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

Eighth Issue العدد الثامن

December 2025 دجنبر

e-ISSN : 3085 - 5039 : الرقم المعياري الدولي
Press number : 1/2025 : رقم الصحافة

8

مجلة المقالات الدولية
العدد الثامن، دجنبر 2025
e-ISSN : 3085 - 5039

مجلة المقالات الدولية
INTERNATIONAL ARTICLES JOURNAL

كلمة العدد

بسم الله الرحمن الرحيم

يسعد مجلة المقالات الدولية أن تضع بين أيدي القراء والباحثين العدد الثامن، في إطار رسالتها الرامية إلى دعم البحث العلمي الرصين وتعزيز ثقافة النشر الأكاديمي الموثوق. ونذكر بفهرسة المجلة ضمن معامل التأثير العربي (AIF)، بما يمثله من اعتراف رسمي وأحد معايير تصنيف الجامعات العربية ضمن أول تصنيف عربي للجامعات. كما نعتز باستمرار إدراج المجلة ضمن International Scientific Indexing (ISI)، في محطة نوعية تعكس ثقة المجتمع العلمي في جودة ما ننشره، وتسهم في توسيع انتشار بحوثنا وتعزيز أثرها العلمي.

وإذ نقدم هذا العدد بما يزخر به من بحوث ودراسات متنوعة، فإننا نؤكد التزامنا الدائم بتحكيم علمي صارم، وأخلاقيات بحثية راسخة، ومعايير جودة وشفافية ثابتة، بما يخدم قيم التميز والمعرفة، ويدعم الباحثين في إنتاج علمي رفيع يسهم في تطوير الفكر والواقع. والله ولي التوفيق

رئيس التحرير

Arab Impact Factor

INTERNATIONAL Scientific Indexing

ISSN INTERNATIONAL STANDARD SERIAL NUMBER
e-ISSN : 3085 - 5039

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 8، دجنبر 2025

اللجان العلمية

محتويات العدد

3-19	**جدلية الأمن الحدودى وحقوق المهاجرين** سعيد خمري - نعمان محمد
20-33	**الدور التشريعي للمستشار الوزاري المكلف بالشؤون البرلمانية: قراءة في الإطار الدستوري والممارسة العملية** عمر الشرقاوي - خديجة مستفيد
34-58	**فعالية مجلس النواب بالمغرب فى تقييم السياسات العمومية: نموذج الولاية الحادية عشر 2021-2026** هشام وداد
59-83	**التكوين المستمر بين الحاجة لتطوير الموارد البشرية وضرورة تحديث الإطار القانوني** فاطمة الزهراء حبيدة
84-127	**مساهمة الاجتهاد القضائي الدستوري في تجويد الصياغة التشريعية تحقيقا للأمن القانونـي** عزيز الساكت
128-141	**السياسات العمومية الموجهة للشباب بالمغرب بعد دستور 2011: بين طموح التأطير وتحديات التفعيل** عزالدين العمارتي
142-167	**L'impact des Technologies de l'information et de la communication (TIC) sur la croissance économique : cas de la Mauritanie** Ahmed SIDIYA - Mohamed M'HAMDI - Dah BELLAHI
168-187	**La conciliation entre propriété intellectuell et intérêt général dans le cadre juridique marocain** Aziza DAALOUS - El Moukhtar TBITBI
188-201	**Valorisation des Services Écosystémiques Culturels et du Potentiel Écotouristique de la Cédraie du Parc National de Khénifra, Maroc : Une Analyse Prospective** Youssef EL-BAZ
202-216	**Le droit marocain face au défi de la réparation du préjudice écologique : entre inspiration comparée et limites internes** Basma RIZQY
217-230	**Le secret médical à l'épreuve de la santé numérique : enjeux éthiques, juridiques et technologiques** Oussama LOUKILI - Nadia AZDDOU

International Articles Journal
مجلة المقالات الدولية
A peer-reviewed, multidisciplinary journal
مجلة محكمة، متعددة التخصصات
Issue 8, December 2025
العدد 8، دجنبر 2025

Le secret médical à l'épreuve de la santé numérique : enjeux éthiques, juridiques et technologiques

Medical confidentiality in the age of digital health: ethical, legal and technological challenges

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

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

Abstract:

In the era of digital health, medical confidentiality — regarded as a cornerstone of the trust-based relationship between patient and practitioner — has been profoundly transformed, even shaken, by the rapid emergence of new digital health technologies in the medical field.

