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

Droit français

VEILLE CONTENTIEUSE

Droit de l'Union européenne

Droit français

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.

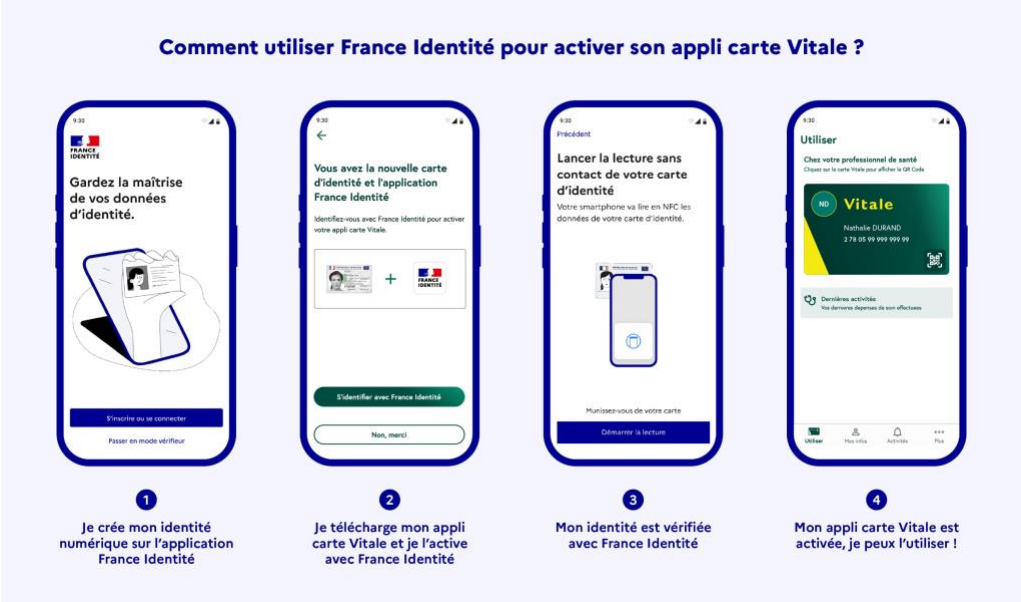
Conseil Constitutionnel, Décision du 28 février 2025 n° 2025-875 DC

[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