



HAL
open science

Regard européen sur le guide de l’OMS pour l’éthique et la gouvernance de l’intelligence artificielle dans le secteur de la santé

Audrey Dequesnes

► **To cite this version:**

Audrey Dequesnes. Regard européen sur le guide de l’OMS pour l’éthique et la gouvernance de l’intelligence artificielle dans le secteur de la santé. *Revue générale de droit médical*, A paraître, *Revue générale de droit médical*, 81. hal-03465019v1

HAL Id: hal-03465019

<https://hal.univ-lille.fr/hal-03465019v1>

Submitted on 3 Dec 2021 (v1), last revised 24 Nov 2023 (v2)

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

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

Regard européen sur le guide de l’OMS pour l’éthique et la gouvernance de l’intelligence artificielle dans le secteur de la santé

Audrey Dequesnes

Univ. Lille, CNRS, UMR 8026 – CERAPS – Centre d’Études et de Recherches Administratives Politiques et Sociales, F-59000 Lille, France

En juin 2021, l’Organisation mondiale de la santé a publié ses lignes directrices pour l’éthique et la gouvernance de l’intelligence artificielle dans le domaine de la santé. Le rapport, qui expose un panorama des utilisations des systèmes d’intelligence artificielle dans la santé, dégage des enjeux éthiques cruciaux auxquels les destinataires du guide, à savoir principalement les pouvoirs publics en charge de la santé et du numérique, vont devoir apporter une réponse appropriée. Pour avoir des effets tangibles, cette réponse devra être juridique, en particulier en ce qui concerne l’attribution de la responsabilité en cas de dommage causé par l’un de ces systèmes, ainsi que la gouvernance des données de santé. Alors que l’Union européenne est en voie de se doter d’un règlement dédié aux systèmes d’intelligence artificielle, ces points indispensables à la garantie de droits fondamentaux devront retenir l’attention du législateur.

Mots clés : OMS – intelligence artificielle – données de santé – responsabilité – règlement européen sur l’IA.

In June 2021, the World Health Organization published its Guidance on ethics and governance of artificial intelligence for health. The report provides an overview of the uses of artificial intelligence systems in health and identifies crucial ethical issues to which the recipients of the guide, mainly public authorities in charge of health and digital technology, will have to respond appropriately. In order to produce tangible effects, this response will have to be legal, in particular with regard to the attribution of liability in the event of damage caused by one of these systems, as well as the governance of health data. As the European Union is drafting a regulation dedicated to artificial intelligence systems, these points, which are key to safeguarding fundamental rights, will need to be carefully considered by the legislator.

Key words: WHO – artificial intelligence – health data – liability – EU regulation on AI.

L’organisation mondiale de la santé (OMS) a publié ses lignes directrices pour l’éthique et la gouvernance de l’intelligence artificielle (IA) dans la santé, sous l’intitulé original *Ethics and governance of artificial intelligence for health: WHO guidance*¹. Ce rapport est le fruit de deux années de travail, réalisé notamment par le département de recherche en santé et celui de

¹ OMS, *Ethics and governance of artificial intelligence for health: WHO guidance*, 28 juin 2021.

santé numérique et d'innovation. De nombreux experts, observateurs et relecteurs extérieurs de vingt-cinq pays, issus du secteur public – académique et administratif – et du secteur privé – entreprises et associations ont également contribué à cette publication. Publié le 28 juin 2021, ce rapport intègre des enseignements de la crise sanitaire du Covid-19, qui a eu un impact fort sur le développement des outils numériques dans la santé et en particulier de l'IA². Ce guide s'inscrit dans la lignée des nombreux outils d'éthique et de droit souple qui ont été publiés jusqu'alors. Nous pouvons citer en particulier en Europe les travaux du groupe d'experts de haut niveau sur l'IA mis en place par la Commission européenne³ qui ont donné lieu entre autres au *Livre blanc sur l'IA* de la Commission européenne⁴, mais aussi les travaux de l'Organisation de coopération et de développement économique (OCDE) pour une IA digne de confiance dans la santé⁵ et ses recommandations juridiques sur l'IA⁶. Le Conseil de l'Europe s'est aussi emparé de la question, avec une attention particulière pour le respect des droits et libertés fondamentaux et de la gouvernance des algorithmes⁷. Cette liste n'est pas exhaustive et n'évoque que les émanations d'organisations supranationales avec un cadrage européen. Toutefois les nombreux documents disponibles sur ce sujet ont en commun de vouloir proposer un cadre commun pour le développement de l'IA qui soit éthique, centré sur l'humain, tout en promouvant l'innovation afin que la société bénéficie pleinement du potentiel de l'IA. La santé est un domaine où l'éthique tient une place prépondérante, et pour lequel l'IA a des applications innombrables et variées, ces deux facteurs expliquant qu'il fasse l'objet d'une attention particulière et de volontés d'orientations stratégiques⁸. Le guide de l'OMS trouve sa pertinence dans l'absence de directives internationales complètes sur l'utilisation de l'IA, et l'Organisation a l'intention de créer ainsi un cadre protecteur et harmonisé pour un développement positif de l'IA dans la santé⁹. Cependant, l'Union européenne semble être en voie de concevoir un cadre juridique dédié à l'IA, dont nous disposons pour le moment d'une version préliminaire, par la proposition de règlement sur l'intelligence artificielle de la Commission européenne¹⁰. Nous comparerons, lorsque ce sera opportun, le guide de l'OMS à ce premier outil de nature juridique voué à

² Conseil de l'Europe, « IA et lutte contre le coronavirus Covid-19 » [en ligne], 2020, disponible sur <https://www.coe.int/fr/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus> [consulté le 18 octobre 2021].

³ High-level expert group on artificial intelligence (AI-HLEG), *A definition of AI: Main capabilities and scientific disciplines*, 8 avril 2019 ; AI-HLEG, *Ethics guidelines for trustworthy AI*, 8 avril 2019 ; AI-HLEG, *Policy and investment recommendations for trustworthy AI*, 26 juin 2019 ; AI-HLEG *Assessment List for Trustworthy AI*, 17 juillet 2020 ; AI-HLEG, *Sectoral considerations on the policy and investment recommendations for trustworthy artificial intelligence*, 23 juillet 2020.

