مجلة شهرية، محكمة متعددة التخصصات
تعنى بنشر الدراسات والأبحاث في مجالات العلوم
القانونية، الإنسانية، الاجتماعية، والاقتصادية

المدير المسؤول ورئيس التحرير: انس المستقل

مجلة المقالات الدولية

INTERNATIONAL ARTICLES JOURNAL

العدد العاشر Eighth Issue

مارس March 2026

الرقم المعياري الدولي : e-ISSN : 3085 - 5039

رقم الصحافة : Press number : 1/2025

10

مجلة المقالات الدولية

العدد العاشر، مارس 2026

e-ISSN : 3085 - 5039

مجلة المقالات الدولية
INTERNATIONAL ARTICLES JOURNAL

كلمة العدد

بسم الله الرحمن الرحيم

يسر مجلة المقالات الدولية أن تضع بين أيدي القراء والباحثين العدد العاشر، في سياق رسالتها العلمية الرامية إلى دعم البحث الأكاديمي الرصين، وترسيخ ثقافة النشر العلمي الموثوق. ونغتنم هذه المناسبة للتذكير بفهرسة المجلة ضمن معامل التأثير العربي (AIF)، بما يمثله ذلك من اعتراف علمي رسمي، وكونه أحد المعايير المعتمدة في تصنيف الجامعات العربية ضمن أول تصنيف عربي للجامعات. كما نعتز باستمرار إدراج المجلة ضمن International Scientific Indexing (ISI)، في خطوة نوعية تجسد ثقة الأوساط العلمية في جودة ما تنشره المجلة، وتسهم في توسيع دائرة انتشار البحوث المنشورة بها وتعزيز أثرها العلمي.وإذ نقدم هذا العدد بما يضمّه من بحوث ودراسات متنوعة، فإننا نؤكد التزامنا الثابت بالتحكيم العلمي الدقيق، والأخلاقيات البحثية الراسخة، ومعايير الجودة والشفافية، بما يخدم قيم التميز والمعرفة، ويدعم الباحثين في إنتاج علمي رفيع يسهم في تطوير الفكر ومواكبة قضايا الواقع.

والله ولي التوفيق

رئيس التحرير

Arab Impact Factor

INTERNATIONAL Scientific Indexing

ISSN INTERNATIONAL STANDARD SERIAL NUMBER

OPEN ACCESS

ORCID

مجلة المقالات الدولية

INTERNATIONAL ARTICLES JOURNAL

IAJ

مجلة علمية، شهرية، محكمة متعددة التخصصات، تعنى بنشر الدراسات والأبحاث في مجالات العلوم الإنسانية، الاجتماعية، والاقتصادية.

الرقم المعياري الدولي: ISSN : 3085 - 5039 رقم الصحافة : Press number: 2025 / 1 العدد 10، مارس 2026

اللجان العلمية

محتويات العدد

International Articles Journal
مجلة المقالات الدولية
A peer-reviewed, multidisciplinary journal
مجلة محكمة، متعددة التخصصات
Issue 10, March 2026
العدد 10، مارس 2026

La transformation digitale dans le domaine de la santé : entre prouesse technologique et défis juridiques et éthiques

Digital transformation in healthcare: between technological prowess and legal and ethical challenges

Nadia AZDDOU
Pr, Faculté des Sciences Juridiques, Économiques et Sociales Université Hassan II de Casablanca

Oussama LOUKILI
Dr Faculté des Sciences Juridiques, Économiques et Sociales Université Hassan II de Casablanca

Abstract:

The digital transformation of healthcare systems represents one of the most structural and far-reaching shifts in contemporary medicine.
The integration of digital technologies (artificial intelligence, Big Data, telemedicine, connected devices, and blockchain) is redefining the modalities of healthcare production, management, and governance.
While these innovations reflect major technological breakthroughs, they simultaneously raise complex legal and ethical challenges, particularly concerning the protection of health data, the preservation of medical confidentiality, the liability of stakeholders, and the regulation of algorithmic uses.
Through an analytical and comparative approach, this article examines the transformations induced by health digitalization in light of different regulatory frameworks
The study highlights regulatory convergences in terms of data security, while also identifying divergences relating to liability mechanisms, consent standards, and digital governance models.
The analysis reveals a persistent gap between the acceleration of technological innovation and the adaptation of legal instruments, generating areas of ethical and normative uncertainty.
The article concludes on the need to develop a global governance framework for health data capable of reconciling innovation, cybersecurity, and the protection of patients' fundamental rights.

Keywords :

Medical Artificial Intelligence, Big Data, Telemedicine, Blockchain, Algorithm, RGPD, HIPA, Ethics, Governance.

Résumé:

La transformation digitale des systèmes de santé constitue l'une des mutations les plus structurantes de la médecine contemporaine.
L'intégration des technologies numériques (intelligence artificielle, Big Data, télémédecine, objets connectés et blockchain) redéfinit les modalités de production, de gestion et de gouvernance des soins.
Si ces innovations traduisent une prouesse technologique majeure, elles soulèvent simultanément des défis juridiques et éthiques complexes, liés notamment à la protection des données de santé, au respect du secret médical, à la responsabilité des acteurs et à la régulation des usages algorithmiques.
À travers une approche analytique et comparative, cet article examine les transformations induites par la digitalisation sanitaire à la lumière de cadres normatifs différents
L'étude met en évidence les convergences réglementaires en matière de sécurisation des données, mais également les divergences relatives aux mécanismes de responsabilité, aux standards de consentement et aux modèles de gouvernance numérique.
L'analyse révèle l'existence d'un décalage persistant entre l'accélération des innovations technologiques et l'adaptation des instruments juridiques, générant des zones d'incertitude éthique et normative.
L'article conclut sur la nécessité d'élaborer une gouvernance globale des données de santé conciliant innovation, sécurité numérique et protection des droits fondamentaux des patients.

Mots clés :

Intelligence artificielle médicale, Big Data, Télémédecine, Blockchain, algorithme, RGPD, HIPA, éthique, gouvernance .

Introduction

De nos jours la digitalisation représente l'un des vecteurs les plus puissants de transformation des systèmes de santé à l'échelle planétaire.

Sous l'effet conjugué de l'essor des technologies de l'information, de la massification des données médicales et du développement de l'intelligence artificielle, la médecine connaît une mutation structurelle qui touche aussi bien les pratiques cliniques que les modes d'organisation des soins.

L'émergence de l'hôpital numérique, la généralisation du dossier médical informatisé, le déploiement de la télémédecine ou encore l'intégration d'algorithmes d'aide à la décision illustrent parfaitement le virement de la santé vers l'ère de la donnée.