The dematerialization of medical records, the expansion of telemedicine, the proliferation of connected medical devices, and the growing use of artificial intelligence (AI) have disrupted the traditional frameworks of confidentiality.

In Morocco, the principle of medical secrecy, firmly anchored in the national legal framework through the Penal Code (Art. 446), Law No. 131-13 governing the practice of medicine, and Law No. 09-08 on the protection of personal data, now faces major technological and legal challenges brought by digitalization.

Although the National Commission for the Control of Personal Data Protection (CNDP), the General Directorate for the Security of Information Systems (DGSSI), and Law No. 05-20 on cybersecurity provide partial regulation, a gap remains concerning the specific management and processing of health data.

This article examines the foundations, challenges, and futurs prospects of medical confidentiality within a digital environment, in light of Moroccan law compared with the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

It highlights the tension between the imperative of innovation and the need for protection, and proposes governance approaches grounded in ethics, accountability, and security.

Keywords :

medical confidentiality, digital health, artificial intelligence, ethics, Moroccan law, GDPR, HIPAA, data protection.

Résumé:

À l'ère de la santé numérique, le secret médical considéré comme une pièce angulaire dans la relation de confiance entre patient et praticien se trouve profondément transformé voir ébranlé par l'entrée en force des nouvelles technologies de la santé numérique dans le domaine médical.

Ainsi la dématérialisation des dossiers médicaux, la télémédecine, les objets connectés et l'usage de l'intelligence artificielle (IA) viennent bouleverser les cadres traditionnels de la confidentialité.

Au Maroc, le principe de secret médical, ancré dans le cadre juridique national à travers le Code pénal (art. 446), la loi 131-13 relative à l'exercice de la médecine, et la loi 09-08 sur la protection des données personnelles, se trouve confronté aux mutations techniques et juridiques du numérique.

Si la Commission nationale de contrôle de la protection des données personnelles (CNDP), la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) et la loi 05-20 sur la cybersécurité encadrent certains aspects, on note toutefois la persistance d'un vide quant à la spécificité du traitement des données de santé.

Cet article passe en revue les fondements, défis et perspectives du secret médical dans un environnement numérique, à la lumière du droit marocain comparé au RGPD et à la loi HIPAA.

Il met en évidence la tension entre l'impératif d'innovation et l'exigence de protection, et propose des pistes de gouvernance fondées sur l'éthique, la responsabilité et la sécurité.

Mots clés :

secret médical, santé numérique, intelligence artificielle, éthique, droit marocain, RGPD, HIPAA, protection des données.

Introduction

Le **secret médical** constitue un principe cardinal du droit de la santé et de la déontologie médicale.

Constituant un Héritage du serment d'Hippocrate, il s'est imposé au fil des décennies comme une garantie fondamentale de la **dignité** et de la **vie privée** du patient.

Au Maroc, ce principe fondamental est expressément consacré par le **Code pénal** (article 446), la **loi 131-13** régissant l'exercice de la médecine, et la **loi 09-08** relative à la protection des données à caractère personnel.

Ces textes représentent le socle d'un dispositif normatif qui vise la préservation de la confidentialité des informations de santé.

Pourtant, depuis quelques années, on assiste à une **révolution numérique** qui bouleverse profondément le système de santé.

La santé numérique, ou l'utilisation des technologies numériques pour la santé, est devenue un domaine de pratique important pour l'utilisation des formes courantes et novatrices des technologies de l'information et de la communication (TIC) pour répondre aux besoins sanitaires. Le terme « santé numérique » trouve ses racines dans la cybersanté, qui est définie comme « l'utilisation des technologies de l'information et de la communication au service de la santé ainsi que des domaines qui lui sont liés ».

La santé mobile (mHealth) est une sous-catégorie de la cybersanté et se définit comme « l'utilisation des technologies mobiles sans fil pour la santé ».

Plus récemment, le terme santé numérique a été introduit en tant que « terme générique englobant la cybersanté (incluant la santé mobile), ainsi que des domaines émergents, tels que l'utilisation des sciences informatiques avancées dans les « mégadonnées », la génomique et l'intelligence artificielle »

Que ça soit La **télémédecine**, la **gestion électronique des dossiers médicaux (DME)**, les **plateformes de e-santé** et l'usage croissant de **l'intelligence artificielle (IA)** on assiste à une modification radicale de la nature, du volume et des circuits de circulation des données médicales.