⁴ Commission européenne, *Livre blanc sur l'intelligence artificielle, Une approche européenne axée sur l'excellence et la confiance*, 19 février 2020.

⁵ OCDE, *Trustworthy AI in health*, avril 2020.

⁶ OCDE, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0049, 2020.

⁷ Cons. Europe, « Politiques, recommandations, déclarations, lignes directrices et autres instruments juridiques publiés par les organes ou comités du Conseil de l'Europe sur l'intelligence artificielle » [en ligne], mise à jour du 5 octobre 2021, disponible sur <https://www.coe.int/fr/web/artificial-intelligence/work-inprogress#01FR> [consulté le 27 octobre 2021].

⁸ UNESCO, *Projet de recommandation sur l'éthique de l'intelligence artificielle*, SHS/IGMAIETHICS/2021/JUN/3 Rev.2, 25 juin 2021, p. 27.

⁹ OMS, *Ethics and governance of artificial intelligence for health: WHO guidance*, 28 juin 2021, p. 2-3.

¹⁰ Commission européenne, « Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union », COM/2021/206 final, 21 avril 2021.

encadrer directement l'IA, les deux documents ayant été rendus publics à seulement deux mois d'intervalle.

Ce guide et les recommandations qu'il contient, s'adressent principalement aux ministères de la santé, mais aux agences gouvernementales en charge de la santé et du numérique, aux ministères en charge du numérique ou des technologies de l'information, ainsi qu'aux entreprises et diverses entités qui seront amenées à concevoir des IA dans le domaine de la santé.

Le contenu du rapport présente des éléments de deux natures : les six premières sections sont de l'ordre du constat, tandis que les trois dernières sections et l'annexe sont à vocation prescriptrices. Après avoir introduit l'intérêt de l'IA dans le domaine de la santé et ses principales préoccupations en la matière, l'OMS définit l'IA de façon pragmatique comme des technologies basées sur des algorithmes capables d'exécuter des tâches sans que chaque étape ne doive être programmée par un humain, en apprenant à partir de données. Les nombreuses utilisations de l'IA en santé sont décrites, suivies des dispositions réglementaires existantes applicables à l'IA, puis des six principes éthiques clés et des enjeux éthiques de l'utilisation de l'IA dans la santé. Forts de cet état des lieux, les rapporteurs émettent alors des propositions pour la construction d'un cadre éthique et juridique approprié à l'IA.

Les six principes éthiques clés, développés dans le guide, sont la protection de l'autonomie des personnes, la promotion du bien-être, de la sécurité et de l'intérêt public, la garantie de transparence, l'intelligibilité et l'explicabilité, la promotion de la responsabilité des acteurs et l'obligation de rendre des comptes en cas de dommages, la garantie d'inclusivité et d'équité, et enfin la promotion d'une IA qui soit adaptable et s'inscrive dans une démarche durable pour la société et l'environnement.

Face à ces enjeux éthiques majeurs, nous pouvons distinguer dans ce guide deux aspects juridiques qui seront les clés d'une mise en œuvre éthique de l'IA dans le secteur de la santé, bien que l'OMS émette d'autres recommandations nécessaires à une gouvernance globale. Il s'agit, d'une part, de l'existence de régimes de responsabilité adaptés (I) et, d'autre part, d'un cadre de gouvernance des données de santé qui permette le respect des libertés et droits fondamentaux, et s'inscrive dans la stratégie globale de l'OMS pour une couverture santé universelle (II).

I. Des régimes de responsabilité à adapter à l'IA dans le domaine de la santé

Aussi évolués et performants que puissent être ou devenir les systèmes d'IA, des risques restent évidemment à prévoir, notamment s'agissant de leurs utilisations dans un domaine aussi sensible que celui de la santé. Afin de faire face à ces risques, des régimes de responsabilité doivent pouvoir s'appliquer dans tous les cas de figure, avec « au moins les mêmes standards et réparations »¹¹ que ceux déjà applicables dans le domaine de la santé, voire des dispositions particulières.

Pour assurer un niveau de réparation suffisant, la responsabilité des utilisateurs, des fournisseurs et fabricants de systèmes d'IA devra être explorée (A), mais aussi l'hypothèse de dispositifs de réparation sans responsabilité (B), tout en gardant à l'esprit les difficultés supplémentaires des régions du monde où ces différents mécanismes seraient plus complexes à appliquer (C).

A. A la recherche des responsabilités : entre utilisateur et fournisseur

Afin de clarifier le propos, nous identifierons l'utilisateur comme la personne physique ou morale qui se sert d'un système d'IA notamment au service d'un patient ou du suivi de sa propre activité, soit, non-exhaustivement, les professionnels et établissements de santé ; le fournisseur (parfois nommé développeur ou fabricant dans le guide de l'OMS) est l'organisme qui développe ou fait développer un système d'IA en vue de sa mise sur le marché ; le fabricant est celui qui met sur le marché un produit intégrant un système d'IA qui en est indissociable, et se substitue alors au fournisseur. Ces acceptions des termes, bien que reprises dans une logique simplificatrice qui omet les distributeurs, importateurs et mandataires, sont celles utilisées par la Commission dans sa proposition de règlement sur l'IA¹² et correspondent à la majorité des usages qui en sont fait dans le guide de l'OMS.

