interopérabilité des données, ainsi que l'élaboration d'une gouvernance nationale impliquant d'autres institutions centrales pour la mise en œuvre du règlement au niveau national. Comme dans d'autres sections de la directive, on constate ici que l'adoption de ces règles communes pour atteindre les objectifs européens reste à l'état de projet en cours d'élaboration, sans que des mesures concrètes soient déjà mises en place.

Collecte, analyse, diffusion des données et soutien à la télémédecine

La directive précise de manière plus concrète comment s'exécute la ligne de financement spécifique du PNRR dans le cadre du 2.7.3 *Potenziamento della capacità di raccolta, analisi e diffusione dei dati a livello centrale e supporto alla diffusione della telemedicina* (p. 35).

Elle détaille les priorités d'utilisation des fonds : moderniser l'infrastructure du Système Informatif Sanitaire National et optimiser tous les processus de gestion des données de santé (collecte, traitement, validation, analyse). Les interventions se concentrent sur trois axes : accélérer l'exploitation des données existantes pour mieux suivre les Niveaux essentiels d'assistance - *Livelli Essenziali di Assistenza* (LEA) ; intégrer de nouvelles sources de données via des plateformes dédiées comme le Système Informatif des Soins Primaires et celui des Hôpitaux de Communauté ; soutenir l'innovation avancée, notamment en définissant une base juridique pour l'intelligence artificielle en santé (p. 36).

Pour exploiter pleinement le potentiel des données tout en respectant la protection des données personnelles, des outils technologiques permettront leur diffusion publique sous forme d'Open Data. Ce projet mobilise l'ensemble du territoire italien, administration centrale, Régions, Provinces autonomes, dans une logique de programmation, monitoring et contrôle sanitaires renforcés.

La Plateforme Nationale de Télémédecine (PNT), placée sous l'égide d'AGENAS (Agence nationale pour les services sanitaires nationaux) avec ses Infrastructures Nationales (INT) et Régionales (IRT), garantira l'accès universel aux services essentiels de télémédecine (téléconsultation, téléassistance, télésurveillance, téléconsultation) grâce à des standards d'interopérabilité communs.

Enfin (§ 2.7.4) la directive confirme que le Ministère de la santé italien continuera sa participation aux activités de santé numérique de l'e Health Network, coordonnant les actions pour l'interopérabilité des données sanitaires au niveau UE, tant pour les finalités de soins (usage primaire) que pour l'usage secondaire (gouvernement, recherche), dans le cadre du Règlement sur l'Espace européen des données de santé.

À travers les infrastructures MyHealth@EU, actuellement en phase expérimentale en Italie pour l'usage primaire des données de santé, et HealthData@EU, dont le pays prépare activement la mise en œuvre pour l'usage secondaire, l'Italie se conforme aux obligations du règlement EEDS en désignant ses autorités nationales compétentes pour garantir l'interopérabilité européenne.

Derniers points sur la santé numérique et dispositions ultérieures

La directive conclut la section sur la santé numérique (§ 2.7) par des mesures transversales de transparence, sécurité et reporting, avant de passer à l'efficience organisationnelle (§ 2.8).

Elle prévoit la pleine mise en œuvre du Sunshine Act (decreto legge. 90/2017) pour une transparence totale des relations financières entre l'industrie pharmaceutique/dispositifs médicaux et les acteurs de santé, transposant la legge 62/2022 "*Disposizioni in materia di trasparenza dei rapporti tra le imprese produttrici, i soggetti che operano nel settore della salute e le organizzazioni sanitarie*"[298] via la plateforme nationale « Santé transparence » gérée par AGENAS : publication annuelle des avantages financiers de l'industrie pharma/dispositifs aux professionnels et structures, avec audits et sensibilisation pour restaurer la confiance publique (p. 36). Elle prévoit une publication annuelle des avantages financiers de l'industrie pharma/dispositifs aux professionnels et structures, avec audits et sensibilisation pour restaurer la confiance du public (§ 2.8).

En conclusion, la directive identifie des actions qui constituent des prérequis indispensables pour sécuriser la transformation numérique du SSN, mais ces mesures demeurent programmatiques et non pleinement opérationnelles, reflétant une vision stratégique encore en phase préparatoire au stade de la directive 2026.

Ministère italien de la Santé, *Direttiva generale per l'attività amministrativa e la gestione (ai sensi degli articoli 4 e 14 del decreto legislativo 30 marzo 2001, n. 165), Anno 2026.*

[298] Loi du 31 mai 2022, n° 62 portant les « Dispositions en matière de transparence des relations entre les entreprises productrices, les acteurs du secteur de la santé et les organisations de santé ».

Droit suédois

Reimbursement of Digital Medical Devices in Sweden

par Sarah DE HEER

Doctorante en Droit public, Université de Lund (Suède)

Introduction

Medical devices come in a wide variety, ranging from simple plasters and thermometers to more advanced technology, such as 3D printed prosthetics and digital tools, including mHealth. Medical devices play a vital role in the provision of healthcare activities and services in Sweden. As such, medical devices are widely used in all parts of the healthcare sector ; when providing highly specialised care in hospitals but also for everyday care for patients in the comfort of their own home.

In this piece, the reimbursement of digital medical devices in Sweden will be discussed. This discussion, however, will be restricted to healthcare activities and services provided under the universal system and the publicly funded private healthcare sector. The common denominator is that both are primarily funded through taxes, which means that patients can rely on the reimbursement schemes. Contrarily, the fully private healthcare sector is not funded by the taxpayers' money, and thus the nationwide reimbursement rules are not applicable to this sector.

Since the responsibility of the provision of healthcare activities and services is decentralized, this contribution will, thus, first introduce the Swedish health care system, focusing on both its legislative and governance framework (**Section 2**). As the use of medical devices when receiving healthcare activities and services and the reimbursement of such medical devices are closely connected in Sweden, this piece will also discuss the use of medical devices in the Swedish healthcare system (**Section 3**). After, this contribution will scrutinise the reimbursement of medical devices in general but also concerning consumable medical devices (**Section 4**). Next, this piece will focus on the reimbursement of digital medical devices (**Section 5**). This contribution will also discuss new developments in Sweden (**Section 6**). Last, a conclusion will follow (**Section 7**).

1. THE SWEDISH HEALTHCARE SYSTEM – A BRIEF OVERVIEW

1.1 The Legislative Framework

While healthcare services in Sweden are governed by multiple legislative frameworks, the main act is the Health and Medical Services Act (hälso-och

sjukvårdslagen)[299]. This Act was adopted in 2017, and aims to make the legal framework easier to understand, clearer, and more accessible[300]. The Health and Medical Services Act is a so-called 'targeted framework law', which means that it solely encapsulates provisions on overall goals, responsibilities and guidelines for the healthcare activities.[301] However, dental care, is in principle excluded by the Health and Medical Services Act[302] Rather, dental care is regulated under the Dental Care Act (*tandvårdslagen*)[303].

Additionally, the healthcare sector in Sweden is regulated by other acts, including the Patient Act (*patientlagen*)[304], Patient Data Act (*patientdatalagen*)[305] and the Patient Safety Act (*patientsäkerhetslagen*)[306]. The legislation governing healthcare activities and services in Sweden are so-called obligation, which means that patients do not derive direct rights under the Swedish legal framework. Rather, the law imposes obligations upon healthcare professionals. Nevertheless, based on the legislative framework, patients can still derive expectations of the healthcare activities and services performed by healthcare professionals.

1.1 The Governance Framework

Various actors play a role in providing healthcare activities and services in Sweden, predominantly the Regions (*Regioner*), and in some instances by the municipalities (*kommuner*). The Regions are responsible for ensuring that everyone who resides in their territory has access to quality care[307]. As such, the Regions are mainly responsible for the provision of healthcare activities and services. However, municipalities in Sweden also play a role, as they take care of the healthcare activities and services for, amongst others, individuals who are awarded special support and services under the Act concerning Support and Service for Persons with Certain Functional Impairments (*lag om stöd och service till vissa funktionshindrade*)[308] and housing with special services for people with disabilities[309].

Consequently, the range of medical devices – whether it be digital or not – depends on the Region or municipality one resides. Certain medical devices may be available for the patient's healthcare journey in one Region or municipality, while patients in other Regions or municipalities may not have access to the same medical device.

2. USE OF MEDICAL DEVICES IN SWEDEN

During the provision of healthcare activities and services by healthcare professionals, a plethora of medical devices are used. Most medical devices are used at healthcare facilities by healthcare professionals. However, a substantial part of medical devices is also used by patients either on their own initiative or prescribed by healthcare professionals. As such, patients can use these medical devices in their own homes. These medical devices for the patients' own use include, among others, assistive devices, medical devices

[299] Health and Medical Services Act (*hälso- och sjukvårdslagen (2017:30*).
[300] Regeringen, *En ny hälso- och sjukvårdslag* (Prop. 2016/17:43), 79.
[301] Regeringen, *En ny hälso- och sjukvårdslag* (Prop. 2016/17:43), 80.
[302] 2 Chapter 1 § Health and Medical Services Act.
[303] 1 Chapter 1 § Dental Care Act (*tandvårdslag (1985:125)*).
[304] Patient Act (*patientlag (2014:821)*).
[305] Patient Data Act (*patientdatalag (2008:355)*).
[306] Patient Safety Act (*patientsäkerhetslag (2010:659)*).
[307] 8 Chapter 1 § Health and Medical Services Act. Section 2 also mentions that Regions are to provide healthcare activities and services to those individuals who do not reside in their territory but are entitled to healthcare benefits under the Social Security Coordination Regulation and students on study visits abroad.
[308] 2 § Act on support and services for certain disabled people (*lag (1993:387) om stöd och service till vissa funktionshindrade*).
[309] 8 Chapter 10 § Social Services Act (*socialtjänstlag (2025:400)*).

consumable for personal use, and therapeutic and treatment devices for home use.

In Sweden, healthcare activities and services are to be performed in such a manner that ensures good care is achieved, which in particular includes that the standard of good quality should be achieved[310]. Further, healthcare professionals need to base their work on scientific evidence and proven clinical evidence[311], which is the golden standard in Swedish health care[312]. This also includes the use of medical devices for patient diagnosis and treatment. Specifically for medical devices, Swedish law requires that they need to enable the provision of good care, irrespective of them being used in a healthcare setting or in the patient's own home[313].

The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care (*Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården*)[314] establishes specific national rules on the use of medical devices in health care and dental care. Before using medical devices during the patient's healthcare journey, medical professionals need to have knowledge of, among others, how the medical device operates and the risk of its use by the patient[315], and are to check the medical device before its use on patients[316]. Further, the Regions and municipalities that are responsible for the provision of health care are to establish routines for the use of medical devices, which are aimed at ensuring– among others – that medical devices are used safely and that only safe devices are used during the diagnosis and treatment of patients[317].

3. REIMBURSEMENT OF MEDICAL DEVICES IN SWEDEN

3.1 General Rule

Unlike the use of medical devices, there are no comprehensive reimbursement rules on national level. Seeing the organisational structure of health care in Sweden, where the responsibility of healthcare activities and services are scattered across the Regions and municipalities, the lack of national-wide reimbursement rules is not surprising. Following this decentralised approach, the Regions and municipalities are also responsible for the purchase of medical devices, which is tied to their reimbursement.

The main rule as regards reimbursement is that the use of medical devices for the diagnosis and treatment of patients is reimbursed by the Region or municipality that bears responsibility for health care. Examples include medical devices used for medical imaging, such as a CT scan and MRI, but also medical devices used for the treatment of patients, including kidney dialysis machine and knee implants.