Cette transformation s'inscrit dans une dynamique plus large de « datafication » des activités humaines, ou la donnée devient de manière simultanée une ressource stratégique, un outil de pilotage et un levier d'innovation.

Dans le domaine de la santé, l'exploitation massive de données de santé ouvre de nouvelles perspectives tant en matière de médecine prédictive, que de détection précoce des pathologies, et d'optimisation des parcours de soins et de recherche biomédicale.

Toutefois, la spécificité de la donnée médicale à travers son caractère intime et sensible, confère à cette révolution numérique une dimension éthique et juridique singulière.

La dématérialisation des données de santé, leur circulation au sein d'écosystèmes interconnectés, leur hébergement et stockage numérique exposent à des risques accrus de violation de la vie privée, de cyberattaques et de l'usage abusive.

Le secret médical, historiquement ancré dans la relation interpersonnelle entre le patient et le médecin, se trouve profondément reconfiguré.

En effet, nous sommes en face d'une pluralité d'intervenants (hébergeurs de données, éditeurs de logiciels, assureurs, plateformes technologiques) qui accède, traite ou stocke des informations médicales, ce qui brouille les frontières traditionnelles de la confidentialité rattachée au secret médical.

Par ailleurs, le recours croissant à des algorithmes décisionnels dans le domaine médical engendre des interrogations fondamentales quant à la responsabilité médicale, à la transparence des décisions automatisées et au risque de biais discriminatoires.

La question phare n'est plus seulement celle de la protection des données, mais plutôt celle qui se rapporte à la gouvernance globale de l'écosystème numérique de santé.

Dans ce contexte, l'analyse de cette transformation digitale de la santé impose une approche de droit comparé.

Les systèmes juridiques ont développé des cadres de régulation distincts pour encadrer la donnée de santé : dans le cadre Marocain à travers la loi 09-08 et les textes relatifs à la cybersécurité ; la Tunisie a adopté la Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, le Bahreïn, l'Algérie et le Liban ont promulgué leur loi nationale sur la protection des données en 2018 et l'Égypte en 2020 , les Émirats arabes unis pour leur part ont adopté une loi fédérale sur la protection des données personnelles en novembre 2021, et l'Arabie saoudite en octobre 2021.

Pour l'Union européenne la protection des données est assurée par le biais du Règlement général sur la protection des données (RGPD) ; alors que pour les États-Unis c'est via le Health Insurance Portability and Accountability Act (HIPAA).

L'ensemble de ces dispositifs traduisent des philosophies juridiques différentes, entre une protection des libertés fondamentales en Europe, une approche sectorielle aux États-Unis et une régulation hybride dans les pays émergents.

Leur confrontation permet de mieux appréhender les forces, limites et perspectives de la gouvernance numérique de la santé.

Dès lors, la transformation digitale apparaît comme une réalité ambivalente : prouesse technologique porteuse de progrès médicaux majeurs, mais également source de vulnérabilités juridiques et éthiques inédites.

L'objet du présent article est d'analyser cette dialectique à travers une lecture croisée technologique, normative et comparative.

Plan

I Les prouesses technologiques de la transformation digitale en santé

1. Intelligence artificielle médicale
2. Big Data et médecine prédictive
3. Télémédecine et santé connectée
4. Blockchain et traçabilité sanitaire

II — La donnée de santé : une catégorie juridique spécifique (droit comparé)

1. Qualification juridique des données de santé
2. Droit marocain (loi 09-08, 05-20…)
3. RGPD européen
4. HIPAA américain
5. Le cadre juridique régional et arabe

III — Les défis juridiques de la digitalisation sanitaire

1. Protection de la vie privée
2. Secret médical numérique
3. Hébergement et souveraineté des données
4. Responsabilité médicale algorithmique

IV — Les enjeux éthiques

1. Consentement éclairé numérique
2. Transparence algorithmique
3. Biais et discrimination IA
4. Déshumanisation du soin

V — Vers une gouvernance numérique globale de la santé

1. Compliance et cybersécurité
2. Autorités de régulation
3. Standards internationaux
4. Modèles de gouvernance futurs

I

Les prouesses technologiques de la transformation digitale en santé

La transformation digitale représente de nos jours l'un des vecteurs majeurs de mutation des systèmes de santé contemporains.

Elle se caractérise par l'intégration de technologies avancées dans l'ensemble du parcours de soins, tant sur le plan de prévention, de diagnostic, du volet thérapeutique, que du suivi et de la gouvernance sanitaire.

Loin de se limiter à une simple modernisation des outils, elle opère une reconfiguration profonde des rapports entre soignants, patients, institutions et données médicales.

Cette mutation repose sur plusieurs piliers technologiques majeurs, au premier rang desquels figurent l'intelligence artificielle médicale, l'exploitation du Big Data, la télémédecine et la blockchain appliquée à la santé.

Chacun de ces outils ouvre de nouvelles perspectives en matière d'efficience clinique, de personnalisation de soins et de gouvernance sanitaire, tout en engendrant des enjeux juridiques et éthiques renouvelés, notamment en matière de secret médical et de protection des données de santé

1. Intelligence artificielle médicale

L'intelligence artificielle (IA) médicale représente sans doute l'innovation la plus marquante de la transformation numérique en santé.

Elle renvoie à l'ensemble des systèmes algorithmiques capables de simuler ou d'augmenter certaines fonctions cognitives humaines, telles que l'apprentissage, le raisonnement, la détection de corrélations ou la prise de décision.

Dans le champ médical, l'IA repose essentiellement sur des techniques d'apprentissage automatique (machine learning) et d'apprentissage profond (deep learning), qui permet l'analyse automatisée de volumes massifs de données cliniques, biologiques ou radiologiques.

a) Applications diagnostiques

L'IA a démontré des performances particulièrement élevées en imagerie médicale.

En effet les algorithmes de reconnaissance visuelle de l'IA peuvent détecter des lésions tumorales, anomalies pulmonaires ou pathologies rétiniennes avec une précision équivalente voire supérieur à celle de praticiens expérimentés.

Elle permet entre autres :

- La détection précoce des cancers.
- L'identification automatisée des fractures.

- Le dépistage des maladies cardiovasculaires.
- L'analyse histopathologique assistée.

b) Aide à la décision clinique

Au-delà du diagnostic, l'IA intervient dans l'aide à la décision thérapeutique.

Des systèmes experts analysent les dossiers médicaux, antécédents, profils génétiques et recommandations scientifiques afin de proposer des protocoles de traitement personnalisés.