La première question, qui concerne directement les utilisateurs des systèmes d'IA, est de savoir si les médecins pourraient être tenus responsables d'avoir suivi les instructions d'une IA, ou à l'inverse de ne pas les avoir suivies, dans le cas où cette décision aboutirait à un préjudice au patient. Selon l'OMS, cela dépend avant tout d'un choix plus général de société face à l'IA, car si les médecins sont pénalisés par les règles de la responsabilité en cas d'erreur due à la machine, ils ne l'utiliseront que pour confirmer leurs conclusions. A l'inverse, s'ils ne sont pas responsables dans ce cas, cela équivaldrait à encourager les praticiens à utiliser l'IA à son plein potentiel, au-delà de leurs propres capacités et connaissances. Ce sont les recommandations des sociétés savantes et des autorités en matière de santé qui promouvront ou non l'utilisation de l'IA de manière étendue, en participant à défendre les praticiens d'une faute médicale. En France, la Haute autorité de santé (HAS) a commencé à s'emparer du sujet en 2019 avec son guide sur l'évaluation des dispositifs médicaux connectés¹². Il fournit de premières instructions aux industriels qui souhaiteraient obtenir un accès au remboursement pour un dispositif médical incluant un système expert de traitement de données basé sur un « algorithme apprenant »¹⁴. La HAS a ensuite intégré à partir de 2020 à son guide de dépôt de dossier pour accéder à la liste des produits et prestations remboursables un outil spécifique à

¹¹ OMS, *Ethics and governance of artificial intelligence for health: WHO guidance*, 28 juin 2021, p. 76.

¹² Art. 3, *Ibid.*, p. 45.

¹² HAS, *Guide sur les spécificités d'évaluation clinique d'un dispositif médical connecté (DMC) en vue de son accès au remboursement*, janvier 2019. ¹⁴ *Ibid.*, p.15.

l'évaluation des dispositifs médicaux embarquant un système d'apprentissage automatique¹³. En utilisant, conformément à l'usage prévu par le fabricant, des dispositifs médicaux remplissant les critères d'évaluation des autorités, les professionnels de santé ne verraient pas leur responsabilité engagée.

Une question connexe à celle de la responsabilité des praticiens est celle de la responsabilité des établissements de santé. Ils pourraient être responsables d'une négligence s'ils sélectionnent et mettent à disposition un outil qui est la source d'un dommage. Ce sont là aussi les recommandations des autorités et l'information fournie par le fournisseur qui permettront d'identifier les outils appropriés à l'usage clinique, mais les établissements pourraient avoir à démontrer qu'ils ont fait preuve de diligence dans leur choix.

Le régime de responsabilité appliqué aux systèmes dotés d'IA dépend du fait que les logiciels soient considérés ou non comme des produits. Pour l'OMS et donc à l'échelle internationale, ce point reste à éclaircir. En revanche concernant l'Union européenne, il l'a été par les règlements relatifs aux dispositifs médicaux et dispositifs médicaux de diagnostic *in vitro*¹⁴. En effet, ces règlements incluent explicitement les logiciels dans leur champ¹⁵, les qualifiant ainsi de produits de santé lorsque que leur finalité est de concourir aux soins de santé. Les règles de responsabilité des produits défectueux¹⁶ s'appliquent ainsi aux logiciels en tant que dispositifs médicaux, bien que deux limites soient relevées dans le guide de l'OMS : d'une part, les cas où l'utilisation effective d'un produit de ce type s'éloigne de la destination du logiciel telle que prévue par le fournisseur, et, d'autre part, le cas où le logiciel est présenté comme un service et non un produit. S'agissant de la première limite, les systèmes de matériovigilance en France et dans l'espace économique européen imposent aux fabricants et aux autorités compétentes une vigilance sur l'utilisation après la mise sur le marché ainsi qu'une surveillance du marché¹⁷. La seconde limite relevée n'est pas illustrée dans le document, mais ces logiciels-services pourraient hypothétiquement correspondre aux logiciels de gestion administrative, de réalisation de téléconsultations, ou encore aux fonctionnalités de signalement des interactions médicamenteuses – hors dosages propres à un patient – qui sont utilisés dans le secteur de la santé mais ne sont pas des dispositifs médicaux par définition, ou encore à des services basés sur l'IA qui seraient proposés directement au patient sans achat d'un produit, comme un diagnostic automatisé par un agent conversationnel (ou *chatbot*) en ligne.

¹³ Id., « Annexe 5 : Informations descriptives spécifiques à fournir pour les fonctionnalités du dispositif médical s'appuyant sur des procédés d'apprentissage automatique (technologies relevant du champ de l'intelligence artificielle) », *LPPR : Dépôt d'un dossier auprès de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS)*, version du 8 septembre 2021, p.45 et s.

¹⁴ Il s'agit des deux règlements du Parlement européen et du Conseil du 5 avril 2017 : le règlement (UE) 2017/745 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n°178/2002 et le règlement (CE) n°1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE*, 5 mai 2017, p.1-175 ; et le règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic *in vitro* et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, *JOUE*, 5 mai 2017, p. 176-332.

¹⁵ Voir le considérant 19 du règlement (UE) 2017/745 relatif aux dispositifs médicaux, ainsi que les définitions du dispositif médical et du dispositif médical de diagnostic *in vitro* dans l'article 2 de chacun des règlements ci-dessus.

¹⁶ Pour l'UE : Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux, *Journal officiel* n° L 210, du 7 août 1985, p. 29 – 33.

¹⁷ Les articles R.5212-14 et suivants du Code de la santé publique font référence à ces obligations en termes de matériovigilance, ainsi que les articles 10, 92 et 100 du règlement (UE) 2017/745 relatif aux dispositifs médicaux.

Si une utilisation étendue de la responsabilité du fabricant semble souhaitable, il pourrait s'avérer complexe pour les patients de prouver une défectuosité, de même qu'une faute, et donc d'obtenir réparation. Cela du fait, d'une part, de la complexité du produit et de ses mécanismes, et, d'autre part, des multiples intervenants entre la conception algorithmique, l'écriture du code, l'association à un éventuel dispositif matériel, la structure de soins et le professionnel de santé.