3.2 Consumable Medical Device

There is an exception to the general approach that the rules of reimbursement are governed by the Regions. Certain medical devices used by patients are subsidised by the State under the high-cost protection scheme (*högkostnadsskyddet*).

---

[310] 5 Chapter 1 § Health and Medical Services Act.
[311] 6 Chapter 1 § Patient Safety Act.
[312] Lena Wahlberg and Johannes Persson, 'Importing Notions in Health Law: Science and Proven Experience' 24 (2017) European Journal of Health Law 565, 566.
[313] 5 Chapter 2 § Health and Medical Services Act.
[314] The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care (*HSLF-FS 2021:52 Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården)*.
[315] 3 Chapter 3 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.
[316] 3 Chapter 4 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.
[317] 2 Chapter 2 § The National Board of Health and Welfare's Regulations on the Use of Medical Devices in Health and Medical Care.

This scheme is primarily applicable to prescription medicine but also to consumable medical supplies (*förbrukningsartiklar*), which include certain medical devices. Unlike durable medical devices, consumable medical devices are characterised by their limited use.

Under Swedish law, these consumable medical supplies need to be prescribed by a physician *either* for a stoma[318] *or* due to an illness to administer medicine or to self-monitor the medication[319]. Such medical supplies for a stoma are ostomy bag and ostomy belts. Examples of consumable medical supplies to self-administer medication include pen needles for diabetes and inhalation aids, while blood glucose test strips and the blood glucose meter are examples of consumable medical supplies to self-monitor medication.

Under the high-cost protection scheme, patients are to pay a maximum amount per year starting from the first purchase of prescription medicine and consumable medical supplies[320]. In short, the more costs you incur, you will pay less percentage wise until you reach a threshold, after which you will receive prescribed medication and consumable medical supplies free of charge[321].

Which consumable medical devices are included in the high-cost protection scheme and the price thereof is decided by the Dental and Pharmaceutical Benefits Agency (*Tandvårds- och läkemedelsförmånsverket*)[322]. However, the Dental and Pharmaceutical Benefits Agency does not decide which medical devices should be purchased by the Regions.

4. A FOCUS ON DIGITAL MEDICAL DEVICES

The AI Healthcare Map (*AI-vårdkartan*) maps AI initiatives used in the Swedish healthcare system[323], which also includes digital medical devices. The AI Healthcare Map is a work-in-progress and is updated on a continuous basis. The AI Healthcare Map indicates that 197 AI initiatives are implemented across Sweden, with every Regions having at least one AI system in place[324]. Almost all Regions in Sweden even use AI systems to improve the healthcare system, such as AI used for translations between Swedish and other languages, AI predicting sick leave at group level of healthcare professionals, and AI warning that equipment need calibration. Nevertheless, the majority of AI initiatives are medical devices used for the provision of health care. Examples of digital medical devices include the use of AI assisting in detecting breast cancer in Region Scania, AI used as an aid to predict strokes in Region Dalarna, and AI helping in diagnosing people with acromegaly in Region Västerbotten. Where these digital medical devices are used to diagnose and treat patients in the Swedish universal healthcare system, the use of such AI medical devices do not incur costs upon patients. Rather, the costs are paid by the State. Furthermore, various Regions are



[318] 18 § 2nd para. Act on pharmaceutical beneifts etc (*lag (2002:160) om läkemedelsförmåner m.m.*).
[319] 18 § 3rd para. Act on pharmaceutical beneifts etc.
[320] 5 § 2nd para. Act on pharmaceutical beneifts etc.
[321] 4 § Act (1996:1150) on high-cost protection scheme when purchasing pharmaceuticals, etc. (*lag (1996:1150) om högkostnadsskydd vid köp av läkemedel m.m.*)
[322] 7 § Act on pharmaceutical beneifts etc.
[323] AI Sweden, 'AI-vårdkartan' (ai.se/) <https://www.ai.se/sv/sektorsinitiativ/halso-och-sjukvard/ai-vardkartan> accessed 12 February 2026.
[324] AI Sweden, 'Vårdkartan' (https://vardkartan.ai.se/) <https://vardkartan.ai.se/> accessed 12 February 2026.

developing medical devices that could be used for patient care. Thus, it would not be surprising to see an increase in the use of such devices in the future.

However, concerns have been raised as regards AI's place in patient care. Specifically, AI Sweden, the national center for applied artificial intelligence and co-created of the AI Healthcare Map, pointed out that AI development is marked by significant regional inequalities. Five out of 21 Regions represent more than 60% of AI initiative in Sweden, with 4 Regions not having any AI system in place[325]. Furthermore, research from the Swedish Medical Association (*Sveriges läkarförbund*) showed that most of the Regions do not have any guidelines in place on how to use AI in the provision of healthcare[326].

Currently, no digital medical devices are included under the consumable medical supplies, and thereby reimbursed under the high-cost protection scheme. This can change following a decision of the Dental and Pharmaceutical Benefits Agency determining that a digital medical device qualifies as self-administrating or self-monitoring medication. However, it is difficult to see how such a classification would apply to digital medical devices, as they are not characterised by their limited use.

5. RECENT DEVELOPMENTS

As the decentralised approach may form an obstacle to effectively purchasing and evaluating – and thus using – medical devices in the Swedish healthcare sector, all Regions have joined forces and collaborate in the 'Regions' collaboration model for medical technology' (*Regionernas Samverkansmodell för Medicinteknik*). The expert group of the this collaboration model, the Medical Technology Products Council (*Medicintekniska produktrådet*) has adopted the so-called 'National Joint Introduction' (*nationellt ordnat införande*). Its aim is to ensure fair, cost-effective and appropriate use of medical devices across Sweden. The National Joint Introduction is a comprehensive process covering all stages necessary for the nationwide adoption of digital medical devices, including market screening, selection, procurement, and follow-up[327].

This national plan will, thus, ensure that patients have access to the same (digital) medical devices – including its reimbursement – across Sweden, as opposed to the availability of medical devices hinging on in which Region one lives. Another benefit of the National Joint Introduction is that the observed the negative impact of the inequalities of AI initiatives on patient care may be restricted, as digital medical devices, including consumable digital medical devices, are implemented nationwide.

Even though the National Joint Introduction may give an answer to the uniform introduction of digital medical devices, introducing AI into patient care is not without obstacles. The Medical Technology Products Council has specifically addressed concerns related to the safety of using digital medical devices in the healthcare system. To this end, they have adopted a recommendation. Before implementing any AI system, including digital medical devices, into the Region's healthcare system, Regions are recommended to use validation platforms, which ensure that AI systems are safe to use

[325] AI Sweden, 'Ny kartläggning: Stor ojämlikhet i regionernas AI-arbete inom vården' (ai.se/) <https://www.ai.se/sv/nyheter/ny-kartlaggning-stor-ojamlikhet-i-regionernas-ai-arbete-inom-varden> accessed 12 February.

[326] Swedish Medical Associaton, 'Regioner saknar riktlinjer för AI i vården' (slf.se/) <https://slf.se/nyheter/regioner-saknar-riktlinjer-for-ai-i-varden/> accessed 12 February.

[327] Regions' collaboration model for medical technology, 'Ordnat införande' (samverkanmedicinteknik.se/) < https://samverkanmedicinteknik.se/ordnat-inforande> accessed 12 February 2026.

in the healthcare system[328]. The aim of this platform, which are also known as VAI platforms (*VAI-plattformer*) is to validate the AI system's clinical performance within the Region's specific clinical environment[329]. There are in total three VAI platforms, each tailored towards AI applications in a specific area, namely[330].

1. VAI-B (Breast) that evaluates AI systems for breast radiology, including determining the diagnostic performance of AI systems in mammography screening
2. VAI-P (Pathology) that assesses AI systems for the analysis of global Ki-67[331] in breast cancer
3. VAI-S (Stroke) that evaluates AI systems that identify and evaluate various forms of stroke

While the VAI platforms do not cover all possible AI systems – and thus digital medical devices –, it is a promising development, as it may help ensure, and potentially even advance, patient safety in Swedish health care.

Conclusion

Reimbursement of medical devices in Sweden is shaped by the decentralised healthcare system, in which the Regions bear primary responsibility and therefore fund digital medical devices when they are used in patient care. This leads to regional disparities amongst patients, as access and reimbursement depend on whether a Region has adopted such technologies. This may mean that an individual in one Region does not have access to a certain digital medical device in their patient healthcare journey, while a patient in another Region may have access to the same device. The only nationwide reimbursement mechanism, namely the high-cost protection scheme for certain prescribed consumable medical devices, currently does not cover digital medical devices.

At the same time, the expanding role of digital medical devices demonstrates the need for a more uniform approach to ensure equal patient access. The National Joint Introduction seeks to enable nationwide adoption of digital medical devices, while validation platforms aim to ensure that AI-based digital medical devices are safe for use in the Swedish healthcare.

---

[328] Regions' collaboration model for medical technology, 'Rekommendation till regionerna att använda valideringsplattformar för AI-produkter' (samverkanmedicinteknik.se/) <https://samverkanmedicinteknik.se/nyheter/nyheter/2025-03-27-rekommendation-till-regionerna-att-anvanda-valideringsplattformar-for-ai-produkter> accessed 12 February 2026.

[329] The Medical Technology Products Council, *Validering av AI-produkter inom bilddiagnostik före införande och under användning* 2025, 3.

[330] The Medical Technology Products Council, *Validering av AI-produkter inom bilddiagnostik före införande och under användning* 2025, 3-4.

[331] Global Ki-67 is a method to measure the proportion of proliferating cancer cells in a tumor sample. For more information, see C. Boyaci and others, 'Global scoring method of Ki67 immunohistochemistry in breast cancer demonstrates improved concordance using real-world multi-institutional data' (2025) 27 Breast Cancer Research 159.

Droit de l'Union européenne

La notion de données personnelles au regard de la pseudonymisation

par Lili-Marie FERRANDO

Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

À l'heure de la révolution du numérique en santé, le partage des données à grande échelle est devenu le socle indispensable d'une médecine personnalisée, prédictive et performante. Cependant, la circulation de ces flux se heurtait jusqu'alors à une interprétation particulièrement rigide du cadre européen de protection des données.

C'est dans ce contexte que la Cour de justice de l'Union européenne (CJUE), dans sa décision du 4 septembre 2025[332], vient de lever un verrou historique en offrant une lecture pragmatique de la pseudonymisation. Par cet arrêt, la Haute juridiction est venue préciser que des données pseudonymisées peuvent perdre leur statut de données personnelles selon le destinataire auquel elles sont transmises. Elle apporte cependant deux conditions majeures : l'impossibilité technique d'identifier la personne via des mesures « raisonnables », et l'incapacité légale du destinataire à obtenir les moyens de réidentification. Cette décision dénote avec l'approche absolue et rigide adoptée jusqu'alors par les autorités de contrôle.

L'affaire s'inscrit dans le cadre de la procédure de résolution bancaire engagée à l'encontre de la *Banco Popular*, un établissement financier espagnol. Le Conseil de résolution unique (CRU) avait mis en œuvre une procédure d'audition des actionnaires et des créanciers. C'est dans ce cadre qu'il a collecté des commentaires et observations des participants dont les identités ont été maintenues confidentielles par le recours à un code alphanumérique unique de 33 caractères, généré aléatoirement au moment de la réponse, qu'il a ensuite pseudonymisés en remplaçant les identités par des codes alphanumériques uniques. Ces commentaires pseudonymisés ont été transmis à un tiers, un cabinet d'audit et de Conseil désigné en tant qu'évaluateur indépendant, mais seul le CRU conservait la clé de correspondance.