Cette nouvelle forme de médecine vise, à la fois la réduction des erreurs médicales, l'optimisation des prescriptions et l'adaptation des traitements aux profils individuels.

c) Robotique médicale et chirurgie assistée

En matière de robotique l'IA alimente les robots chirurgicaux de nouvelle génération, en améliorant la précision gestuelle, réduisant la dangerosité des actes invasifs tout en optimisant les suites opératoires des patients pris en charge par ces nouveaux procédés.

d) Enjeux éthiques et juridiques

Cependant, l'IA médicale soulève des interrogations majeures :

- La problématique de la responsabilité en cas d'erreur algorithmique.
- L'éventualité de Biais discriminatoires dans les bases de données.
- Le cas d'Opacité décisionnelle dite « boîte noire ».
- Les risques pour la confidentialité des données.

2. Big Data et médecine prédictive

Le Big Data médical désigne l'exploitation massive de données de santé issues de sources à la fois multiples et différentes, on parle entre autres des dossiers médicaux électroniques, des objets connectés, des essais cliniques, et des bases génomiques ou applications mobiles.

Ces données se caractérisent par le principe des « 5 V » attribué à la Big Data, à savoir : Volume, Vélocité, Variété, Véracité, Valeur

L'analyse algorithmique de ces données permet d'anticiper l'apparition de pathologies avant même les premiers symptômes.

Il s'agit d'une révolution dans la prise en charge des patients avec le passage d'une médecine curative à une médecine prédictive et préventive.

Les applications majeures sont :

- La prédiction des risques cardiovasculaires.
- L'anticipation des épidémies.
- La détection précoce du diabète.

- L’identification des prédispositions génétiques.

Le Big Data permet également le développement de la médecine personnalisée, cette personnalisation des soins serait fondée sur le profil biologique, génétique et comportemental du patient.

À l’échelle macro-sanitaire, l’exploitation des mégadonnées facilite :

- La planification hospitalière.
- L’allocation des ressources.
- La surveillance épidémiologique.
- La gestion des crises sanitaires.

Toutefois, l’agrégation de données sensibles amplifie les risques de réidentification des patients, de fuites massives de données, de détournement de ces données pour des fins d’exploitation commerciale et surtout la violation du secret médical par recoupement algorithmique.

3. Télémédecine et santé connectée

La télémédecine désigne l’ensemble des pratiques médicales réalisées à distance grâce aux technologies de l’information et de la communication.

Le Maroc a mis à jour son cadre juridique afin de réglementer cette nouvelle forme de pratique médicale, notamment à travers la loi 131.13 qui régit l’exercice de la profession médicale, et selon ladite loi la télémédecine engloberait plusieurs actes à savoir la Téléconsultation, la Téléexpertise, la Télésurveillance, la Téléassistance médicale et la Régulation médicale à distance.

Les avantages de la télémédecine sont multiples, toutefois cette pratique médicale ne serait pas anodine mais bien au contraire entachée de risques et de dangers

La télémédecine constitue un levier majeur de réduction des inégalités territoriales, particulièrement dans les zones rurales ou sous-médicalisées, le ministère de santé marocain a multiplié les démarches pour équiper les zones enclavées par des moyens adéquats de télémédecine et assurer la formation du personnel soignant pour le maniement de ces nouveaux outils

Dans le cadre du suivi des maladies chroniques dite de longues durées, les dispositifs connectés permettraient de suivre les différents types de diabète, d’assurer la surveillance cardiaque, de contrôler de la tension artérielle et de gérer les cas d’insuffisance respiratoire.

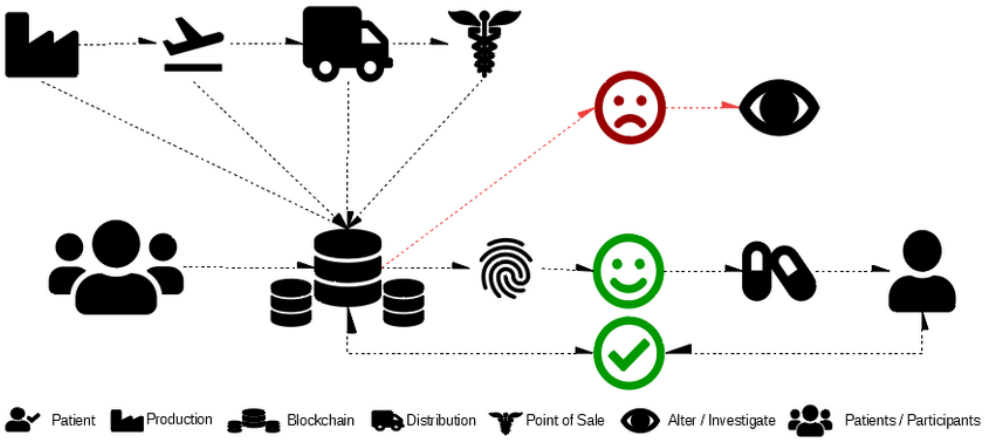
La crise sanitaire du COVID-19 qui a bousculé les systèmes de santé à travers la planète a contribué à l’accélération de l’adoption de ces pratiques, garantissant la continuité des soins malgré les contraintes de mobilité mettant fin aux résistances qui empêchaient la promotion de la télémédecine

Le recours aux nouvelles technologies dans le cadre de la télémédecine est entaché de risques de piratages et de détournement des données de santé recueillies d’où l’intérêt de la sécurisation

des plateformes numériques, de la Confidentialité des échanges, de Fiabilité des données transmises.

4. Blockchain et traçabilité sanitaire

La blockchain constitue une technologie de stockage et de transmission d'informations reposant sur un registre distribué, sécurisé, transparent et infalsifiable.



Shema retraçant les avantages et les risques de la blockchain

La blockchain permet la création de dossiers médicaux électroniques hautement sécurisés, accessibles uniquement aux acteurs autorisés, avec traçabilité complète des accès.

Elle offre des solutions efficaces contre :

- La contrefaçon de médicaments.
- Les ruptures de chaîne d'approvisionnement.
- Les fraudes logistiques.

La blockchain garantit l'intégrité des données d'essais cliniques, renforçant la confiance scientifique.

Plusieurs avantages juridiques et éthiques sont associés à la blockchain grâce à la protection des données contre la falsification, la transparence des accès et la traçabilité du Consentement des patients.

La multiplicité des avantages de la blockchain ne peut pas cacher les limites structurelles de cette dernière, à cause de son coût énergétique, de sa complexité technique, de l'interopérabilité avec les systèmes existants et de son cadre juridique encore lacunaire.