Concernant la première de ces deux raisons, le régime de responsabilité du fabricant serait vertueux dans la mesure où il encouragerait les développeurs à s'assurer de la sécurité de leurs produits et à mettre en place des mesures de sécurité (qui seront exposées dans la dernière section du guide), mais les failles de sécurité et les risques imprévisibles viennent fragiliser son utilité pour le patient. Face à ce risque, le Parlement européen a proposé dans sa résolution concernant la responsabilité civile pour l'IA d'octobre 2020 un régime de responsabilité sans faute pour les systèmes à « haut risque »¹⁸. Cependant, l'OMS soulève qu'il est difficile d'évaluer à quel point un développeur peut être tenu pour responsable sans faute à l'heure de l'utilisation grandissante des réseaux de neurones et des apprentissages profonds, car les performances du système d'IA pourraient être amenées à changer au cours du temps. Concernant la seconde raison de l'incertitude pour le patient d'obtenir réparation, à savoir la multiplicité des acteurs impliqués, la proposition de règlement sur l'IA de la Commission européenne désigne comme responsable le fournisseur d'un système d'IA¹⁹. Dans le cas d'un produit auquel est lié un système d'IA à haut risque, c'est le fabricant du produit, qui a mis ce dernier sur le marché sous son nom, qui doit assumer la responsabilité du système d'IA au même titre qu'un fournisseur dans le sens du règlement²⁰.

L'OMS souligne cependant, comme l'objectent de nombreux acteurs du marché de l'IA, qu'une telle acception de la responsabilité tendrait à diminuer le potentiel de l'IA à améliorer les soins. Une responsabilité sans faute pourrait être envisagée, à condition d'être complétée par la notion de tiers compétent que serait le professionnel de santé, afin que le fournisseur ne soit pas tenu responsable d'un dommage s'il a fourni une information adéquate sur l'utilisation et les risques à l'intermédiaire qu'est ledit professionnel.

B. Vers une réparation sans responsabilité

Les incertitudes autour de l'applicabilité des régimes de responsabilité évoqués amènent les auteurs du guide de l'OMS à envisager une réparation sans responsabilité ni faute, sur le modèle de l'indemnisation des dommages causés par les effets indésirables des vaccins. La preuve d'un défaut, et a fortiori d'un lien de causalité, paraissant difficile voire impossible à apporter pour la victime les victimes seraient dédommagées par un fond d'indemnisation, alimenté par des entreprises fournissant les systèmes d'IA, sur la constatation d'un dommage qui pourrait avoir été causé par l'IA. Concernant les vaccins, de tels mécanismes fonctionnent – dont celui organisé par l'OMS elle-même pour la vaccination contre le Covid-19 dans les pays à faible revenu – sur la base du constat chez la personne vaccinée de la manifestation d'un effet

¹⁸ Parlement européen, « Résolution du Parlement européen du 20 octobre 2020 portant recommandations à la Commission sur un régime de responsabilité civile pour intelligence artificielle », 2020/2014(INL), 20 octobre 2020, p. 23.

¹⁹ Ce fournisseur est défini dans l'article 3 de la proposition de règlement, et le considérant 53 explicite : « Il convient qu'une personne physique ou morale spécifique, définie comme étant le fournisseur, assume la responsabilité de la mise sur le marché ou de la mise en service d'un système d'IA à haut risque, indépendamment du fait que cette personne physique ou morale soit ou non la personne qui a conçu ou développé le système. », Commission européenne, « Proposition de règlement [...] concernant l'intelligence artificielle [...], *op. cit.*, p. 36.

²⁰ Article 24, *Ibid.*, p. 62

indésirable grave, rapporté dans la littérature scientifique, sans que la personne n'ait de preuve d'une faute à apporter. Si cette solution paraît enviable, rapporter ce schéma à l'IA semble pourtant périlleux : la nature des dommages potentiellement causés par chaque IA serait difficile à identifier, et leur liste serait en constante évolution.

Des considérations précédentes, nous pouvons constater que le contrôle réglementaire, par des systèmes d'évaluation et de validation, est amené à s'intensifier en matière d'IA. L'OMS émet alors l'hypothèse selon laquelle les décisions des agences en charge de cette validation vont supplanter toute autre forme de recours fondé sur le droit civil. Or, l'Organisation estime que ce ne serait pas forcément pertinent, notamment dans le cas où peu d'informations auraient été fournies pour l'autorisation, concernant l'évolution des performances de l'algorithme et sa conception. Le fait que les algorithmes puissent évoluer au cours du temps pose là aussi un obstacle à ce qu'un tel système de validation antérieurement à la mise sur le marché prévale sur d'autres systèmes de responsabilité.

C. Une nécessaire prise en compte des inégalités de développement

Toutes les solutions explorées ont toutefois comme point commun de nécessiter un système réglementaire avec ses capacités d'évaluation et de contrôle du marché, et des approches de la responsabilité qui sont, en réalité, ceux des pays occidentaux, en particulier des États-Unis et de l'Union européenne, qui les déploient déjà. Les pays à revenus faibles et intermédiaires sont alors confrontés à une double nécessité : celle d'accélérer l'usage des technologies basées sur l'IA pour pallier un manque d'infrastructures, en particulier de santé, et celle de garantir une utilisation vertueuse de ces systèmes, sûre et transparente, ce pour quoi un régime de responsabilité solide est indispensable. En effet, l'accès à la justice pouvant être difficile voire impossible, les populations les plus défavorisées se trouveraient davantage fragilisées sans régime de responsabilité adéquat. Une difficulté supplémentaire réside dans le fait que la plupart des systèmes d'IA est conçue en dehors des pays à faible revenu, où les entreprises ne sont souvent pas présentes. L'utilisation et l'efficacité mêmes des systèmes d'IA peuvent de fait être entravées par le manque de données d'entraînement dans le contexte de ces pays, créant des biais contextuels et donc des risques additionnels²¹, en plus de quoi un appareil judiciaire fragile ne permettrait pas à la population d'obtenir réparation pour les dommages causés. L'OMS rappelle que les pays concernés font face à des défis supplémentaires et différents des pays à hauts revenus, et qu'elle devra travailler avec les agences internationales et les gouvernements pour que des règles de responsabilité adéquates soient mises en place.