En 2019, soit deux ans plus tard, plusieurs participants ont saisi le contrôleur européen de la protection des données (CEPD), reprochant au CRU de ne pas avoir été informés de cette transmission. Le

[332] CJUE, 4 septembre 2025, aff.C-413/23 P, ECLI.EU.

CEPD a adressé un rappel à l'ordre au CRU, estimant que ces données restaient des données à caractère personnel par nature, impliquant une obligation d'information renforcée. Ce dernier a introduit un recours en annulation devant le Tribunal de l'Union qui a annulé la décision du CEPD. C'est dans ce cadre que la Cour de justice a saisie dans le cadre d'un pourvoi.

Bien qu'en l'espèce l'affaire porte sur des données bancaires, la décision était très attendue pour clarifier le régime juridique de la pseudonymisation dans des secteurs sensibles comme celui de la santé.

Il revenait ainsi à la CJUE de trancher une question fondamentale : La qualification de « données personnelles » est-elle absolue ou peut-elle être écartée selon le contexte et le détenteur de l'information ?

En d'autres termes, des données pseudonymisées transmises à un tiers doivent-elles toujours être considérées comme des données personnelles au sens du RGPD et du Règlement UE 2018/1725 ? Cette qualification peut-elle être écartée et si oui, sous quelles conditions techniques et juridiques ?

Par son arrêt en date du 4 septembre 2025, la Cour annule (partiellement) l'arrêt rendu par la juridiction antérieure. Mais elle procède aussi et surtout à une distinction fondamentale entre la nature de la donnée pour l'émetteur et son statut pour le destinataire. Ainsi, une donnée pseudonymisée, peut dans certains cas, ne pas être considérée comme une donnée personnelle à l'égard de son destinataire, sous certaines conditions (appréciation pragmatique et contextuelle). La Cour adopte ainsi une approche casuistique et relative de l'identifiabilité.

Dès lors, il convient d'analyser comment le juge européen est passé d'une approche absolue à une approche relative de la donnée (**I**), avant d'étudier le dualisme du régime juridique qui en découle entre émetteur et destinataire (**II**).

I. DE L'APPROCHE ABSOLUE À UNE APPROCHE RELATIVE : LA « SUBJECTIVISATION » DE LA DONNÉE A CARACTÈRE PERSONNEL

La Cour rompt avec une conception rigide (**A**), pour s'attacher au contexte et à la finalité du traitement, par le prisme d'une conception pragmatique (**B**).

A. Le dépassement de la vision objective

Avant l'arrêt du 4 septembre 2025, prévalait une vision dite « absolue » de la donnée personnelle. En effet, dès lors qu'une clé d'identification existait, peu importe son détenteur, la donnée conservait son caractère personnel pour l'ensemble des acteurs. Cette approche rigide et objective fixait le statut de l'information.

Comme le souligne le Professeur Douville, constituent ainsi des données à caractère personnel des identifiants tels que le nom, l'image, ou encore l'adresse IP « *dès lors que la personne est identifiable à l'aide d'informations supplémentaires*[333] ».

Pour revêtir cette qualification, l'information doit se rapporter à une personne concernée. Dans son arrêt *NOWAK,* la Cour avait déjà dégagé trois critères de rattachement non cumulatifs : le contenu, la finalité et l'effet de l'information. En l'espèce, les opinions exprimées par les créanciers étaient « intimement liées » à ces derniers en tant qu'expression de leurs pensées[334]. Jusqu'à récemment, cette nature personnelle était considérée comme immuable. Cette vision imposait systématiquement l'application du RGPD, entraînant des lourdeurs administratives même si le destinataire des

[333] DOUVILLE, T., « Éthique et données à caractère personnel (Approche française et européenne*) »*, *Revue internationale de droit économique*, 2021 t. XXXV (3), 29-45.

[334] DOUVILLE, T., « La notion de données à caractère personnel après l'arrêt CRU », *Revue trimestrielle de droit commercial et de droit économique*, 2025. 1019. Voir aussi NAFTALSKI, F., *Dalloz IP/IT* 2026, p.158.

données n'avait aucun moyen de savoir qui se cachait derrière tel ou tel code.

La pseudonymisation est un processus réversible défini à l'article 3 (6ème point) du RGPD. Il s'agit d'un traitement permettant que les données ne puissent plus être attribuées à une personne précise « *sans avoir recours à des informations supplémentaires* », à condition que ces dernières soient conservées séparément. À titre d'exemple, la cryptographie à clé secrète permet de lier des données pseudonymisées à l'identité réelle, tant que la clé est stockée de manière sécurisée.

À l'inverse, l'anonymisation, est par principe, irréversible et définitive. Elle détruit définitivement tout lien entre la donnée et l'identité en répondant à trois impératifs : individualisation, corrélation et inférence. Par des techniques de randomisation ou de généralisation, la donnée anonymisée sort instantanément du champ du RGPD.

C'est précisément sur cette distinction que la CJUE apporte une clarification majeure en 2025. Ainsi les données pseudonymisées peuvent désormais perdre leur statut de données personnelles à l'égard du destinataire sous certaines conditions.

B. L'analyse à travers les « yeux » du destinataire

Le point de bascule réside dans le passage d'une approche objective de la donnée à une approche contextuelle, fondée sur le détenteur. La Cour s'appuie sur le considérant 16 du règlement 2018/1725 (équivalent au considérant 26 RGPD) pour affirmer que l'identifiabilité est une notion contextuelle.

Désormais, la donnée est qualifiée à travers son destinataire, sa nature dépend de ce dernier. Dans l'affaire commentée, si le CRU détient la clé de déchiffrement, le cabinet d'audit quant à lui, est juridiquement et techniquement, dépourvu de toute information à caractère personnel. N'ayant accès ni à l'identité des participants, ni aux informations supplémentaires permettant de briser la pseudonymisation mise en place, la donnée change de dimension juridique à son égard. Elle quitte la sphère des données personnelles pour rentrer dans celle des données anonymes.

Comme le souligne le Professeur Douville, cette approche consacre une conception relative :

> *« Ce n'est donc pas parce que des informations supplémentaires permettant d'identifier la personne concernée existent que les informations dont l'attribution à des personnes physiques est discutée dans le cadre d'un traitement de données sont à caractère personnel, tout dépend de qui détient ou peut avoir accès à ces informations supplémentaires. Cette conception relative de la notion de données à caractère personnel s'appuie sur l'interprétation préexistante de la notion de « moyens raisonnablement susceptibles d'être utilisés » et sur la conception dorénavant restrictive de l'expression « toute personne »*[335].

Cette lecture repose sur le critère des « moyens raisonnablement susceptibles d'être utilisés ». Si le destinataire n'a aucun moyen légal ou technique d'accéder à la clé, l'identification n'est plus « raisonnablement envisageable ». La Cour adopte ainsi une interprétation restrictive de l'expression « toute personne », limitant l'analyse aux seuls moyens dont dispose réellement l'entité qui traite la donnée.

Concernant le droit de la santé, cette approche constitue un véritable changement de paradigme. En validant le fait qu'une donnée puisse être anonyme pour celui qui la reçoit sans l'aide pour celui qui l'envoie, la CJUE facilite les échanges. Concrètement, cela sécurise le partage des données massives nécessaires à la médecine de précision ainsi qu'à la recherche, sans pour autant fragiliser la vie privée des patients.

---

[335] DOUVILLE, T., *op cit.* « La notion de données à caractère personnel après l'arrêt CRU », *Revue trimestrielle de droit commercial et de droit économique*, 2025. 1019.

II. LE DUALISME DU RÉGIME JURIDIQUE APPLICABLE : ENTRE SÉCURITÉ DE L'ÉMETTEUR ET SOUPLESSE DU DESTINATAIRE

Si le destinataire bénéficie d'une souplesse nouvelle grâce à l'anonymisation relative (A), l'émetteur quant à lui reste fermement tenu par ses obligations en tant que responsable de traitement (B).

A. Les critères de l'anonymisation relative

Pour que la donnée change de nature aux yeux du destinataire, la Cour ne se contente pas d'une simple promesse de confidentialité. Elle impose un test de réidentification fondé sur « *les moyens raisonnablement susceptibles d'être utilisés* ».

L'anonymisation classique (ou absolue) est irréversible et doit résister à trois impératifs techniques, comme nous avons pu le voir, qui reposent sur des techniques lourdes. L'arrêt crée une anonymisation relative. Ainsi la donnée n'est pas anonyme dans l'absolu, mais elle le devient pour un acteur spécifique selon trois conditions cumulatives. D'abord, on parle de l'impossibilité technique, le destinataire ne dispose d'aucun moyen raisonnable pour identifier les personnes. Ensuite, il y a l'impossibilité légale, qui suppose qu'il n'existe aucune voie de droit permettant au tiers d'accéder aux informations supplémentaires détenues par l'émetteur. Enfin on retrouve l'effort démesuré, c'est l'idée que le coût et le temps nécessaires à une réidentification éventuelle doivent être disproportionnés au regard des technologies disponibles.

Comme l'énonce la Cour, il faut prendre en compte « *l'ensemble des facteurs objectifs, tel que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponible au moment du traitement*[336] ». Si le risque de réidentification est insignifiant ou simplement illicite, le destinataire sort alors du champ d'application du RGPD.

B. Le maintien des obligations du responsable du traitement

Le paradoxe apparent de cette décision réside dans le fait que, bien que les données soient jugées anonymes pour le destinataire (en l'espèce, le cabinet d'audit), le responsable (CRU) est tout de même sanctionné. Ce dualisme s'explique par la nature même de la relation juridique entre le collecteur de données et la personne concernée.

Le statut « personnel » ou « anonyme » d'une donnée est ainsi relatif à son détenteur. Le CRU, en tant qu'émetteur, conserve la clé d'identification, pour lui les données n'ont jamais changé de nature et restent des données à caractère personnel soumises au RGPD. Par conséquent, le fait que la donnée devienne « anonyme » pour un tiers après un transfert, n'efface en aucun cas les obligations initiales du responsable du traitement.

L'obligation d'information, prévue par les articles 14 et 15 du RGPD, naît au moment précis de la collecte. La CJUE rappelle que cette obligation « *s'inscrit dans la relation juridique existant entre la personne concernée et le responsable du traitement*[337] » et porte les informations telles qu'elles ont été transmises aux responsables avant tout transfert à un tiers.

En l'espèce, dès lors que le CRU collectait des noms et des commentaires, il traitait des données personnelles. Il devait ainsi impérativement informer les utilisateurs de l'identité des futurs destinataires, peu importe si ces derniers était incapable de les identifier par la suite.

Ainsi cette décision impose aux responsables de traitement, notamment dans le secteur de la santé, une vigilance accrue. L'anonymisation relative au niveau du destinataire n'est pas une clause

[336] CJUE, aff. C-413/23 P, *opt. cit.*, pt. 79.

[337] *Ibid.*

d'exonération. L'identité des tiers receveurs doit être documentée et communiquée dès la collecte, sous peine de litige, comme en témoigne ledit arrêt. Le responsable du traitement doit continuer de garantir l'exercice des droits car il est le seul maître de la clé de réidentification.