L'ensemble de ces technologies illustre l'ampleur de la révolution numérique en santé. L'intelligence artificielle améliore la précision diagnostique, le Big Data permet l'anticipation des risques sanitaires, la télémédecine abolit les distances géographiques, tandis que la blockchain renforce la sécurité et la traçabilité des données médicales.

Toutefois, ces prouesses technologiques s'accompagnent de vulnérabilités nouvelles. L'extension des flux de données de santé, leur interconnexion et leur exploitation algorithmique redessinent les contours du secret médical, appelant à une adaptation continue des cadres juridiques, éthiques et déontologiques.

II

La donnée de santé : une catégorie juridique spécifique en droit comparé

La reconnaissance juridique de la donnée de santé comme catégorie spécifique constitue aujourd'hui un point de convergence majeur des systèmes normatifs contemporains.

En raison de son caractère intime, sensible et potentiellement discriminant, l'information médicale fait l'objet d'un encadrement renforcé, tant en matière de collecte que de traitement, de conservation et de circulation.

Toutefois, si les finalités de protection apparaissent partagées, les mécanismes juridiques mobilisés diffèrent sensiblement selon les traditions légales et les philosophies de régulation. L'analyse comparée du droit marocain, du droit de l'Union européenne et du droit américain permet d'en mesurer les convergences et les singularités.

1. Le cadre juridique marocain : une régulation en construction

Au Maroc, la protection des données de santé s'inscrit dans un dispositif normatif composite, articulant droit pénal, droit médical et droit des données personnelles.

La loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue le socle principal.

Elle qualifie expressément les données de santé comme étant des données sensibles, et dont le traitement est soumis à des conditions rigoureuses, notamment l'obtention du consentement explicite de la personne concernée et l'autorisation préalable de la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP).

Ce cadre légal est complété par d'autres instruments :

- La loi n° 131-13 relative à l'exercice de la médecine.
- Le Code de déontologie médicale.
- La loi n° 05-20 relative à la cybersécurité.

Ces textes consacrent la confidentialité des informations médicales en imposant des obligations de sécurisation des systèmes d'information sanitaires et d'encadrement de l'hébergement des données de santé.

Toutefois, la digitalisation accélérée du système de santé marocain (dossiers médicaux informatiques, télémédecine, plateformes numériques) met en évidence certaines lacunes : l'absence d'un statut juridique détaillé de l'IA médicale, la limitation de l'encadrement de la responsabilité algorithmique et la dépendance technologique à des hébergeurs internationaux.

2. Le modèle européen : le RGPD comme standard international

Le droit de l'Union européenne offre aujourd'hui le cadre le plus structuré en matière de protection des données de santé, à travers le Règlement général sur la protection des données (RGPD).

Le RGPD classe les données relatives à la santé parmi les catégories particulières de données, dont le traitement est en principe interdit, sauf exceptions strictement encadrées : un consentement explicite de la personne concernée, l'usage pour des finalités médicales des données collectées dans le cadre de la santé publique ou de la recherche scientifique.

Plusieurs principes structurent ce régime :

- La minimisation des données.
- La limitation des finalités.
- L'Obligation de sécurité renforcée.

Le règlement consacre également des droits étendus au profit des patients, avec notamment le droit d'accès, de rectification, d'effacement, de limitation du traitement et de portabilité des données.

En matière de santé digitale, le RGPD impose :

- L'analyse d'impact (DPIA) pour les traitements à risque.
- La notification des violations de données.
- L'encadrement des transferts hors UE.

Ce modèle attribue à l'Europe une position normative dominante, influençant de nombreuses législations étrangères dont celles du continent africain

3. Le modèle américain : la HIPAA

Contrairement au modèle européen global, les États-Unis ont adopté pour leur part une approche sectorielle de la protection des données de santé à travers le Health Insurance Portability and Accountability Act (HIPAA).

Ce dispositif encadre spécifiquement les informations de santé protégées (Protected Health Information : PHI) détenues par les acteurs de santé, à savoir les hôpitaux, les assureurs, les professionnels médicaux et leurs partenaires.

La HIPAA repose sur plusieurs piliers :

- Privacy Rule : confidentialité des données médicales.
- Security Rule : sécurisation des données électroniques.
- Breach Notification Rule : notification des violations.

Elle impose des obligations techniques strictes :

- Le Chiffrement.
- Le Contrôle d'accès.
- La Traçabilité des consultations.

Toutefois, le modèle américain se distingue du modèle européen par :

- Une protection variable selon les États.
- Une place importante accordée aux acteurs privés.
- Une moindre reconnaissance de droits subjectifs comparativement au RGPD.

Par ailleurs, certaines plateformes technologiques manipulant des données de santé échappent partiellement au champ d'application de la HIPAA, créant des zones grises juridiques à l'ère des applications mobiles et des objets connectés.

4. Lecture comparative des trois modèles

L'analyse croisée met en évidence trois philosophies de régulation :

- Le Maroc adopte un modèle hybride, inspiré du droit européen mais encore en consolidation institutionnelle.
- L'Union européenne développe une approche fondée sur la protection des libertés fondamentales et la responsabilisation des acteurs.
- Les États-Unis privilégient une logique pragmatique sectorielle centrée sur la sécurité des flux d'information.

Ces divergences influencent directement la gouvernance de la santé digitale, notamment en matière de transferts internationaux de données, de responsabilité des opérateurs technologiques et de protection du secret médical à l'ère algorithmique.

5 Les cadres juridiques émergents de protection des données de santé en Égypte, en Tunisie et au Moyen-Orient

Les pays de l'Afrique du Nord et du Moyen-Orient connaissent une accélération notable de la digitalisation du domaine médical, portée à la fois par des impératifs d'efficacité des systèmes de soins, des stratégies de modernisation étatique et des investissements technologiques massifs.

Cette dynamique s'accompagne de la mise en place progressive de cadres normatifs destinés à encadrer la collecte, le traitement et la circulation des données de santé, lesquelles sont unanimement qualifiées de données sensibles en raison de leur nature intime et des risques de discrimination ou de stigmatisation qu'elles comportent.

L'Égypte s'est dotée tardivement d'un dispositif global de protection des données personnelles avec l'adoption de la loi n° 151 de 2020 relative à la protection des données à caractère personnel.

Ce texte marque une étape structurante dans la régulation de l'écosystème numérique égyptien, en consacrant expressément la catégorie des données sensibles, au sein de laquelle figurent les données de santé.