Finalement, quatre recommandations sont émises par l'OMS sur ce sujet. Tout d'abord les agences internationales et les sociétés professionnelles doivent s'assurer que leurs guidelines évoluent suffisamment rapidement pour tenir compte des technologies d'IA et de leur évolution. Ensuite, l'OMS devrait accompagner les agences réglementaires nationales dans l'évaluation des technologies d'IA utilisées dans la santé. Elle devrait aussi les accompagner pour évaluer les régimes de responsabilité mis en place, en veillant à ce qu'ils soient adaptés aux différents contextes et systèmes de santé. Enfin, l'organisation et les agences partenaires doivent chercher à établir des normes internationales et des standards pour assurer une responsabilité nationale pour protéger les patients contre les erreurs médicales. Les régimes de responsabilité jouent une

²¹ Ces risques sont d'autant plus prégnants en matière de santé, car les données phénotypiques (les caractères observables) comme génotypiques (les caractères génétiques) entraînant les algorithmes peuvent varier sensiblement d'une population à l'autre, de même que les prises en charge selon l'environnement, la réponse aux traitements, et d'autres traits particuliers des populations.

part importante dans le déploiement éthique et sûr des systèmes d'IA dans la santé. Pour autant, ils ne sont pas suffisants et appellent des règles de gouvernance plus générales.

II. De nombreux enjeux liés aux à la gouvernance des données

Les divers éléments techniques, organisationnels et juridiques liés à l'IA dans le secteur de la santé, rappelés dans les premières sections du document étudié, appellent à ce que de nombreux aspects de l'environnement réglementaire de l'IA soient encadrés. L'IA doit être développée selon les standards éthiques dégagés par l'OMS, mais aussi en respectant les droits fondamentaux, et les lois concernant la vie privée et la protection des données. Bien que gouvernée en partie par ce corpus législatif préexistant, l'IA amène des nouveaux défis qui nécessitent un encadrement supplémentaire. Les politiques de santé devront adapter de nombreux paramètres pour que le numérique dans la santé participe à l'accomplissement des objectifs de santé publique, et à la mission de l'OMS, qui est une couverture sanitaire universelle.

Le principal enjeu est celui de la gouvernance des données, qui relève du droit à la vie privée, de la liberté de consentement, de transparence et de partage des données et de leurs bénéfices. Ces données sont en effet le terrain de tiraillements, entre la vie privée et l'intérêt général (A), entre partage et centralisation (B), et entre appropriation et libre circulation (C).

A. Une atténuation de la vie privée au bénéfice de l'intérêt général

Pour l'OMS, les mécanismes habituels de contrôle par l'utilisateur tels que le consentement éclairé, la confidentialité des données, ou le fait de rendre les données non-identifiantes ne sont pas suffisants pour préserver les droits fondamentaux des patients, et ne permettent pas non plus le développement de tous les usages de l'IA.

Des approches nouvelles du consentement sont explorées, dans le but de permettre une plus large réutilisation des données de santé dans un objectif d'amélioration générale des connaissances et de la santé. Au sein de l'Union européenne, le traitement des données de santé est autorisé lorsqu'il est nécessaire à l'intérêt public, notamment pour garantir une qualité et une sécurité élevée des soins et des produits de santé, ou pour la recherche scientifique²². Une conception qui deviendrait trop large ou détournée de la notion d'intérêt public pourrait cependant, selon l'OMS, mener à établir des usages à « faible risque » pour lesquels le bénéfice de partager des données personnelles de santé sans consentement serait toujours plus important que ce risque considéré comme faible de violation de la vie privée. Du moment que ce partage aurait lieu dans le but d'améliorer la santé, y compris par la surveillance de certaines maladies ou le développement de nouveaux médicaments, le principe de respect de la vie privée se trouverait amoindri. L'OMS s'inquiète aussi de la définition que peuvent donner les gouvernements de l'intérêt général, afin d'éviter que les données soient partagées avec des entreprises sous prétexte d'améliorer la santé, quand ces entreprises pourraient ne pas faire bénéficier la population des produits ou services ainsi développés. Le guide rapporte que le Japon a résolu ces problèmes d'une façon innovante, en instaurant des intermédiaires qui sont

²² Article 9, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JOUE*, 4 mai 2016, p. 38 – 39.

chargés d'anonymiser les données collectées auprès des patients dans les hôpitaux, après information et avec la possibilité d'exprimer son refus, de stocker ces données en respectant des hauts standards de cybersécurité, et de les rendre disponibles pour la recherche, qu'elle soit publique ou privée, moyennant des frais d'accès. Cette solution ne va pas sans rappeler la mise en place, en France, de la plateforme de données de santé (ou *Health Data Hub*), qui sera amenée à remplir ce rôle d'intermédiaire²³, mais de façon centralisée et sous la forme d'un groupement d'intérêt public plutôt que de multiples acteurs privés.

Le rapport indique que l'Union européenne envisagerait d'organiser le partage de données, y compris personnelles, autour du concept d'« altruisme des données », qui permettrait une collecte de données pour des projets qui vont dans le sens de l'intérêt public, pour des entités sans but lucratif. Ce mécanisme suscite l'inquiétude des rapporteurs, car il pourrait laisser des zones grises d'utilisation à but commercial de données sans le consentement des personnes concernées, notamment parce que les entités autorisées à collecter ces données pourraient être redéfinies de façon moins restrictive, et surtout parce que même si l'entité qui traite les données le fait initialement dans un but altruiste comme la découverte d'un nouveau médicament, le produit qui en découle serait breveté ou acheté par une entité commerciale, qui ne le distribuera pas pour le bien commun et l'enlèvera du domaine public.