Pour conclure, cet arrêt constitue indéniablement une décision importante pour le droit des données personnelles. En droit de la santé, et plus particulièrement dans le cadre de l'Espace Européen des Données de Santé (EEDS)[338], elle ouvre des perspectives considérables tout en soulevant de nouvelles incertitudes.

L'EEDS, dont l'ambition est de faciliter la circulation des données de santé à des fins de recherche, d'innovation et de soins, repose précisément sur des mécanismes de partage de données à grande échelle entre acteurs multiples. La reconnaissance d'une anonymisation relative par la CJUE pourrait ainsi fluidifier ces échanges.

Toutefois, comme le souligne l'avocate Lorette Dubois, cette avancée pragmatique soulève à elle seule une « *myriade de questions*[339] » aux conséquences pratiques considérables.

D'abord, la question du statut des sous-traitants est particulièrement sensible : les hébergeurs de données de santé recevant des données pseudonymisées pourraient-ils se voir exclus du champ du RGPD ? Une telle exclusion, si elle allégeait leurs obligations formelles, affaiblirait corrélativement les garanties offertes aux patients.

Par ailleurs, la question des transferts de données hors de l'Espace Économique Européen (EEE), fréquents dans le cadre de la recherche médicale internationale, reste, elle aussi en suspens.

Plus fondamentalement, comme le relève l'auteure, « *les notions ont probablement gagné en flexibilité mais la matière perd en sécurité juridique*[340] ». Dans un domaine aussi sensible que celui de la santé, où la réidentification des patients expose à des risques particulièrement graves, cette insécurité appelle une vigilance accrue. Les travaux engagés par le Comité européen de la protection des données sur l'anonymisation et la pseudonymisation, influencés par l'arrêt CRU, ainsi que le projet de règlement *Digital Omnibus* publié en novembre 2025, constituent des développements à suivre attentivement pour les acteurs de l'EEDS.
Ainsi, si l'arrêt CRU ouvre une voie prometteuse pour la médecine de précision et la recherche en santé, il appartient désormais au législateur, ainsi qu'aux autorités de contrôle, de combler les nombreuses « *zones d'ombres et incertitudes* », afin que la flexibilité nouvellement acquise ne se fasse pas au détriment de la protection des données des patients.

CJUE, 4 septembre 2025, *CRE / CRU*, aff. C-413/23 P, ECLI:EU:C:2025:645.

[338] Règlement (UE)2025/327 du Parlement européen et du Conseil du 11 février 2025, *JOUE* L 5 mars 2025

[339] DUBOIS, L., « L'arrêt CRU : un digne épisode de fin pour une série d'anthologie sur la notion de donnée à caractère personnel ? », *Revue Lamy Droit de l'Immatériel*, n° 233, 1er février 2026.

[340] Citation de L. MAISNIER-BROCHE, reprise par l'auteure L. DUBOIS dans « L'arrêt CRU : un digne épisode de fin pour une série d'anthologie sur la notion de donnée à caractère personnel ? », *Revue Lamy Droit de l'Immatériel*, n° 233, 1er février 2026.

La construction prétorienne de la notion de « télémédecine » dans le cadre des soins de santé transfrontaliers

A propos de l'arrêt de la Cour de justice de l'Union européenne du 11 septembre 2025, *UJ c. Österreichische Zahnärztekamme*, aff. C-115/24

par Salaheddine ZAHID

Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Objet de l'arrêt. Par cet arrêt du 11 novembre 2025, UJ c. *Österreichische Zahnärztekammer* (C-115/24), la Cour de justice de l'Union européenne (ci-après « Cour de justice ») précise les contours juridiques de la télémédecine en droit de l'Union, tout en déterminant le régime applicable aux prestations transfrontalières de soins dispensées à distance.

Résumé des faits. Le litige trouve son origine dans la commercialisation, sous la marque « DrSmile », de traitements orthodontiques en délivrant des aligneurs dentaires transparents. UJ, médecin-dentiste établie en Autriche, procédait à certains actes réalisés en présentiels (anamnèse, entretien d'information, scanner 3D de la mâchoire ainsi que des soins préliminaires), tandis que la société allemande *DZK Deutsche Zahnklinik* assurait à distance le suivi orthodontique des patients au moyen d'outils numériques et d'une application dédiée. La chambre autrichienne des médecins-dentistes estimait que cette organisation permettait à une société étrangère (ne disposant pas des autorisations requises par le droit autrichien) d'accéder indirectement à des activités de médecine dentaire en Autriche.

Procédure. La chambre autrichienne des médecins-dentistes introduit une action en cessation assortie d'une demande en référé afin d'interdire à UJ toute participation directe ou indirecte à des activités de médecine dentaire exercées en Autriche par des sociétés étrangères ne disposant pas des autorisations prévues par le droit autrichien. Rejetée en première instance, l'*Oberlandesgericht Graz* (tribunal régional supérieur de Graz, Autriche) accueille la demande d'appel, considérant que UJ agissait en tant qu'auxiliaire d'exécution de l'entreprise allemande. Saisi d'un pourvoi contre cette dernière décision, l'*Oberster Gerichtshof* (Cour suprême, Autriche) sursoit à statuer pour poser des questions préjudicielles à la Cour de justice.

Les questions préjudicielles. La juridiction de renvoi cherchait, pour l'essentiel, à savoir si un traitement médical complexe, mêlant prestations réalisées physiquement dans l'Etat du patient et suivi numérique à distance, pouvait relever de la notion de « télémédecine » au sens de la directive 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers. Elle s'interrogeait, dans un deuxième temps, sur le droit applicable à ces prestations transfrontalières et, dans un troisième, sur l'articulation entre la directive de 2011, la directive 2000/31 (voir *infra*) et la directive 2005/36 (voir *infra*).

Réponses de la Cour de justice. La télémédecine est ainsi « *une notion autonome* » du droit de l'Union, désignant « *exclusivement* » des soins de santé fournis à distance, sans présence physique simultanée du patient et du prestataire, « *au moyen des technologies de l'information et de la communication* » (« TIC »). La Cour précise également qu'un traitement médical complexe peut comprendre des prestations de soins de santé soumises à des régimes juridiques distincts. Enfin, elle en déduit que les prestations de télémédecine doivent être soumises à la législation de l'Etat membre dans lequel le prestataire est établi.

Problématisation et problématique. La Cour de justice se trouve confrontée aux difficultés engendrées par la dématérialisation croissante des prestations de soins de santé au sein du marché intérieur. Le développement de traitements médicaux complexes mêlant prestations numériques et actes réalisés physiquement, remet en cause les critères de rattachement des soins. Et ce, en mettant en tension la libre prestation de services (art. 56 du Traité sur le fonctionnement de l'Union européenne (ci-après « TFUE »), la sécurité des patients et les compétences conservées par les Etats membres en matière d'organisation des systèmes de santé (art. 168, paragraphe 7 du TFUE). Dès lors, la Cour de justice construit, à travers la notion de télémédecine (**I**), un régime autonome applicable aux prestations de soins de santé transfrontalières de télémédecine (**II**).

I. LA CONSTRUCTION PRÉTORIENNE D'UNE CONCEPTION AUTONOME DU DROIT DE L'UNION DE LA TÉLÉMÉDECINE

Une définition autonome. La directive 2011/24/UE ne contient aucune définition explicite de la notion de « télémédecine » et n'opère aucun renvoi au droit des Etats membres pour en déterminer le contenu. La Cour de justice en conclut que le terme « télémédecine » doit recevoir une interprétation uniforme, constituant une « *notion autonome du droit de l'Union* » (§ 62). Dès lors, cette dernière doit être interprétée « *conformément à son sens habituel en langage courant* » et « *du contexte dans lequel [elle] est utilisé[e] et des objectifs poursuivis par la réglementation dont [elle] fait partie* ». Ce considérant méthodologique structure l'ensemble du raisonnement de la Cour de justice, laquelle mobilise successivement les interprétations littérale, contextuelle, téléologique puis historique afin de dégager une véritable conception de la télémédecine dans le droit de l'Union.

Interprétation littérale. Cette interprétation souligne que « *le sens habituel du terme « télémédecine » par son étymologie même, fait référence à des prestations de médecine qui sont fournies à distance* » (§ 63). La Cour rattache cette approche linguistique au libellé de l'article 3, sous d) et e) de la directive 2011/24, dont il ressort qu'un soin dispensé dans le cadre de la télémédecine ne peut relever des « *soins transfrontaliers* » qu'à la condition d'être fourni « *dans un État membre autre que l'État membre d'affiliation* ». La télémédecine apparaît ainsi intrinsèquement liée à la logique de circulation transfrontalière des soins au sein du marché intérieur.

Interprétation contextuelle (§64 à 81). La Cour oppose d'abord la règle générale posée par l'article 3, sous d), première phrase, de la directive selon laquelle « *l' État membre de traitement est celui sur le territoire duquel les soins de santé sont effectivement dispensés* » (§ 64), à l'exception propre à la télémédecine (lieu d'établissement du prestataire), laquelle doit être interprétée strictement afin que « *les règles générales ne soient pas vidées de leur substance* » (§65). De toute évidence, la Cour veille à préserver le principe de rattachement territorial des soins, la télémédecine n'apparaissant que comme une exception fonctionnelle justifiée par les spécificités techniques des « *technologies de l'information et de la communication* » (TIC). Ainsi, « *l'État membre de traitement pour des soins autres que ceux relevant de la télémédecine doit être déterminé sur le fondement du territoire où ces soins sont effectivement dispensés* » (§ 66).

Traitement médical complexe. A partir de la définition des « soins de santé » englobant les services fournis par des professionnels de santé afin « *d'évaluer, maintenir ou rétablir* » l'état de santé des patients (§ 67), la Cour souligne qu'un traitement médical peut comprendre « *une large variété de services de santé* », certains pouvant être réalisés dans différents *États*

membres et par différents professionnels (§ 68). Donc, même lorsqu'un acte réalisé par télémédecine fait partie d'un traitement médical complexe comprenant des soins réalisés physiquement dans l'Etat d'affiliation du patient, un acte effectué par télémédecine peut être considéré, à lui seul, comme un soin de santé transfrontalier et être soumis à des règles juridiques spécifiques (§ 69).

Service de la société de l'information (art. 2 directive 2000/31 et art. 1er, paragraphe premier 1, sous b), directive 2015/1535). La Cour précise que seuls les services de santé effectivement fournis « *à distance* », sans présence physique simultanée du patient et du prestataire, peuvent relever de la télémédecine et, plus largement, des « *services de la société de l'information* » (§ 71 à 74). A l'inverse, les soins réalisés en présence du patient, « *même s'ils impliquent l'utilisation de dispositifs électroniques* », sont exclus de cette qualification (§ 72). Toutefois, la Cour refuse assimiler le traitement médical complexe à un « *service global unique* » au sens de la jurisprudence relative aux plateformes numériques (§ 75 à 77). Par conséquent, chaque acte conserve son autonomie juridique en raison des « *compétences professionnelles spécifiques* » et des « *exigences techniques* » qui lui sont propres (§ 78). Appliquant ce raisonnement au cas en l'espèce, la Cour considère que les actes accomplis physiquement en Autriche par UJ et les prestations réalisées à distance depuis l'Allemagne seront appréciés distinctement, bien qu'ils participent à un seul « *traitement orthodontique* » (§79 à 81).