Le traitement de ces informations est subordonné à l'obtention d'un consentement explicite de la personne concernée, ainsi qu'à des garanties renforcées en matière de sécurité, de confidentialité et de limitation des finalités.

La loi encadre également les transferts internationaux de données, soumis à autorisation préalable de l'autorité compétente, traduisant une volonté de préserver une forme de souveraineté informationnelle.

Toutefois, malgré cette avancée normative, plusieurs limites subsistent, avec l'entrée en vigueur différée de certains décrets d'application, la structuration progressive de l'autorité nationale de protection des données et l'insuffisance de jurisprudence relative aux violations de données de santé traduisant un cadre encore en phase de maturation.

Sans oublier la question spécifique de la responsabilité en cas de défaillance algorithmique ou de cyberattaque affectant des infrastructures médicales qui demeure largement non traitée.

La Tunisie pour sa part fait figure de pionnière régionale avec l'adoption, dès 2004, d'une loi organique relative à la protection des données personnelles.

Ce texte institue une autorité de contrôle indépendante et consacre les données de santé comme données sensibles nécessitant un régime de protection renforcé.

Le traitement de ces données suppose un consentement préalable, éclairé et écrit, ainsi qu'une autorisation de l'autorité nationale dans certains cas, notamment pour les transferts transfrontaliers.

Ce dispositif confère une base juridique relativement solide à la digitalisation du système de santé tunisien, qui a engagé plusieurs programmes de dématérialisation des dossiers médicaux et de développement de la télémédecine.

Néanmoins, ce cadre demeure confronté à des défis contemporains, avec notamment l'externalisation de l'hébergement des données vers des prestataires technologiques internationaux, l'usage croissant du cloud computing et l'émergence d'applications de santé connectée mettent à l'épreuve un dispositif juridique conçu dans un contexte technologique antérieur à l'ère du Big Data.

Des réformes seraient actuellement envisageables afin d'aligner davantage le droit tunisien aux standards européens issus du RGPD.

Quant aux États du Golfe, elle se caractérisent par une digitalisation extrêmement rapide de leurs systèmes de santé, inscrite dans des stratégies nationales de transformation économique et d'innovation technologique.

Les programmes de smart health, d'hôpitaux numériques et d'intégration de l'intelligence artificielle y sont particulièrement développés.

Cette modernisation s'accompagne de l'adoption de lois récentes sur la protection des données personnelles, lesquelles reconnaissent systématiquement la sensibilité des données de santé.

Plusieurs États ont instauré des exigences strictes en matière de localisation des données, imposant leur stockage sur le territoire national.

Cette approche traduit une préoccupation centrale de souveraineté numérique et de contrôle étatique des infrastructures informationnelles sanitaires.

Parallèlement, des réglementations sectorielles spécifiques encadrent l'usage des dossiers médicaux électroniques, la télémédecine et l'échange interinstitutionnel de données. Toutefois, malgré ce volontarisme réglementaire, la question de la responsabilité médicale liée à l'usage de l'intelligence artificielle, ainsi que celle de la transparence algorithmique, demeure embryonnaire.

L'analyse comparée de ces systèmes juridiques met en évidence une convergence autour de la reconnaissance de la donnée de santé comme catégorie juridiquement sensible nécessitant une protection renforcée.

Elle révèle également une influence notable des standards internationaux, en particulier européens, dans la structuration des législations nationales.

Cependant, des disparités importantes subsistent quant au degré de maturité institutionnelle, à l'effectivité des mécanismes de contrôle et à l'encadrement des technologies émergentes. Alors que certains États privilégient une approche souverainiste centrée sur la localisation des données, d'autres adoptent des modèles plus ouverts mais juridiquement moins consolidés.

Cette diversité normative illustre la complexité croissante de la gouvernance juridique des données de santé à l'ère digitale.

Elle met en lumière la nécessité d'une harmonisation internationale des standards de protection, condition essentielle à la sécurisation des flux transfrontaliers de données médicales et au développement d'une coopération sanitaire numérique globale.

III

Les défis juridiques de la digitalisation sanitaire

Si on considère que la transformation digitale du secteur de la santé constitue un levier majeur d'amélioration de la qualité et de l'efficience des soins, elle engendre parallèlement des vulnérabilités juridiques inédites.

La dématérialisation des données médicales, l'interconnexion des systèmes d'information et l'intégration d'outils algorithmiques décisionnels déplacent les frontières traditionnelles de la responsabilité, de la confidentialité et de la sécurité sanitaire.

Ces mutations imposent une relecture des cadres normatifs existants à l'aune des nouveaux risques numériques.

1. La responsabilité médicale à l'ère de la santé numérique

Traditionnellement, la responsabilité médicale repose sur une relation bilatérale entre le praticien et le patient, fondée sur l'obligation de moyens, l'appréciation clinique et la faute professionnelle.

La santé numérique introduit un tiers technologique dans cette relation, complexifiant la chaîne de décision.

Plusieurs formes de responsabilité émergent en matière d'algorithme à titre d'exemple :

- **Responsabilité du médecin utilisateur** : lorsqu'il suit ou ignore la recommandation algorithmique.
- **Responsabilité du concepteur du logiciel** : en cas de défaut de conception ou de biais algorithmique.
- **Responsabilité de l'établissement de santé** : pour défaut de choix, de paramétrage ou de supervision du dispositif.
- **Responsabilité du fournisseur de données** : si l'algorithme est biaisé par une base d'apprentissage défaillante.

Cette dilution de la responsabilité pose le risque d'une « irresponsabilité systémique », où chaque acteur invoque l'autonomie de l'outil numérique.

Les systèmes juridiques comparés n'offrent, à ce stade, que des réponses partielles.

Le droit européen mobilise les régimes de responsabilité du fait des produits défectueux et les projets de régulation de l'IA.

Le droit américain recourt aux mécanismes de malpractice et de product liability.

Au Maroc, l'encadrement demeure embryonnaire, reposant sur les règles générales de responsabilité civile et pénale.

2. Le secret médical à l'épreuve de la dématérialisation

Historiquement, le secret médical s'inscrivait dans une relation interpersonnelle protégée par des règles déontologiques et pénales strictes.

La digitalisation transforme profondément cette configuration.

Les données médicales circulent désormais au sein d'écosystèmes numériques impliquant des acteurs différents :

- Hébergeurs de données.
- Éditeurs de logiciels.
- Plateformes cloud.
- Assureurs.
- Opérateurs de télémédecine.

La multiplication de ces intervenants élargit le cercle des dépositaires du secret médical, rendant sa maîtrise plus complexe.