L'exemple de la recherche aux États-Unis permet de constater que la protection qu'offre le consentement, tel qu'il est actuellement pratiqué, est limitée. Il a lieu au moment de l'inscription dans le service de soins, et mène le patient à donner un accord général à la réutilisation de ses données pour un certain nombre de partenaires spécifiés, dont il est informé à ce moment-là. Dans la pratique, malgré les standards en vigueur, très peu d'accès secondaires aux données sont refusés pour des nouveaux projets utilisant des données qui avaient déjà été collectées, sans nouvelle information donnée au patient. L'OMS soulève aussi le problème de la vente de données de santé par les personnes concernées elles-mêmes, ce qui mènerait à des inégalités inacceptables, car les personnes aux plus faibles revenus auraient moins de capacité à préserver leur vie privée, un tel système porterait donc atteinte aux droits fondamentaux. Ce sont les mêmes problèmes qui sont déjà rencontrés avec le don d'éléments ou de produits du corps humain, qui ne peuvent donner lieu à rémunération en France²⁴, mais le peuvent dans d'autres États.

Dans l'annexe du guide de l'OMS, les recommandations en relation avec le consentement s'adressent aux développeurs d'IA en leur demandant de considérer les règles spécifiques locales des utilisateurs potentiels en matière de consentement, et de prévoir une gestion des données qui respecte la vie privée. Les ministères de la santé sont aussi enjoins à s'assurer que la collecte des données de santé a lieu dans le respect de la vie privée et avec le consentement éclairé des patients, et de faire de ces principes des prérequis à l'utilisation d'IA, en s'assurant de leur respect au moyen de contrôles effectués par des experts.

B. Des données personnelles à partager

Concernant la protection des données, le guide rappelle que les droits des personnes sur leurs données à caractère personnel, bien que liées à la notion de possession, ne sont pas des biens, et sont basées sur des concepts tels que le droit à la vie privée, l'autonomie et la dignité

²³ Les missions du *Health Data Hub* sont définies à l'article L. 1462-1 du Code de la santé publique.

²⁴ L. n°94-653 du 29 juillet 1994, art. 3, *JO*, 30 juillet 1994.

humaine, ce qui est en accord avec les lignes tracées par la loi informatique et liberté en 1978²⁵, puis le Règlement général sur la protection des données (RGPD).

Le RGPD apparaît plébiscité par l'OMS, du fait d'abord de sa portée géographique, qui permet en théorie de protéger la vie privée des habitants de l'Union européenne même lorsque leurs données personnelles font l'objet d'un traitement hors de l'Union, et des personnes extérieures à l'Union dès lors que leurs données sont traitées par un organisme responsable de traitement établi sur le territoire européen. Ensuite la notion de droit à la portabilité des données²⁶, qui est une innovation sur le plan du contrôle des données par la personne concernée, permet de décentraliser et de redistribuer la maîtrise sur les données et l'innovation.

Le guide expose aussi des notions absentes du droit européen : celles de souveraineté d'une communauté sur ses données, et de coopératives de données. Ce sont des États particulièrement concernés par la cohabitation de plusieurs peuples qui ont vu émerger ces particularités (la Nouvelle Zélande avec la population Maori, le Canada avec les Premières Nations). Il s'agit dans les deux cas pour la population de garder un contrôle sur les données la concernant, afin d'en bénéficier, d'éviter de futurs préjudices causés à cette population, ce qui pourrait arriver par méconnaissance de caractéristiques spécifiques, ou encore de décider de façon collective de la réutilisation des données concernées. On peut voir dans cette pratique un intérêt pour la recherche en anthropologie historique plus large.

Bien que la proposition de règlement de la Commission européenne sur l'IA ne fasse pas mention de souveraineté de populations, il est spécifié que les jeux de données d'entraînement, de validation et de test doivent tenir compte des éléments de contexte géographique, comportemental ou fonctionnel spécifiques dans lequel un système d'IA à haut risque est destiné à être utilisé²⁷. Cela s'inscrit dans les différentes mesures destinées à repérer et éviter les biais, présentes dans la proposition de règlement mais détaillées dans les recommandations du rapport, qui demande spécifiquement d'examiner l'impact de certaines caractéristiques sur les IA (ethnie, genre, race, âge entre autres) et de préparer une stratégie de surveillance post-mise sur le marché.

Une autre pratique de plus en plus courante est de fédérer des données entre plusieurs entités qui les collectent dans le but d'augmenter les partages entre entités, qu'elles soient publiques ou privées et entre les pays, en gardant localement un contrôle sur ces données. Il ne s'agit pas de les échanger ou de les envoyer, mais d'autoriser des requêtes, comme une étude statistique ou entraîner un algorithme. Cependant, cette pratique rejoint les réflexions précédentes quant au consentement à une réutilisation ultérieure des données, qui pourrait ne pas avoir été prévue, voire servirait à contourner cette absence de consentement car les données alors partagées ne sont pas à proprement parler en la « possession » du tiers qui en tire bénéfice.

La question du partage des données, que ce soit pour la recherche scientifique ou à des fins commerciales, a été prise au sérieux par plusieurs États, dont les États-Unis qui ont adopté

²⁵ L'article 1^{er} disposait que « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». – L. n°78-17, *JO*, 7 janvier 1978, p. 227.

²⁶ Le droit à la portabilité, qui correspond à l'article 20 du RGPD, est la possibilité pour une personne de récupérer ses données issues d'un service, dans un format ouvert et lisible par une machine, afin de les réutiliser auprès d'un autre fournisseur de service ou à une autre fin.