Interprétation téléologique. La Cour justifie le régime dérogatoire applicable à la télémédecine par « *la nature et [les] spécificités* » de cette pratique (§ 84). Soumettre alors un médecin, exerçant dans l'Etat où il est établi, aux règles applicables dans tous les Etats où se trouveraient ses patients, « *porterait atteinte à la compétence de l'Etat de traitement pour organiser ses soins de santé et exposerait les médecins et les patients à une insécurité juridique* » (§83 à 86 ; v. aussi l'article 168, paragraphes 1 et 7 du Traité sur le fonctionnement de l'Union européenne – TFUE).

Interprétation historique. La Cour rappelle la définition de la télémédecine de la Commission (COM (2008) 689 final) comme la « *fourniture à distance de services de soins de santé* » au moyen des TIC, « *dans des situations où le professionnel de la santé et le patient [...] ne se trouvent pas physiquement au même endroit* » impliquant « *la transmission en toute sécurité de données et d'informations médicales* » (§ 87). Cette conception a ensuite été reprise dans la proposition de directive de 2008 (COM (2008) 414 final) relative à l'application des droits des patients en matière de soins de santé transfrontaliers, laquelle qualifiait notamment de « télémédecine » « *la fourniture d'un service depuis le territoire d'un État membre vers le territoire d'un autre État membre* » (§ 88), distinctement des soins reçus à l'étranger, de l'installation permanente ou de la présence temporaire du praticien.

Par conséquent, la Cour conclut sur l'interprétation de la notion de soins de santé transfrontaliers dispensés dans le cas de la télémédecine que celle-ci est caractérisée par « une prestation d'un service de santé dispensé à un patient par un prestataire de soins de santé établi dans un Etat membre autre que l'Etat membre d'affiliation ~~de ce patient~~, à distance et donc sans la présence physique simultanée au même endroit de ce patient et de ce prestataire, au moyen des technologies de l'information et de la communication » (§90).

II. L'ENCADREMENT JURIDIQUE DE LA TÉLÉMÉDECINE ENTRE LIBRE PRESTATION DE SERVICES ET COMPÉTENCES NATIONALES EN SANTÉ

A. Sur le rapport avec la directive 2000/31 relative aux services de la société de l'information.

Le champ d'application de la directive 2011/24/UE. La directive 2011/24/UE (art. 1er et considérant 10) vise à « *faciliter l'accès à des soins de santé transfrontaliers sûrs et de qualité élevée* », à « *garantir la mobilité des patients* » et à « *promouvoir la coopération en matière de soins de santé entre les États membre* » (§ 95). La Cour souligne que cette directive « *ne se limite pas à édicter des règles en matière de remboursement des coûts des soins de santé transfrontaliers* » (§ 96). En effet, outre les règles relatives au remboursement des soins (§ 97), celle-ci comporte également, pour l'essentiel, des dispositions relatives à la *qualité*, à *la sécurité des soins* et à la *coopération en matière de soins de santé* (§ 97 et 98). La Cour en déduit ainsi que le « *champ d'application de la directive 2011/24 [...] ne se limit[e] pas au remboursement des coûts des soins de santé transfrontaliers* » (§ 99).

Application du droit de l'État membre de traitement. La Cour rappelle que les soins de santé transfrontaliers doivent être dispensés conformément « *à la législation de l'Etat membre de traitement* » ainsi qu'aux « *normes et orientations en matière de qualité et de sécurité* » établies par celui-ci (§ 100). Il en résulte que, en dehors des normes de sécurité fixées par le droit de l'Union, seules les règles de l'Etat membre de traitement ont vocation à s'appliquer (§ 101). Par conséquent, les soins relevant de la télémédecine, étant réputés dispensés dans l'Etat où le prestataire est établi, doivent respecter la législation ainsi que les exigences de qualité et de sécurité de cet Etat membre (§ 102).

Service de la société de l'information. La Cour rappelle que l'application de la directive 2011/24 s'effectue « *sans préjudice* » de la directive 2000/31 relative aux services de la société de l'information (§ 103). De fait, dès lors qu'une prestation de télémédecine peut relever de cette qualification, elle entre également dans le champ d'application de la directive 2000/31. L'article 3 de cette dernière prévoit que les services de la société de l'information doivent respecter les dispositions nationales applicables dans l'Etat membre où le prestataire est établi (§ 104), notamment les « *qualifications ou autorisations* » nécessaires à l'exercice de cette activité (§ 105). Tant la directive 2011/24 que la directive 2000/31 conduisent à appliquer à la télémédecine la législation de l'Etat membre d'établissement du prestataire (§ 106).

B. Sur le rapport avec la directive 2005/36 relative à la reconnaissance des qualifications professionnelles.

L'absence de déplacement dans le cadre de la télémédecine. L'article 5 de la directive 2005/36 ne s'applique qu'en cas de « *déplacement du prestataire vers le territoire de l'Etat membre d'accueil* ». Or, la télémédecine implique précisément qu'aucun déplacement physique n'ait lieu, le service de santé étant fourni « *à distance* » exclusivement au moyen des TIC. Dès lors, la prestation de soins de santé par télémédecine s'effectue sans déplacement du patient ni du prestataire, la Cour relevant ainsi que « *c'est le service de santé qui, en raison de son caractère transfrontalier, « se déplace »* » (§ 111).

L'impossibilité de caractériser un déplacement indirect du prestataire. La Cour écarte l'idée selon laquelle un prestataire établi dans un Etat membre pourrait être regardé comme s'étant déplacé dans un autre Etat membre, du seul fait qu'il y fait réaliser des soins en présentiel par un professionnel lié contractuellement à lui (§ 112). Elle rappelle qu'un « prestataire de soins de santé » est toute entité dispensant légalement des soins sur le territoire d'un État membre (§ 113). Or, *DZK Deutsche Zahnklinik* ne pouvant légalement exercer en Autriche, celle-ci ne saurait être considérée comme le prestataire des soins réalisés physiquement dans cet Etat (§ 114). A l'inverse, UJ, habilitée à exercer

légalement la profession de médecin-dentiste en Autriche, doit être regardée comme le prestataire des soins concernés, indépendamment de l'existence d'un contrat liant ce professionnel et une entité établie dans un autre Etat membre (§ 115). La Cour considère alors qu'il serait « *artificiel* » de considérer que des soins dispensés physiquement en Autriche, l'auraient en réalité été par une société établie en Allemagne (§ 116). Enfin, *« la circonstance que le prestataire exerçant dans l'État membre de résidence du patient ait pu agir au nom du professionnel de santé établi dans un autre État membre ne permet pas de considérer que ce dernier se soit, pour cette seule raison, déplacé dans le premier État membre* » (§ 117).

La Cour conclut donc à l'inapplication de l'article 5 de la directive 2005/36.

CJUE, 11 septembre 2025, *Österreichische Zahnärztekamme*, aff. C-115/24, ECLI:EU:C:2025:694.

Droit français

Accès au dossier médical partagé : *« pas sans le consentement initial du patient »* nous dit le Conseil d'État

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

La décision n° 490409 rendue par le Conseil d'État le 15 octobre 2025 porte sur l'équilibre, souvent délicat, qu'il convient d'établir entre l'efficacité et la fluidité de la prise en charge d'un patient et la protection de ses données personnelles. Il s'agissait en l'espèce de savoir si des membres de l'équipe de soins du patient pouvaient accéder et alimenter son dossier médical partagé, alors même qu'ils ne relèvent pas de la catégorie des professionnels de santé.

Saisi par le Conseil national de l'Ordre des médecins, le Conseil d'État avait à statuer sur la légalité de l'arrêté du 26 octobre 2023 du ministre de la santé et de la prévention. Cet arrêté, pris en application de l'article R. 1111-46 du code de la santé publique[341], fixe les règles de gestion des droits d'accès des professionnels, mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 de ce même code, au dossier médical partagé du patient. Figure donc en annexe de l'arrêté attaqué une matrice d'habilitation qui définit les droits d'accès aux documents contenus dans ledit dossier médical, en fonction de la catégorie dont relève le professionnel (de santé, du social ou du médico-social).

Plusieurs moyens, ayant trait à la légalité externe comme interne de l'arrêté, sont soulevés par le Conseil national de l'Ordre des médecins. Le premier, portant sur la procédure d'adoption de l'arrêté, est aisément écarté par le Conseil d'État. Cette procédure prévoit que le projet d'arrêté soit soumis à l'avis de divers organismes[342].

---

[341] Cet article dispose que *« L'accès au dossier médical partagé des professionnels mentionnés à l'article L. 1111-15 et au III de l'article L. 1111-17 ainsi que des établissements de santé, établissements ou services sociaux ou médico-sociaux est subordonné au consentement préalable du titulaire selon les modalités prévues aux alinéas suivants. […] Ces professionnels ont accès aux seules données strictement nécessaires à la prise en charge du titulaire du dossier médical partagé dans le respect des règles de gestion des droits d'accès fixées par un arrêté du ministre chargé de la santé, pris après avis de la Caisse nationale de l'assurance maladie, des conseils nationaux des ordres des professionnels de santé, de l'Union nationale des associations agréées d'usagers du système de santé mentionnée à l'article L. 1114-6 et de la Commission nationale de l'informatique et des libertés. »* Nous soulignons.

[342] Il s'agit de Caisse nationale de l'assurance maladie, des conseils nationaux des ordres des professionnels de santé, de l'Union nationale des

Toutefois, une modification ultérieure du projet soumis ne se traduit pas *ipso facto* par l'obligation de procéder à une nouvelle consultation de ces derniers. Le Conseil d'État précise en effet que seule la survenance de questions nouvelles du fait de cette modification est de nature à faire renaitre cette obligation.

Les moyens tirés de la légalité interne font l'objet de développements plus importants qui exigent qu'il soit rappelé, préalablement à leur examen, qu'ils se sont accompagnés d'une demande distincte, d'ordre procédural. Le Conseil national de l'Ordre des médecins avait demandé que soit transmise au Conseil constitutionnel une question prioritaire de constitutionnalité portant sur le paragraphe III de l'article L. 1111-17 du code de la santé publique. Il estimait que ces dispositions portaient atteinte au droit au respect de la vie privée car elles autorisaient tout professionnel participant à la prise en charge d'un patient – nonobstant sa non-appartenance à la catégorie des professionnels de santé – d'accéder à son dossier médical partagé, sous réserve de son consentement[343]. Par une décision du 12 septembre 2024, le Conseil constitutionnel a déclaré cette disposition conforme à la Constitution, estimant qu'elle visait à améliorer la coordination des soins du patient et donc à permettre la poursuite de l'objectif de valeur constitutionnelle de protection de la santé[344]. Ainsi, le consentement donné par le patient pour l'accès à son dossier médical partagé vaut pour l'ensemble de l'équipe des soins.

Se fondant sur cette décision, le juge administratif suprême écarte tout naturellement le moyen tiré de la méconnaissance de la Constitution, validant à son tour l'accès de tous les professionnels concourant effectivement à la prise en charge du patient à son dossier médical partagé. Le Conseil d'État ne nie pas pour autant que la matrice d'habilitation accorde, à l'ensemble desdits professionnels, un *« droit d'accès par défaut »* aux données de santé du patient. Il précise simplement que *« par défaut »* ne signifie pas *« absolu et inconditionné ».* La matrice d'habilitation ne décharge pas ces professionnels de leur obligation d'accéder aux *« seules données strictement nécessaires à la prise en charge du patient »*. En effet, et tel que l'a relevé le Conseil constitutionnel dans la décision précitée, le non-respect de cette obligation peut conduire à l'application des sanctions prévues aux articles L. 1110-4 paragraphe V du code de la santé publique[345] et 226-13 du code pénal[346]. Des considérations similaires, se rapportant au principe de minimisation des données, sont mobilisées par le Conseil d'État pour attester de la conformité de l'arrêté attaqué à l'article 8 de la Convention européenne des droits de l'homme et au règlement général sur la protection des données[347].