Deux mutations majeures apparaissent :

- Le Passage d'un secret individuel à un secret systémique et ou La confidentialité ne dépend plus uniquement du médecin, mais de l'ensemble de la chaîne technologique.
- La traçabilité et confidentialité des données de santé, dans la mesure que les systèmes numériques permettent de tracer chaque accès au dossier médical, renforçant la sécurité, mais multipliant les points de vulnérabilité et les cyberattaques contre les hôpitaux illustrent cette fragilisation : rançongiciels, vols de données patients, paralysie des systèmes hospitaliers.

3. L'hébergement des données de santé entre souveraineté et extraterritorialité

La question de l'hébergement constitue l'un des enjeux juridiques les plus sensibles de la santé digitale.

Le constat est que les données de santé sont souvent stockées sur des serveurs cloud internationaux, chez des prestataires technologiques privés et le plus souvent en dehors du territoire national.

Cette situation soulève plusieurs problématiques :

En premier lieu la souveraineté numérique, du fait que le stockage à l'étranger expose les données aux législations extraterritoriales.

En deuxième lieu quel droit est-il applicable en cas de violation du secret médical ?

Certains systèmes juridiques imposent l'hébergement local ou certifié (modèles européens ou du Golfe) de leurs données de santé, alors que pour le contexte Marocain on assiste à un développent progressive des régimes d'agrément des hébergeurs de données de santé.

4. Cybersécurité et vulnérabilité des infrastructures sanitaires

La digitalisation accroît l'exposition du secteur de la santé aux risques cybernétiques.

Les établissements hospitaliers constituent des cibles privilégiées pour plusieurs raisons : la valeur marchande des données médicales, la criticité des systèmes et la nécessité de continuité des soins.

Les attaques peuvent entraîner une interruption des services, une altération des données et des risques pouvant engager les pronostics vitaux des patients.

Pour toutes ces raisons les législations imposent désormais des Protocoles de sécurité renforcés, des Audits réguliers, des notifications en cas de violations et des plans de continuité informatique.

Au Maroc, la loi relative à la cybersécurité et les directives des autorités nationales encadrent progressivement ces obligations, en convergence avec les standards internationaux.

5. Vers une redéfinition de la gouvernance juridique de la santé digitale

L'ensemble de ces défis révèle l'insuffisance des cadres juridiques classiques fondés sur :

- La responsabilité individuelle.
- Le secret interpersonnel.
- La territorialité des données.

La santé digitale impose une approche systémique qui intègre à la fois :

- La Gouvernance des données.
- La Régulation algorithmique.
- La Certification des technologies médicales.
- La Coopération internationale.

Au-delà des enjeux strictement juridiques, la transformation digitale de la santé soulève des interrogations éthiques fondamentales relatives au consentement, à l'autonomie du patient, à la transparence des décisions automatisées et au risque de déshumanisation du soin.

L'ensemble de ces dimensions appellent une analyse spécifique.

IV
Les enjeux éthiques

La transformation digitale des systèmes de santé ne se limite pas à une mutation technologique ; elle constitue une rupture anthropologique et éthique majeure dans la relation classique de soin.

L'intégration de l'intelligence artificielle, de la big Data et des dispositifs connectés modifie profondément les modalités de décision médicale, de recueil du consentement, d'accès à l'information et d'interaction entre patient et professionnel de santé.

Dans ce contexte, les principes classiques de la bioéthique que sont l'autonomie, la bienfaisance, la non-malfaisance et la justice se trouvent réinterprétés à la lumière des logiques algorithmiques.

Les enjeux éthiques se cristallisent particulièrement autour du consentement éclairé numérique, de la transparence des systèmes d'IA, des risques de biais discriminatoires et de la crainte d'une déshumanisation du soin.

1. Consentement éclairé numérique

Le consentement éclairé constitue l'un des piliers fondamentaux de l'éthique médicale contemporaine.

Il repose sur le respect du droit du patient à recevoir une information loyale, claire et appropriée afin de prendre une décision libre concernant sa prise en charge.

La digitalisation de la santé perturbe de manière indéniable le processus informationnel.

Le patient n'est plus seulement informé d'un acte médical, mais également tout ce qui se rapporte avec le stockage de ses données, leur partage éventuel, leur réutilisation à des fins scientifique et leur traitement algorithmique.

De ce fait le consentement devient ainsi multicouche : médical, technologique, informationnel et parfois commercial.

On parle de l'illusion du consentement

Plusieurs limites surgissent par le recours à la digitalisation, notamment la complexité des interfaces numériques, la longueur excessive des Conditions d'utilisation et leur technicité, sans oublier l'Opacité des traitements algorithmiques et un consentement considéré comme étant « cliqué » et non pas compris.

Le risque réel est celui d'un consentement formel, vidé de sa substance éthique.

Pour surpasser ces limites et obstacles plusieurs solutions sont envisageable :

- Le Consentement granulaire.
- Le Consentement révocable.

- La Blockchain pour la traçabilité.
- Des Tableaux de bord patient pour la gestion des autorisations.

2. Transparence algorithmique

L'essor de l'IA médicale pose la question centrale de la compréhensibilité des décisions automatisées.

Les algorithmes d'apprentissage profond fonctionnent souvent comme des « boîtes noires » à cause d'un raisonnements non explicables, des corrélations statistiques sans causalité et la difficulté d'audit externe.

Cette opacité entre en tension avec les exigences d'information du patient, de justification médicale et de responsabilité juridique.

La transparence algorithmique implique donc la Compréhension des critères décisionnels, l'accès aux variables utilisées, la traçabilité des calculs et la possibilité de contestation.

Elle conditionne la confiance dans la médecine algorithmique.

Des recherches visent à développer des systèmes capables de Justifier leurs recommandations de visualiser les zones d'analyse (imagerie) et de fournir des scores interprétables.

3. Biais et discrimination IA

L'éthique de l'IA médicale se trouve également confrontée au risque de reproduction des inégalités existantes.

On estime que les principales sources des biais algorithmiques sont le recours à des bases de données non représentatives, à des antécédents médicaux discriminatoires, à la sous-représentation de certaines populations et la présence de variables socio-économiques indirectes.

Ces biais peuvent conduire à des diagnostics moins précis pour certaines ethnies, des retards diagnostics pour certaines pathologies, une mauvaise évaluation de la gravité de la douleur et des inégalités d'accès aux traitements.

Le principe de justice impose l'équité des algorithmes la réalisation des audits de performance différenciés, la diversification des bases de données et le rôle de la supervision humaine corrective.