²⁷ Commission européenne, « Proposition de règlement [...] concernant l'intelligence artificielle [...], *op. cit.*, p. 54 – 55.

dès 2014 une politique de partage des données génomiques, étendue à d'autres données depuis 2016 par le *21st Century Cures Act*. Cette loi promeut l'interopérabilité entre les fournisseurs de technologies de santé pour favoriser le partage des données, et l'accès des patients à leurs propres données. Le modèle des *hubs* de données, comme le *Health Data Hub* français évoqué plus haut, est une solution déployée de différentes manières dans d'autres pays, comme aux États-Unis avec les plateformes spécialisées sur la médecine de précision (*Precision Medicine Initiative* « *All of Us* ») et celle du département des Vétérans, majoritairement financés par le gouvernement fédéral^{28,29}, ainsi qu'au Royaume-Uni, où le *Health Data Research UK* est une initiative de vingt-deux instituts de recherche à but non lucratif, publics et privés. L'Union européenne a conduit des travaux préparatoires pour la création de son Espace européen des données de santé, qui devrait être opérationnel d'ici 2025. L'initiative est en fait plus large que le secteur de la santé, qui n'est qu'un pan de l'espace européen de données, avec pour objectif de partager des données de qualité et interopérables en conformité avec le RGPD, en fusionnant les structures existantes telles qu'en santé le *Genomics project*, les services électroniques de santé transfrontalière, et les réseaux européen de référence³⁰.

Le partage du contenu des entrepôts de données peut être exclusivement à destination de la recherche publique, ou en partenariat avec le secteur privé. Ces collaborations peuvent avoir lieu de manière réciproque : soit en intégrant des données issues d'une entreprise, soit en lui laissant accès aux données, par exemple pour l'entraînement ou la validation d'un algorithme. À nouveau, il faudrait avoir informé les patients d'une réutilisation commerciale de leurs données, ce qui est rarement le cas, et le guide l'illustre avec des exemples saisissants de dérives rendues publiques outre-Atlantique, de cliniques qui ont coopéré avec des entreprises, dans lesquelles elles ont aussi investi, et auxquelles elles ont donné accès aux données générées lors des soins sans en informer les patients ni avoir obtenu leur consentement pour de telles utilisations. Ces cas font écho aux voix qui se sont élevées en France lors de la révélation de suspicion de conflit d'intérêt autour de la création du *Health Data Hub*³¹. La personne principalement en charge du projet, à la tête de la Direction de la recherche, des études, de l'évaluation et des statistiques, ayant été un employé d'IQVIA (une entreprise américaine spécialisée dans l'exploitation des données de santé) avant d'intégrer l'administration, puis de quitter cette dernière pour le poste de Directeur général d'IQVIA France.

Des plateformes de partage de données exclusives à des entreprises existent aussi, parfois mutualisées entre acteurs privés. Si l'intérêt de ces partenariats pour le développement des produits et services utiles à la santé pourrait être réel, il est cependant contrebalancé par les inquiétudes autour de la supervision de ces échanges, de la transparence et du consentement des personnes concernées.

Les recommandations de l'OMS en matière de gouvernance des données sont pour les gouvernements de s'assurer qu'ils ont un cadre légal de protection des données, en particulier de santé, qui protège les droits des personnes et permettent de s'assurer d'un consentement réellement éclairé ; d'en assurer l'application grâce à une autorité indépendante ayant

²⁸ Department of Veterans Affairs, *Fiscal year 2020 Agency financial report*, 24 novembre 2020, p. 23, disponible sur www.va.gov.

²⁹ All of Us Research Program Investigators, "The "All of Us" Research Program", *New England Journal of Medicine* n°381, 15 août 2019, p. 668 et 675, doi:10.1056/NEJMs1809937.

³⁰ Commission européenne, « European Health Data Space » [en ligne], https://ec.europa.eu/health/ehealth/dataspace_en [consulté le 27 octobre 2021].

³¹ « Données de santé : conflit d'intérêt au cœur de la nouvelle plateforme » [en ligne], *Le Monde.fr*, 24 décembre 2019, [consulté le 20 octobre 2021].

suffisamment de pouvoir et de ressources ; d'exiger des organismes qui traitent des données de santé une transparence sur leur utilisation ; d'encourager les mécanismes de supervision par les communautés et la souveraineté des groupes marginalisés sur leurs données ; et enfin d'appliquer les plus hauts standards de consentement et de transparence pour les données qui ont vocation à se trouver sur des plateformes. Relativement à ce dernier point, soulignons qu'en France les entrepôts de données de santé, comme le *Health Data Hub*, les entrepôts créés par des établissements de santé, ou des entreprises, doivent être autorisés par la Commission nationale de l'informatique et des libertés (CNIL) et ont un régime juridique particulier, exigeant des garanties élevées en matière d'information, de consentement, des droits des personnes, de sécurité et de confidentialité³². Les données ne peuvent être utilisées que pour des finalités d'intérêt public et ne peuvent être transférées hors de l'Union européenne afin d'assurer un niveau de protection conforme au RGPD³³. Le Code de la santé publique prévoit aussi que l'hébergement et l'infogérance³⁴ des données de santé ne puissent être effectués qu'auprès de structures certifiées « hébergeur de données de santé »³⁵.

Ces mécanismes de partage des données ne doivent pas occulter les enjeux autour de leur contrôle souvent exclusif, et éloigné du patient.

C. L'accapement et le contrôle des données

Le guide soulève deux derniers points au sujet de la gouvernance des données qui ne sont pas en lien avec les droits fondamentaux, mais relatifs aux droits de propriété et à la protection juridique des bases de données. Les droits de propriété intellectuelle qui peuvent s'appliquer aux données et logiciels sont nombreux et complexes : le secret des affaires, le droit d'auteur, les droits sur les bases de données (qui existent en France, mais cela relève plutôt de l'exception), l'exclusivité réglementaire, et parfois le brevet. L'OMS n'entend pas résoudre la question des mécanismes de protection des algorithmes d'IA ou des bases de données par la propriété intellectuelle, mais souligne que cette dernière (et les intérêts commerciaux) est en conflit avec le partage des données, nécessaire au progrès scientifique – et donc finalement au bien-être général qui fait partie des principes éthiques clés de l'Organisation. Cependant, la protection juridique des données est réputée pour encourager l'innovation et les investissements dans l'IA et la santé, l'équilibre entre les deux objectifs semble être difficile à trouver. En

³² Délibération n° 2021-118 du 7 octobre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé, *JO*, 24 octobre 2021, texte n°44 p. 80-89.