---

associations agréées d'usagers du système de santé et de la Commission nationale de l'informatique et des libertés.

[343] Le consentement du patient doit être libre et éclairé. Un consentement est libre lorsqu'il est donné sans contrainte et lorsque le patient est en état de l'exprimer. Un consentement est éclairé lorsqu'il est donné à la suite d'une information loyale, claire et adaptée à la capacité de compréhension du patient. De surcroît, il doit être donné *avant* l'ouverture de l'accès au dossier médical partagé, raison pour laquelle nous l'avons qualifié dans la suite de nos propos de consentement *initial.*

[344] Cons. constit, 12 septembre 2024, décision n° 2024-1101 QPC. Cette décision a fait l'objet d'un commentaire dans la deuxième édition de ce Bulletin. Joud Gharzeddine, « Modalités d'accès au dossier médical partagé d'un patient par des professionnels « hors santé » participant à sa prise en charge : une affirmation non équivoque de constitutionnalité », *Bulletin de l'EDiHL*, p. 108.

[345] Conformément à cet article, *« le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende. ».*

[346] Aux termes de cet article, *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. ».*

[347] Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des

Toutefois, si cette habilitation collective est validée par le Conseil d'État, l'absence de mention explicite quant à la nécessité de recueillir le consentement initial du patient ne saurait l'être. Cette condition, énoncée à l'article L. 1111-17 du code de la santé publique et rappelée à l'article R. 1111-46 du même code, constitue la pierre angulaire du dispositif tout entier. Elle permet au patient de décider de l'avenir de ses données de santé et de considérer que le droit au respect de sa vie privée et du secret des informations le concernant[348] ait véritablement été respecté. L'omission de la nécessité de recueillir le consentement initial du patient amène le Conseil d'État à considérer que l'arrêté attaqué est entaché d'une erreur de droit, ce qui conduit à son annulation partielle.

CE, 10ème et 9ème chambres réunies, 15 octobre 2025, n° 490409, ECLI:FR:CECHR:2025:490409.2025101.

données à caractère personnel et à la libre circulation de ces données

[348] Conformément à cet article, *« 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 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant.».*

Consultation irrégulière de 441 dossiers médicaux : quand le Conseil d'État rappelle l'importance du consentement des patients pour la recherche

par Joud GHARZEDDINE

Étudiante en Master 2 Droit des Libertés et titulaire du Master 2 Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Par sa décision n° 491701 rendue le 4 juillet 2025, le Conseil d'État clarifie la notion *« équipe de soins »*, précisant les professionnels de santé, du social ou du médico-social qui peuvent être considérés comme y relevant. Cette clarification est fondamentale en ce que si le recueil du consentement du patient[349] est obligatoire préalablement à l'ouverture de l'accès à son dossier médical partagé, une fois donné, les informations y figurant sont *« réputées confiées à l'ensemble de l'équipe »*[350].

En l'espèce, le ministre de l'enseignement supérieur et de la recherche et le ministre de la santé et de la prévention – requérants devant le Conseil – demandaient l'annulation de la décision disciplinaire visant M. A., professeur des universités-praticien hospitalier exerçant à l'hôpital Henri Mondor. Ladite décision l'avait en effet déchargée de toute responsabilité et ce, malgré la consultation irrégulière de 441 dossiers médicaux entre le 1er janvier et le 31 août 2020. La juridiction disciplinaire avait considéré que M. A. appartenait à l'équipe de soins, telle que définie par l'article L. 1110-12 du code de la santé publique[351]. Elle se fondait pour se faire sur sa participation *« aux réunions de l'équipe médico-soignante du service de chirurgie cardiaque et au dispositif de permanences et d'astreintes de ce service »* et sa qualité de « *responsable de la recherche »* au sein dudit service. Elle en déduit que les informations disponibles dans les dossiers médicaux consultés étaient réputées confiées à l'*ensemble* de l'équipe de soins et partant, à M. A.

Le Conseil d'État est, quant à lui, d'un tout autre avis. Il lui parait inexact de considérer que M. A. appartenait à l'équipe de soins, en ce qu'il n'avait pas consulté les dossiers médicaux à l'occasion d'une prise en charge *effective* des patients concernés, mais en vue de réaliser une étude sur la morbi-mortalité des patients du service. De surcroît, sa responsabilité en matière de recherche au sein du service ne le dispense pas de l'obligation prévue à l'article L. 1122-1 du code de la santé publique[352], soumettant la conduite de tout protocole de recherche impliquant la consultation des dossiers médicaux de patients au recueil préalable de leur consentement. Ainsi, en estimant que la juridiction disciplinaire a inexactement qualifié les faits de l'espèce, le Conseil d'État apporte une clarification nécessaire quant aux professionnels pouvant être entendus comme relevant effectivement de *« l'équipe de soins »* et ceux qui, n'y appartenant pas, restent soumis à l'obligation de recueillir leur consentement.

CE, 5ème chambre, 04 juillet 2025, n° 491701, ECLI:FR:CECHS:2025:491701.20250704.

[349] Le consentement du patient doit être libre et éclairé. Un consentement est libre lorsqu'il est donné sans contrainte et lorsque le patient est en état de l'exprimer. Un consentement est éclairé lorsqu'il est donné à la suite d'une information loyale, claire et adaptée à la capacité de compréhension du patient.

[350] Cela est précisé au III de l'article L. 1110-4 du code de la santé publique qui dispose que *« Lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe. ».*

[351] Aux termes de cet article, *« l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes (...) ».* Nous soulignons.

[352] Cet article dispose que *« Préalablement à la réalisation d'une recherche impliquant la personne humaine, une information est délivrée à la personne qui y participe par l'investigateur ou par un médecin qui le représente. (...) ».*

Commentaire sous l'arrêt du Conseil d'État, *Association Les Licornes célestes et autres c. CNIL*, 20 mars 2026 (n°s 503159 et 504171)

par Chaimae HBA

Étudiante en Master 1 Droit du numérique IA, École de droit de Toulouse, Université Toulouse Capitole

La France porte à travers son Système national des données de santé *(SNDS)* la base médico-administrative la plus complète d'Europe, dont l'exploitation à des fins de recherche soulève d'inévitables questions quant au choix de l'hébergeur et à la protection des données des patients face aux législations extraterritoriales, au premier rang desquelles le CLOUD Act américain[353]. C'est dans ce contexte que le Conseil d'État, par une décision du 20 mars 2026, a été appelé à se prononcer sur la légalité de l'autorisation délivrée par la Commission nationale de l'informatique et des libertés *(CNIL)* à l'Agence européenne des médicaments (EMA) pour traiter des données de santé de dix millions de Français, hébergées par la filiale irlandaise de Microsoft, dans le cadre du projet européen DARWIN EU[354].

En l'espèce, l'Agence européenne des médicaments coordonne le réseau DARWIN EU, infrastructure européenne destinée à exploiter des données de santé réelles pour étudier l'emploi, la sécurité et l'efficacité des médicaments et des vaccins. Pour mener des études épidémiologiques portant sur l'estimation de l'incidence et de la prévalence de pathologies dans la population générale en France, l'EMA a sollicité l'extraction de données issues du SNDS, confiant cette mission au groupement d'intérêt public « Plateforme des données de santé » *(PDS, ou Health Data Hub)*, agissant en qualité de sous-traitant. Ce dernier a lui-même recours à la société Microsoft Ireland Operations Ltd, filiale de droit irlandais de Microsoft Corporation, groupe soumis au droit américain, pour héberger les données sur des serveurs situés en France. La CNIL a, par délibération du 13 février 2025[355], autorisé ces traitements automatisés pour une durée de trois ans.

Deux requêtes distinctes en annulation pour excès de pouvoir sont enregistrées devant le Conseil d'État. La première est présentée par l'association Les Licornes célestes, accompagnée de personnes physiques et soutenue par une intervention de sociétés françaises de cloud souverain et d'associations du logiciel libre. La seconde émane de l'association Interhop, de l'association Constances, du Syndicat de la médecine générale, de la Fédération Sud Santé Sociaux et de la Ligue des droits de l'homme. Le Conseil d'État les joint pour statuer par une seule décision, conformément au principe d'économie de procédure.

Les requérants soulèvent quatre séries de moyens. En premier lieu, ils invoquent une erreur de droit tirée de l'impossibilité pour le sous-traitant de garantir l'absence de transfert de données vers les États-Unis, en méconnaissance de l'article 28 §3 a) du RGPD[356] et de l'article R. 1461-1 du code

[353] CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), loi fédérale américaine adoptée le 23 mars 2018. Elle permet aux autorités judiciaires américaines d'exiger d'un fournisseur de services cloud établi aux États-Unis la communication de données stockées sur ses serveurs, y compris lorsque ceux-ci se trouvent hors du territoire américain.

[354] DARWIN EU (*Data Analysis and Real-World Interrogation Network – European Union*) : réseau piloté par l'Agence européenne des médicaments (EMA) depuis 2022 visant à exploiter des données de santé réelles pour évaluer l'efficacité et la sécurité des médicaments tout au long de leur cycle de vie.

[355] CNIL, délibération n° 2025-014 du 13 février 2025, publiée au Journal officiel le 11 mars 2025.

[356] RGPD, art. 28 §3 a) : le sous-traitant « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ».

de la santé publique[357]. En deuxième lieu, ils soutiennent que la CNIL a méconnu les articles 44 et 46 du RGPD[358] en autorisant des transferts de données techniques d'usage vers les États-Unis sans vérification suffisante des garanties. En troisième lieu, ils excipent de l'illégalité de la décision d'adéquation UE-États-Unis du 10 juillet 2023[359] *(Data Privacy Framework)*, dont ils demandent le renvoi préjudiciel devant la CJUE au regard des articles 7, 8, 47 et 52 de la Charte des droits fondamentaux. En quatrième et dernier lieu, ils soutiennent que la délibération méconnaît l'article 31 de la loi SREN du 21 mai 2024[360] relatif à l'exigence de certification SecNumCloud pour les administrations recourant à l'informatique en nuage.

Dès lors, le nœud du litige était de déterminer si l'autorisation délivrée par la CNIL permettant à l'EMA de traiter des données de santé du SNDS hébergées par la filiale irlandaise d'une société soumise au droit américain est légale au regard des exigences du RGPD relatives aux garanties du sous-traitant et à l'encadrement des transferts de données vers des pays tiers, eu égard notamment au risque d'accès extraterritorial fondé sur le CLOUD Act américain.

Le Conseil d'État rejette les requêtes. Il juge, d'une part, que la délibération attaquée n'a pour objet que d'autoriser un traitement de données hébergé sur le territoire français et n'autorise aucun transfert vers les États-Unis, rendant inopérante l'exception d'illégalité de la décision d'adéquation. Il juge, d'autre part, que les données techniques d'usage susceptibles d'être accessibles depuis les États-Unis ne constituent pas des données de santé et sont encadrées par des clauses contractuelles types conformes au RGPD. Il retient enfin que les garanties techniques et organisationnelles déployées *(pseudonymisation, limitation de la durée de conservation, contrôle des risques de réidentification, certification HDS[361])* sont suffisantes au regard des articles 28 et 32 du RGPD[362], et que l'article 31 de la loi SREN était inapplicable en l'absence de décret d'application à la date de la délibération.