4. Déshumanisation du soin

Au-delà des risques techniques, la transformation numérique interroge la nature même de la relation thérapeutique.

On assiste à une érosion de la relation médecin–patient dans la mesure que la médiation technologique peut engendrer une réduction du temps de consultation, la focalisation du

médecin sur l'écran plutôt que le patient, une standardisation des décisions et une accentuation de la distance émotionnelle qui sépare les deux.

Il est classique de considérer que le soin délivré par le professionnel médical comporte à la fois une dimension empathique, une écoute subjective et une compréhension contextuelle et ne se réduit pas un simple acte technique.

Or, ces éléments émotionnels échappent largement aux systèmes automatisés et de ce fait le patient peut être réduit à un profil statistique, un score de risque, voir une suite de variables biologiques.

Cette objectivation algorithmique menace la dignité et la singularité de la personne.

L'enjeu éthique n'est pas d'opposer IA et médecins, mais d'organiser leur complémentarité IA est réservée pour l'analyse, l'humain pour la prise de la décision finale.

Dans l'idéale la technologie resterait un support dans la pratique médicale courante et ne pourrait constituer un substitut au facteur humain.

Les enjeux éthiques de la santé numérique révèlent l'ambivalence de la transformation digitale entre la promesse d'une médecine plus précise et le risque d'une médecine moins humaine.

Le consentement éclairé doit être repensé face à la complexité des traitements de données ; la transparence algorithmique devient une condition de légitimité des décisions automatisées ; la lutte contre les biais s'impose comme un impératif de justice sanitaire ; enfin, la préservation de la relation de soin constitue un enjeu anthropologique majeur.

Ainsi, l'éthique apparaît non comme un frein à l'innovation, mais comme une boussole normative, destinée à garantir que le progrès technologique demeure au service de la personne humaine, et non l'inverse.

V

Vers une gouvernance numérique globale de la santé

L'essor des technologies numériques appliquées à la santé (intelligence artificielle, Big Data, télémédecine, blockchain) a profondément reconfiguré les modalités de production, de circulation et de protection des données médicales.

Cette mutation ne se limite pas à une évolution technique ; elle appelle la mise en place d'une véritable gouvernance numérique globale de la santé, articulant sécurité, conformité juridique, supervision institutionnelle et harmonisation internationale.

La gouvernance numérique vise ainsi à encadrer l'usage des technologies de santé par des mécanismes intégrés de compliance, des autorités de régulation spécialisées, des standards internationaux et des modèles prospectifs capables d'anticiper les mutations technologiques futures.

1. Compliance et cybersécurité

La digitalisation des systèmes de santé s'accompagne d'une exposition accrue aux risques cybernétiques.

Les données médicales figurent parmi les informations les plus sensibles et les plus convoitées, tant pour leur valeur économique que pour leur potentiel d'exploitation malveillante.

Les établissements de santé sont devenus des cibles privilégiées des cyberattaques, entre les ransomwares paralysant les hôpitaux, les vols de dossiers médicaux, l'altération de données cliniques et le sabotage d'équipements connectés.

Ces attaques à l'encontre des systèmes de santé ont eu de graves conséquences et on a assisté une perturbation de la continuité des soins, la mise en danger de la sécurité des patients, un impact négatif sur la réputation des institutions et l'engagement de la responsabilité juridique des gestionnaires.

Pour faire face à ses menaces une politique de compliance numérique en santé a été élaborée et qui correspond à l'ensemble des mécanismes internes permettant aux organisations de soins se conformer aux normes juridiques, techniques et éthiques applicables.

Cette compliance numérique de santé comprend plusieurs volets

- Les politiques de sécurité des systèmes d'information.
- La cartographie des risques numériques.
- Les audits de cybersécurité.
- Les protocoles de gestion des violations de données.
- La formation du personnel médical.

Dans le secteur de la santé, la compliance implique une articulation étroite entre gouvernance hospitalière, protection des données et éthique médicale.

Pour ce qui est des dispositifs de cybersécurité dédiés au domaine médical ils incluent entre autres le chiffrement des données, une Authentification forte, la traçabilité des accès, l'hébergement certifié des données de santé et la Sauvegarde sécurisée des données de santé.

2. Autorités de régulation

La gouvernance numérique de la santé repose sur l'intervention d'autorités administratives et techniques chargées de superviser la conformité des pratiques.

Les Autorités nationales de protection des données veillent à la licéité des traitements, le respect du consentement, la sécurité des systèmes et à la sanction des violations.

Dans de nombreux pays, elles disposent de pouvoirs d'enquête, de contrôle et de sanction.

Outre les autorités de données personnelles, d'autres organismes (Ministères de la Santé, agence du médicament, les Ordres professionnels et les autorités de certification des logiciels médicaux) et qui sont des régulateurs sectoriels de la santé interviennent activement pour l'homologation des dispositifs numériques, l'encadrement de l'IA médicale, la régulation de la télémédecine et l'évaluation éthique des innovations.

La gouvernance efficace suppose une coordination entre les autorités sanitaires, les autorités numériques, les Instances éthiques et les acteurs privés technologiques.

3. Standards internationaux

La mondialisation des flux de données de santé impose une harmonisation normative au-delà des frontières nationales.

Plusieurs standards internationaux structurent la cybersécurité sanitaire :

- L'ISO/IEC 27001 pour le Management de la sécurité de l'information.
- L'ISO 27799 pour la Sécurité de l'information en santé.
- L'ISO 82304 pour la Qualité des applications de santé.

Ces référentiels définissent les procédures de gestion des risques, les exigences de sécurité et les obligations de traçabilité.

La gouvernance numérique s'appuie également sur des instruments juridiques supranationaux qui assure la réglementation de protection des données, les accords de transfert transfrontalier et qui dictent les directives de santé numérique.

Ils visent à garantir la souveraineté des données, la continuité des soins transfrontaliers et l'interopérabilité des systèmes.

Des organisations internationales ont formulé des principes encadrant l'IA et la santé numérique afin d'assurer la transparence algorithmique, l'équité des traitements, la responsabilité humaine finale et la protection de la dignité du patient.

4. Modèles de gouvernance futurs

La rapidité des innovations technologiques impose de repenser les modèles classiques de régulation sanitaire.

Les systèmes d'IA décisionnels nécessitent des audits algorithmiques, des certifications éthiques, des mécanismes d'explicabilité et une supervision humaine permanente.

Les futurs systèmes de santé doivent reposer sur des plateformes nationales de donnée, des entrepôts de données de santé et des infrastructures d'interopérabilité.