³³ Ce dernier principe a été inscrit pour la première fois dans l'arrêté du 9 octobre 2020 modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé, *JO*, 10 octobre 2020, texte n°28, art. 1. Il porte sur le fonctionnement de l'entrepôt de données de santé du *Health Data Hub* dans le cadre de la crise sanitaire du Covid-19. Suite à l'arrêt « Schrems II » de la CJUE du 16 juillet 2020, l'hébergement du HDH sur le cloud Azure de la multinationale américaine Microsoft a été source de plusieurs recours devant le Conseil d'État afin de stopper cet hébergement. Le 13 octobre 2020, le CE a tout de même considéré que cet hébergement « une atteinte grave et manifestement illégale [...] au droit au respect de la vie privée, comprenant le droit à la protection des données personnelles » - CE, Juge des référés, 13 octobre 2020, n°444937.

³⁴ L'infogérance est le fait de confier à un prestataire un ensemble de services informatiques externalisables, qui effectuera tout ou partie des activités de mise à disposition et de fonctionnement d'un système d'information.

³⁵ Ord. n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JO*, 13 janvier 2017, texte n°17, art. 1.

centrant à nouveau sur l'Union européenne, on peut constater que les principes FAIR Data, de l'*European Open Science Cloud*, prévoient la création de *clouds* « aussi ouverts que possible et aussi fermés que nécessaire », n'excluant pas la protection juridique des données. La proposition de règlement sur l'IA mentionne la propriété intellectuelle à une seule occasion, et précise que les autorités compétentes et organismes en charge du contrôle des systèmes d'IA exécuteront leurs tâches de manière à protéger « les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source »³⁶

Les pays à revenus faibles et intermédiaires pourraient avoir plus de mal à profiter des bénéfices générés par les données qui en sont issues, en n'ayant pas ou peu accès aux technologies, produits ou services. L'OMS recommande que les gouvernements, les instituts de recherche et les universités qui participent au développement des technologies de l'IA conservent un droit de propriété sur les résultats, de sorte que les bénéfices soient partagés, disponibles et accessibles, notamment pour les populations qui ont fourni leurs données pour le développement de l'IA. Elle suggère une forme de droit de garde sur les données plutôt que de modifier les règles de la propriété intellectuelle. Ces principes sont proches de la proposition de la Commission européenne de créer des « bacs à sable réglementaires de l'IA », qui correspondent à « un environnement contrôlé qui facilite le développement, la mise à l'essai et la validation de systèmes d'IA innovants »³⁷, mis à disposition par le Contrôleur européen de la protection des données ou les autorités compétentes des États. Cependant, l'inquiétude de l'OMS concernant les dérogations au consentement se sont pas infondées, car la proposition de règlement prévoit aussi que « des données à caractère personnel collectées légalement à d'autres fins sont traitées aux fins du développement et du test de certains systèmes d'IA innovants dans le bac à sable », ces systèmes innovants devant être développés pour l'intérêt public et incluant la santé publique, y compris la prévention, le contrôle et le traitement des maladies (aux côtés de la sécurité publique, la détection et la prévention d'infractions pénales, et la protection de l'environnement)³⁸.

La seconde question relative à la propriété est celle de l'appartenance de produits, méthodes et services basés sur l'IA. En principe ceux-ci peuvent être brevetés et exploités commercialement, mais cela pourrait être à nuancer lorsque l'appropriation de méthodes freine le développement de technologies médicales ou de médicaments et octroie ainsi un grand pouvoir de contrôle à une entreprise. L'appropriation de ce contrôle interroge d'autant plus lorsqu'une entité publique a participé au financement de la technologie d'IA en question, et qu'elle a profité de données provenant des citoyens. A ce sujet, l'OMS conclut qu'elle devra s'assurer du respect des règles entourant les droits de propriété sur les données, les algorithmes et les technologies d'IA pour la santé, et que la transparence et l'interopérabilité doivent être encouragées.

En conclusion, ce rapport de l'OMS traite de tous les enjeux éthiques autour de l'utilisation de l'IA dans le domaine de la santé, et leur donne une résonance concrète à travers des réflexions juridiques qui examinent le domaine dans sa globalité, de façon plutôt approfondie, bien que chaque sujet nécessiterait un second examen approfondi dans les différents contextes juridiques nationaux. De nombreuses recommandations de gouvernance de

³⁶ Commission européenne, « Proposition de règlement [...] concernant l'intelligence artificielle [...], *op. cit.*, p. 89.

³⁷ *Ibid.*, p. 77.

³⁸ *Ibid.*, p. 78.

l'IA sont présents en sus de ceux évoqués dans le présent article, comme la nécessité d'analyser l'impact d'une technologie d'IA dans la santé avant de la mettre en oeuvre, d'en évaluer le ratio bénéfice-risque, l'instauration d'autorités compétentes et d'organismes de contrôles, ou encore un accès au marché facilité aux systèmes à faible risque. Ce sont des éléments que l'on retrouve dans la proposition de règlement sur l'IA de la Commission européenne, avec le marquage CE pour les systèmes à haut risque, la création d'organismes notifiés, l'évaluation avant et après la mise sur le marché, etc. Ces recommandations semblent globalement compatibles avec le cadre juridique européen en cours de construction, toutefois certains éléments, notamment en matière de consentement, de transparence ou de partage des bénéfices des données sont en conflit.

Le 15 septembre dernier, le Haut-Commissariat de l'ONU aux droits de l'homme a demandé un moratoire sur l'utilisation de certains systèmes d'IA présentant des risques forts d'atteinte à la vie privée, en attendant d'avoir un dispositif pour protéger les droits fondamentaux³⁹. Les principes éthiques ont plus que jamais besoin d'être rendus concrets par des dispositions juridiques, en santé comme dans les autres domaines d'application de l'IA.

³⁹ ONU, « Intelligence artificielle : face aux risques d'atteinte à la vie privée, l'ONU demande un moratoire sur certains systèmes » [en ligne], <https://news.un.org/fr/story/2021/09/1103762> [consulté le 25 octobre 2021].