Cette décision traduit d'abord une approche pragmatique de l'encadrement du risque extraterritorial par la validation des garanties techniques et juridiques entourant l'hébergement nuage (**I**), mais révèle dans le même temps les limites structurelles d'une souveraineté numérique sanitaire encore inachevée, à l'heure où le droit européen de l'e-santé s'affirme avec l'EHDS (**II**).

I. LA VALIDATION PRAGMATIQUE DU RISQUE EXTRATERRITORIAL : UNE CONCILIATION ENTRE IMPÉRATIFS DE RECHERCHE ET PROTECTION DES DONNÉES

La décision du Conseil d'État s'inscrit dans une longue série de contentieux liés à l'hébergement du Health Data Hub par Microsoft. Elle témoigne d'une méthode de contrôle fondée sur la pondération concrète

[357] Article R. 1461-1 du code de la santé publique : interdit les transferts de données de santé issues du SNDS en dehors du territoire de l'Union européenne.
[358] RGPD, art. 45 : décision d'adéquation adoptée par la Commission européenne ; art. 46 : garanties appropriées en l'absence de décision d'adéquation.
[359] Décision d'exécution n° 2023/1795/UE de la Commission du 10 juillet 2023 constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis (*Data Privacy Framework*), *JOUE* n° L 231 du 20 juillet 2023.
[360] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (SREN), art. 31 : obligation pour les administrations gérant des données sensibles de recourir à des prestataires titulaires de la qualification SecNumCloud délivrée par l'ANSSI.
[361] Article L. 1111-8 du Code de la santé publique : certification « hébergeur de données de santé » (HDS), délivrée après audit régulier par un organisme accrédité par le COFRAC.
[362] RGPD, art. 32 : obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées, comprenant notamment la pseudonymisation, le chiffrement, et la garantie de la disponibilité et de la résilience des systèmes.

des risques plutôt que sur une approche absolutiste de la souveraineté numérique. Le juge administratif valide la délibération de la CNIL en distinguant soigneusement, d'une part, l'absence de transfert de données de santé vers les États-Unis (**A**) et, d'autre part, la suffisance des garanties techniques et contractuelles entourant les rares transferts de données non médicales (**B**).

A. L'absence de transfert de données de santé : une délimitation stricte de l'objet de l'autorisation

Le Conseil d'État pose en premier lieu un constat déterminant, qui dessine le périmètre du contrôle juridictionnel. La délibération du 13 février 2025 [363] a pour seul objet d'autoriser un traitement de données de santé hébergées sur des serveurs situés en France. Elle *« n'a pas pour objet et ne saurait avoir pour effet »* d'autoriser un transfert de données vers les États-Unis. Cette qualification est décisive, car elle neutralise l'ensemble des moyens construits sur l'hypothèse d'un tel transfert, qu'il s'agisse de l'exception d'illégalité de la décision d'adéquation UE-États-Unis *(Data Privacy Framework)* ou de la violation de l'article R. 1461-1 du code de la santé publique[364] qui prohibe les transferts de données du SNDS hors de l'Union européenne.

Cette démarche de délimitation stricte de l'objet de l'autorisation est juridiquement rigoureuse. En droit du RGPD, le régime des transferts vers des pays tiers *(articles 44 à 49)* ne s'applique que lorsqu'il y a effectivement communication de données à un destinataire situé hors de l'Union européenne. Dès lors que les données de santé demeurent hébergées sur le territoire français, dans des centres de données localisés en France, les dispositions relatives aux décisions d'adéquation[365] n'ont vocation à s'appliquer ni directement ni par voie d'exception. Le raisonnement du Conseil d'État est ici cohérent avec la lettre du règlement.

On peut néanmoins s'interroger sur la portée réelle de cette délimitation. Comme le Conseil d'État le reconnaît lui-même au considérant 10, le risque d'accès extraterritorial fondé sur les lois américaines, au premier rang desquelles le CLOUD Act, *« ne peut être totalement exclu »*. Cette reconnaissance implicite de l'imperfection structurelle du dispositif est significative. Elle traduit la tension inhérente à la désignation d'un hébergeur soumis à un ordre juridique extraterritorial, tension que le RGPD lui-même identifie à son article 48 sans y apporter de solution universelle. La CNIL avait d'ailleurs expressément reconnu dans sa propre délibération que *« les données stockées par un hébergeur soumis à un droit extra-européen peuvent être exposées à un risque de communication à des puissances étrangères »*. En décidant de valider malgré tout l'autorisation, le juge administratif opère une forme de mise en balance entre l'impératif de protection des données et le bénéfice scientifique et public du projet DARWIN EU.

B. La suffisance des garanties entourant les transferts résiduels de données techniques

Le Conseil d'État reconnaît l'existence de transferts de données vers les États-Unis, mais les cantonne à la catégorie des *«*

---

[363] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 66 : compétence de la CNIL pour autoriser les traitements de données de santé à des fins de recherche.

[364] CJUE, 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems*, aff. C-311/18 (ECLI:EU:C:2020:559), dit « Schrems II » : invalidation du Privacy Shield, exigence de vérification au cas par cas des garanties offertes par le pays destinataire.

[365] RGPD, art. 48 : « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international […] ».

données techniques d'usage de la plateforme » : informations relatives aux connexions des utilisateurs, sans aucune donnée de santé. Pour ces transferts résiduels, il vérifie que les garanties prévues à l'article 46 du RGPD sont respectées, en l'espèce à travers des clauses contractuelles types (CCT). Ce faisant, il applique la méthode de contrôle *in concreto* imposée par l'arrêt *Schrems II* de la CJUE[366] : les clauses contractuelles ne sont pas suffisantes par elles-mêmes, mais doivent être complétées par une appréciation des circonstances concrètes du cas d'espèce.

S'agissant des données de santé à proprement parler, le Conseil d'État examine avec soin les mesures techniques et organisationnelles au regard des articles 28 §1 et 32 du RGPD[367]. Il recense : la pseudonymisation réalisée sous le contrôle de la Caisse nationale d'assurance maladie et de la PDS, la limitation de la durée de conservation des données brutes extraites du SNDS, l'analyse systématique des risques de réidentification lors de chaque export, et le contrôle des traces d'utilisation par la PDS. Il relève également que Microsoft Ireland, bien qu'incapable d'obtenir la qualification SecNumCloud, réservée aux prestataires non soumis à un droit extra-européen, est titulaire de la certification « hébergeur de données de santé » (HDS) prévue par l'article L. 1111-8 du code de la santé publique[368], impliquant un audit régulier par un organisme accrédité.

Ce raisonnement appelle plusieurs observations critiques. En premier lieu, le juge administratif n'entre pas dans une analyse comparative entre la certification HDS et la qualification SecNumCloud, dont les exigences en matière d'immunité face aux législations extraterritoriales sont pourtant d'une nature différente. La doctrine cloud de l'État[369], confirmée par la circulaire du Premier ministre du 5 février 2026, impose précisément le recours à la qualification SecNumCloud pour les systèmes traitant des données particulièrement sensibles, afin de les *« immuniser contre toute demande d'autorité publique d'États tiers »*. Or le Conseil d'État semble accepter que la certification HDS puisse, en l'espèce et à titre temporaire, se substituer à cette exigence de souveraineté, sans expliciter les raisons juridiques de cette équivalence fonctionnelle. En second lieu, la durée limitée de trois ans de l'autorisation délivrée, sur laquelle le juge insiste, constitue moins une garantie juridique qu'un outil de gestion du risque dans le temps.

Si la décision valide le dispositif mis en place, elle révèle dans le même temps les insuffisances d'un cadre juridique qui peine à concilier les ambitions de la politique européenne des données de santé avec les réalités du marché du cloud. C'est cette tension structurelle qu'il convient d'examiner à présent.

---

[366] Circulaire du Premier ministre du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État, complétée par la circulaire du 5 février 2026 : exigence de solutions qualifiées SecNumCloud pour les données sensibles et les systèmes critiques.

[367] CNIL, délibération précitée, point sur la recommandation : « La CNIL ne peut qu'inciter à nouveau le Gouvernement et la Plateforme des données de santé à travailler activement à la mise en place d'une solution souveraine permettant aux organismes d'avoir accès rapidement aux données du SNDS à des fins de recherche scientifique ».

[368] Annonce du gouvernement du 7 février 2026 : la ministre de la Santé Stéphanie Rist a annoncé la migration du Health Data Hub vers un hébergeur qualifié SecNumCloud, avec appel d'offres lancé le 6 mars 2026 ; attribution prévue fin mars 2026.

[369] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 5 mars 2025 relatif à l'espace européen des données de santé (EHDS), JOUE n° L 96 du 5/04/2025 : vise à garantir aux citoyens l'accès à leurs données de santé électroniques dans toute l'Union et à encadrer l'usage secondaire de ces données pour la recherche et l'innovation.

II. LES LIMITES STRUCTURELLES D'UNE SOUVERAINETÉ NUMÉRIQUE SANITAIRE INACHEVÉE : L'APPEL À UNE GOUVERNANCE COHÉRENTE DES DONNÉES DE SANTÉ EUROPÉENNES

La décision du Conseil d'État du 20 mars 2026 s'inscrit dans un contexte de transition normative accélérée. Elle intervient alors que la question de l'hébergement souverain du Health Data Hub demeure en suspens depuis la création de la plateforme en 2019, et que le règlement européen sur l'espace européen des données de santé *(EHDS)* vient d'entrer en vigueur. Elle met en lumière tant l'inapplication provisoire de la loi SREN, révélatrice des difficultés de mise en œuvre du principe de souveraineté numérique (A), que la nécessité d'une articulation cohérente entre les ambitions de l'EHDS et les conditions concrètes d'hébergement des données de santé (B).

A. L'inapplication de la loi SREN : les difficultés de la souveraineté numérique comme impératif juridique

Le quatrième moyen soulevé par les requérants était tiré de la méconnaissance de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique. Cet article fixe les conditions dans lesquelles les administrations peuvent recourir à des services d'informatique en nuage fournis par des prestataires privés pour des systèmes ou applications informatiques. Il impose, pour les données sensibles, le recours à des offres titulaires de la qualification SecNumCloud de l'ANSSI. Le décret d'application, que la loi prévoyait dans un délai de six mois à compter de sa promulgation, n'avait pas été adopté à la date de la délibération du 13 février 2025. Le Conseil d'État en déduit que les dispositions de cet article n'étaient *« pas invocables »* à l'encontre de la délibération contestée.

Ce raisonnement est formellement correct : un texte législatif qui subordonne lui-même son entrée en vigueur à la publication d'un décret d'application ne peut être opposé aux actes pris avant cette publication. Mais il révèle une situation paradoxale. La loi SREN traduit une volonté politique claire d'ériger la souveraineté numérique en exigence juridique contraignante pour les administrations gérant des données sensibles. Le dépassement du délai de six mois prévus par le législateur pour la publication du décret d'application constitue une carence réglementaire qui a pour effet de priver la loi d'effectivité, précisément dans un contexte où les enjeux de souveraineté étaient au cœur du litige. La CNIL avait elle-même, dans sa délibération, formulé une recommandation explicite en faveur d'un hébergeur souverain, soulignant implicitement l'inadéquation du dispositif existant.