La gouvernance devra organiser :

- L'accès des chercheurs.
- Le partage sécurisé.
- La finalité des usages.

L'innovation numérique en santé dépend largement d'acteurs technologiques privés.

D'où l'émergence de gouvernances hybrides associant les États, les structures hospitalières, les Start-ups et les Assureurs.

Les modèles de gouvernance futurs doivent intégrer des dispositifs prospectifs :

- Des Comités d'éthique du numérique.
- Des Sandboxes réglementaires.
- Des évaluations de l'impact éthique.
- La démocratie sanitaire numérique.

La gouvernance numérique globale de la santé apparaît aujourd'hui comme une nécessité structurelle face à l'expansion des technologies digitales.

La sécurisation des systèmes par la compliance et la cybersécurité, la supervision par des autorités de régulation spécialisées, l'harmonisation par des standards internationaux et l'anticipation par des modèles prospectifs constituent les quatre piliers d'un écosystème sanitaire numérique fiable.

Toutefois, cette gouvernance demeure en construction, elle doit concilier innovation technologique, protection des libertés individuelles, souveraineté des données et efficience des systèmes de soins.

L'enjeu n'est plus seulement technique ou juridique : il est civilisationnel, engageant la manière dont les sociétés entendent protéger l'intimité médicale à l'ère de la donnée globale.

Conclusion

La transformation digitale du secteur de la santé constitue l'une des mutations systémiques les plus profondes qu'ait connues la médecine contemporaine.

L'irruption conjointe de l'intelligence artificielle, du Big Data, de la télémédecine et de la blockchain redessine les contours de la pratique médicale, de la gouvernance sanitaire et de la relation de soin elle-même.

Sur le plan technologique, ces innovations ouvrent des perspectives considérables. L'intelligence artificielle améliore la précision diagnostique et l'aide à la décision clinique ; l'exploitation des mégadonnées permet l'émergence d'une médecine prédictive et personnalisée ; la télémédecine réduit les inégalités territoriales d'accès aux soins ; enfin, la blockchain renforce la sécurité, la traçabilité et l'intégrité des informations médicales. Ensemble, ces outils participent à la construction d'un écosystème sanitaire plus efficient, plus connecté et potentiellement plus équitable.

Toutefois, ces avancées s'accompagnent de vulnérabilités nouvelles.

L'extension des flux de données de santé, leur interconnexion et leur traitement algorithmique exposent les systèmes de santé à des risques accrus de cyberattaques, de violations de confidentialité et de détournements informationnels.

La protection du secret médical ,pilier historique de la relation thérapeutique, se trouve ainsi confrontée à des défis inédits, appelant une refondation de ses mécanismes juridiques et techniques.

Les enjeux éthiques apparaissent, dans ce contexte, comme structurants.

Le consentement éclairé doit être repensé à l'ère des traitements algorithmiques complexes ; la transparence des systèmes d'intelligence artificielle devient une condition de légitimité décisionnelle ; la lutte contre les biais discriminatoires s'impose comme une exigence de justice sanitaire ; enfin, la crainte d'une déshumanisation du soin rappelle que la médecine demeure avant tout une pratique relationnelle, fondée sur l'écoute, l'empathie et la confiance.

Face à ces mutations, l'émergence d'une gouvernance numérique globale de la santé apparaît indispensable.

Celle-ci repose sur quatre piliers complémentaires : la compliance et la cybersécurité, garantes de la résilience des systèmes d'information ; l'action des autorités de régulation, chargées de superviser les usages technologiques ; l'harmonisation par des standards internationaux, assurant l'interopérabilité et la sécurité transfrontalière ; enfin, l'élaboration de modèles prospectifs de gouvernance, capables d'anticiper les innovations futures.

L'enjeu dépasse désormais la seule modernisation technique des systèmes de santé.

Il s'agit de construire un cadre de confiance numérique, conciliant innovation, protection des libertés fondamentales, souveraineté des données et éthique du soin.

La santé numérique ne pourra tenir ses promesses qu'à la condition de demeurer gouvernée par des principes humanistes, plaçant la dignité de la personne au cœur des architectures technologiques.

Ainsi, la transformation digitale en santé ne doit pas être pensée comme une substitution de la machine à l'humain, mais comme l'avènement d'une médecine augmentée, éthiquement encadrée, juridiquement sécurisée et socialement responsable.

Bibliographie

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare. *Healthcare, 7*(2).

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics* (8th ed.). Oxford University Press.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care — Addressing ethical challenges. *The New England Journal of Medicine, 378*(11), 981-983.

Fidelia Ibekwe-Sanjuan. VERS LA DATAFICATION DE LA SOCIÉTÉ ? Vincent Meyer. Transition digitale, handicaps et travail social, LEH Editions, pp.31-49, 2017, 978-2-84874-703-3. ffhal-01898457f

Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines, 28*, 689-707.

Jiang, F., Jiang, Y., Zhi, H., et al. (2017). Artificial intelligence in healthcare: Past, present and future. *Stroke and Vascular Neurology, 2*(4), 230-243.

Keesara, S., Jonas, A., & Schulman, K. (2020). Covid-19 and health care's digital revolution. *The New England Journal of Medicine, 382*, e82.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical applications. *Journal of the American Medical Informatics Association, 24*(6

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms. *Big Data & Society, 3*(2).

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare. *Health Information Science and Systems, 2*(3).

Shen, N., Bernier, T., Sequeira, L., et al. (2018). Understanding the patient perspective of AI in healthcare. *JMIR Human Factors, 5*(3).

Topol, E. (2019). *Deep medicine: How artificial intelligence can make healthcare human again*. Basic Books.

Les Cadres juridiques et réglementaires

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD).

Health Insurance Portability and Accountability Act (HIPAA), U.S. Department of Health & Human Services, 1996.

Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (Maroc).

Loi n° 131-13 relative à l'exercice de la médecine (Maroc).

Loi n° 05-20 relative à la cybersécurité (Maroc).

Code pénal marocain

Rapports institutionnels et organisations internationales

Organisation mondiale de la Santé. (2021). *Ethics and governance of artificial intelligence for health*. WHO.

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*.

OCDE. (2019). *Artificial Intelligence in Society*.

Commission européenne. (2020). *White Paper on Artificial Intelligence*.

CNIL. (2020). *L'intelligence artificielle : enjeux et perspectives pour la protection des données*.

Standards techniques et cybersécurité

ISO/IEC 27001. (2022). *Information security management systems*.

ISO 27799. (2016). *Health informatics — Information security management in health*.

ISO 82304-1. (2016). *Health software — General requirements for product safety*.