Cette tension entre l'impératif normatif et l'impossibilité pratique immédiate illustre l'un des problèmes récurrents de la souveraineté numérique française : l'absence d'équivalent souverain opérationnel pour des besoins aussi spécifiques que ceux du Health Data Hub. La CNIL avait expressément noté l'impossibilité de trouver une solution souveraine *« susceptible de répondre à ses besoins tout en protégeant les données du SNDS contre les accès des autorités publiques d'État tiers »*. C'est cette réalité économique et technique qui a conduit à l'autorisation provisoire sous conditions. Ce n'est qu'en février 2026 que le gouvernement a officiellement décidé de migrer le Health Data Hub vers un hébergeur qualifié SecNumCloud, avec un appel d'offres lancé le 6 mars 2026, signalant que la décision du Conseil d'État n'épuise pas la question mais la reporte au plan politique.

B. L'avenir de la gouvernance des données de santé : vers une exigence renforcée de souveraineté dans l'espace européen des données de santé (EEDS)

La décision commentée s'inscrit dans un contexte normatif européen en pleine mutation. Le règlement sur l'espace européen des données de santé du 11 février 2025 constitue l'aboutissement d'un projet qui trouve son origine dans la directive 2011/24/UE relative aux soins transfrontaliers, laquelle avait créé le réseau e-santé, posé les jalons de l'interopérabilité des systèmes et amorcé la coopération entre la Commission et les représentants des Etats membres au sein de ce réseau en matière d'e-prescriptions. Le règlement franchit une étape qualitative en imposant des règles communes pour l'utilisation primaire et secondaire des données de santé électroniques à l'échelle de l'Union, avec des obligations de mise à disposition pesant sur les détenteurs de données, et la création de deux infrastructures transfrontalières d'échange *(MyHealth@EU pour les données primaires et HealthData@EU pour les données secondaires).*

Or, ce nouvel espace européen, qui sera mis en oeuvre progressivement soulève des questions de gouvernance directement en lien avec l'affaire DARWIN EU. Le règlement prévoit en effet la désignation, dans chaque État membre, d'un organisme responsable de l'accès aux données de santé *(« HDAB » ou « ORAD »),* chargé notamment de maintenir un environnement de traitement sécurisé. Il impose des règles strictes quant aux finalités de l'usage secondaire des données et aux garanties protégeant les droits des personnes concernées, incluant un droit de refus *(opt out).* En revanche, le règlement ne tranche pas expressément la question de l'hébergeur : il se contente d'exiger un *« environnement de traitement sécurisé »*, laissant aux États membres une marge d'appréciation sur les modalités techniques. Cette lacune risque de reproduire, à l'échelle européenne, les difficultés observées en France avec le Health Data Hub sauf à développer une solution souveraine au niveau européen.

Le projet DARWIN EU[370] lui-même illustre les tensions que l'EHDS sera appelé à résoudre. Une double base juridique a été retenue pour le règlement EHDS, fondé sur les articles 114 et 16 du TFUE. L'article 114 TFUE, relatif au marché intérieur, habilite l'Union à adopter des mesures d'harmonisation des législations nationales ayant pour objet l'établissement et le fonctionnement du marché intérieur tandis que l'article 16 du TFUE constitue, quant à lui, le fondement du droit fondamental à la protection des données à caractère personnel : il dispose que « *toute personne a droit à la protection des données à caractère personnel la concernant* » et habilite le Parlement européen et le Conseil à fixer les règles relatives à ce droit, c'est-à-dire le cadre même du RGPD. L'article 16 TFUE fonde matériellement les dispositions de l'EHDS relatives aux droits des patients sur leurs données. Il est à noter que l'article 168§ 4 c) TFUE relatif aux normes de qualité et de sécurité des dispositifs médicaux n'a pas été retenu comme base juridique de l'EHDS, choix critiqué par une partie de la doctrine eu égard à la dimension qualité des soins du règlement. Le projet DARWIN.EU[371] soulève simultanément des enjeux de marché intérieur des données et des enjeux de protection des données personnelles de santé. Or, ni l'un ni l'autre de ces fondements ne règle la question de la protection des données face aux législations extraterritoriales, qui relève du RGPD et des choix d'hébergement opérés par les États membres et les institutions européennes.

Cependant, la décision du Conseil d'État valide un état transitoire sans fixer de critères précis permettant de déterminer à partir de quel seuil les garanties techniques

[370] V. site officiel.

[371] https://darwin-eu.org/

ne sauraient plus suppléer l'absence de souveraineté juridique de l'hébergeur. En reconnaissant que le risque d'accès extraterritorial *« ne peut être totalement exclu »* tout en le jugeant acceptable, le juge administratif s'engage sur un terrain d'appréciation casuistique qui, s'il peut se justifier dans un contexte de transition, ne saurait constituer une doctrine durable de gouvernance des données de santé. L'article 48 du RGPD, qui interdit la reconnaissance de toute injonction de transfert d'une juridiction d'un pays tiers non fondée sur un accord international, demeure une protection formelle dont l'effectivité réelle, en cas de demande fondée sur le CLOUD Act, reste incertaine ainsi que le souligne la doctrine.

En définitive, l'arrêt du 20 mars 2026 apporte une réponse juridique solide aux questions de droit positif, mais laisse en suspens les enjeux de politique publique numérique que la construction de l'EHDS et la migration vers un hébergeur souverain devront collectivement résoudre. Il confirme que le droit de la e-santé européen, ce droit *sui generis* en construction, ne peut se passer d'une architecture de gouvernance des données cohérente, associant exigences juridiques, capacités techniques et souveraineté numérique opérationnelle. La récente annonce de la migration de l'hébergement vers Scaleway, une solution française, fait parfaitement suite à cette succession de polémiques et illustre par ailleurs les recompositions actuellement à l'œuvre en matière de souveraineté numérique et d'hébergement des données de santé : la souveraineté est amenée à devenir un enjeu de premier ordre[372].

CE, Section du contentieux, 10ème chambre, 26 mars 2026, n°s 503159-504171, ECLI:FR:CECHS:2026:503159.20260320.

[372] « Le Health Data Hub choisit l'hébergeur français Scaleway", Léo Caravagna et Marion-Jeanne Lefebvre,Tic Pharma, 24/04/2026

Bulletin de
l'EDiHL
European Digital Health Law

LISTE DES CONTRIBUTEURS

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

Franck AZNAR
Diplomé en biotechnologies, biologie moléculaire et cellulaire
Titulaire du DU EDiHL

Sarah BISTER
Avocate au Barreau de Paris
Docteure en Droit public

Claire BORIES
Docteure en Droit public
Chargée de mission à la Direction de la Sécurité sociale (DSS/DACI)

Thomas BOUDON
Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Maïlys CAPELL
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Maddalena DE CARLO
Etudiante en Master 2 Droit international et comparé, École de droit de Toulouse, Université Toulouse Capitole

Sarah DE HEER
Doctorante en Droit public, Université de Lund (Suède)

Marie DESMEULES
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Winnie DONGBOU WAMBA
Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

Noémie DUBRUEL
Docteure en Droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Lisa FERIOL
Doctorante CIFRE, Ekitia et Équipe BIOETHICS, CERPOP UMR1295 Inserm et Université Toulouse Paul Sabatier

Alizée FERNANDEZ
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Lili-Marie FERRANDO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Joud GHARZEDDINE
Étudiante en Master 2 Droit des Libertés et titulaire du Master Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Chaimae HBA
Étudiante en Master 1 Droit du numérique IA, École de droit de Toulouse, Université Toulouse Capitole

Clarance JEAN-PIERRE
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Lukas MARA
Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Amina MOUSTOIFA
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Mélanie SOUSA BARBEIRO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Salaheddine ZAHID
Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Bulletin de l'EDiHL

European Digital Health Law



N° 3

3ème année – Bulletin annuel
Juin 2025 – Juin 2026

Cofinancé par l'Union européenne

LISTE DES CONTRIBUTEURS 2023-2026

Chaire Jean Monnet « Droit européen du numérique en santé » 2023-2026

Bulletin de l'EDiHL
European Digital Health Law

Direction scientifique

Nathalie DE GROVE-VALDEYRON
Professeure de Droit public, École de droit de Toulouse, Université Toulouse Capitole

Claire BORIES
Docteure en Droit public
Chargée de mission à la Direction de la Sécurité sociale (DSS/DACI)

Docteures et professionnels du droit

Sarah BISTER
Avocate au Barreau de Paris
Docteure en Droit public

Claire BORIES
Docteure en Droit public
Chargée de mission à la Direction de la Sécurité sociale (DSS/DACI)

Noémie DUBRUEL
Docteure en Droit de la santé, IMH Université Toulouse Capitole & Cerpop Université Paul Sabatier, UMR 1295 Inserm équipe BIOETHICS

Doctorants et jeunes chercheurs

FRANCK AZNAR
Diplomé en biotechnologies, biologie moléculaire et cellulaire
Titulaire du DU EDiHL

Sarah DE HEER
Doctorante en Droit public, Université de Lund (Suède)

Winnie DONGBOU WAMBA
Doctorant en Droit public, EDT-R-IRDEIC, Université Toulouse Capitole
Juriste en droit de la protection des données de santé MyData-TRUST

Valentine DURAND
Doctorante en Droit public, Thèse CIFRE (Ipsen), IRDEIC, École de droit de Toulouse, Université Toulouse Capitole

Lisa FERIOL
Doctorante CIFRE, Ekitia et Équipe BIOETHICS, CERPOP UMR1295 Inserm et Université Toulouse Paul Sabatier

Étudiantes et étudiants

Thomas BOUDON
Étudiant en Master 1 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Maïlys CAPELL
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Dorianne CATTOEN
Titulaire du Master de Droit européen, École de droit de Toulouse, UniversitéToulouse Capitole

Maddalena DE CARLO
Étudiante en Master 2 Droit international et comparé, École de droit de Toulouse, Université Toulouse Capitole

Marie DESMEULES
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Nino ESCUDIER
Titulaire du Master de Droit européen, École de droit de Toulouse, UniversitéToulouse Capitole

Alizée FERNANDEZ
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Lili-Marie FERRANDO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Joud GHARZEDDINE
Étudiante en Master 2 Droit des Libertés et titulaire du Master Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Luis HALEGA
Tutulaire du Master Droit de la santé et de la protection sociale, Université Toulouse Capitole

Chaimae HBA
Étudiante en Master 1 Droit du numérique IA, École de droit de Toulouse, Université Toulouse Capitole

Clarance JEAN-PIERRE
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Shana LEVI
Titulaire du Master DIDE, École de droit de Toulouse, Université Toulouse Capitole

Lukas MARA
Étudiant en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Romane MASSIMI
Titulaire du Master Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Maximilien MAUGEAIS
Titulaire du Master Droit du numérique, Université Paris Panthéon-Sorbonne

Kévin MINGOT
Titulaire du Master Droit de la santé, École de droit de Toulouse, Université Toulouse Capitole

Amina MOUSTOIFA
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Pierre-Emmanuel PARENT DE CURZON
Titulaire du Master Juriste européen, École de droit de Toulouse, Université Toulouse Capitole

Mélanie SOUSA BARBEIRO
Étudiante en Master 2 Droit de la Santé, École de droit de Toulouse, Université Toulouse Capitole

Salaheddine ZAHID
Étudiant en Master 2 Juriste européen et titulaire du diplôme EDiHL, École de droit de Toulouse, Université Toulouse Capitole

Bulletin de

l'EDiHL

European Digital Health Law

RECUEIL DES BULLETINS DE L'EDiHL

2023-2026

Volumes 1 à 3