Ces transformations, tout en contribuant à la modernisation du système de soins, soulèvent de nouveau défis et exposent les patients à de nouveaux risques, on peut citer la violation du secret, le piratage des bases de données, le détournement des données sensibles pour des fins commerciales ou encore les biais algorithmiques qui peuvent affecter la confidentialité.

Au Maroc, la Commission nationale de contrôle de la protection des données personnelles (CNDP), instituée par la loi 09-08, joue un rôle primordial dans la régulation des traitements de données à caractère personnel, toutefois son action reste freinée par l'absence d'un cadre juridique spécifique à la santé numérique malgré la sensibilité des données de santé.

De même, la **Direction Générale de la Sécurité des Systèmes d'Information (DGSSI)**, qui relève de l'administration de la défense nationale, et qui veille sur la cybersécurité, ne dispose pas d'une approche sectorielle propre à la santé.

Dans un contexte où le Maroc aspire à un **système national intégré de e-santé**, les enjeux sont majeurs : comment concilier l'**innovation technologique** avec le **respect du secret médical** ? Comment garantir la **confidentialité des données de santé** sans freiner la recherche et la coopération numérique internationale ?

Cet article ambitionne d'explorer ces interrogations à travers une approche **pluridisciplinaire** — à la fois **juridique, éthique et technologique** —, en s'appuyant sur le droit marocain, la comparaison internationale et les standards de gouvernance des données.

La réflexion s'articulera autour de trois axes :

- Le premier axe traitera les **fondements et principes du secret médical** dans le contexte numérique (I) ;
- Le deuxième axe abordera les **nouveaux défis éthiques, juridiques et technologiques** auxquels ce secret est confronté (II) ;
- Et enfin, le troisième axe abordera les **perspectives d'adaptation et de gouvernance** du cadre marocain pour son alignement avec les meilleures pratiques internationales (III).

Partie I – Les fondements et principes du secret médical à l'ère numérique

1. Le secret médical : un principe éthique et déontologique universel

Le secret médical est un principe ancien, ancré dans l'histoire de la médecine et du droit, et ce depuis le **serment d'Hippocrate**, il impose au médecin une obligation de discrétion absolue : « Tout ce que je verrai ou entendrai dans la société, je tairai ce qui ne doit pas être divulgué ». Au-delà de la simple confidentialité, ce serment reflète le **fondement moral** de la médecine, qui repose sur la **confiance** du patient envers son médecin.

La doctrine s'accorde à considérer que le secret médical représente **à la fois une obligation professionnelle, un devoir moral et un droit du patient** (Carbonnier, 2016). Dans cette perspective, le respect du secret médical vise une double finalité :

- **La Protection la vie privée** du malade, en interdisant toute divulgation sans consentement préalable de ce dernier
- La préservation **de la crédibilité du système de soins**, fondée sur une confiance réciproque.

L'Organisation mondiale de la santé (OMS) rappelle que le respect du secret médical fait partie intégrante du **droit à la santé** et du **principe de non-discrimination**. De même, la **Déclaration universelle sur la bioéthique et les droits de l'homme** adoptée par l'UNESCO (2005) affirme que la confidentialité est une condition essentielle de la dignité humaine.

On considère alors le secret médical comme étant une **valeur universelle**, un principe de civilisation, un pilier de l'éthique médicale à l'ère numérique qui dépasse la vision classique du simple devoir individuel du praticien

2. Le cadre juridique marocain du secret médical

Au Maroc, la protection du secret médical repose sur un **socle juridique pluriel**, par la combinaison des sources pénales, déontologiques et numériques.

a. Le Code pénal : la répression de la violation du secret

L'**article 446 du Code pénal marocain** érige en délit la révélation d'un secret par un médecin, un chirurgien, un pharmacien ou tout autre professionnel de santé.
Cette disposition, inspiré du droit pénal français, assure la protection de la **confidentialité absolue** des informations obtenues dans le cadre de l'exercice médical.
Elle sanctionne toute divulgation, qu'elle soit **intentionnelle ou par négligence**, les cas de dérogations légales à ce principe (à titre d'exemple, la déclaration obligatoire de certaines maladies, oule témoignage devant la justice sur autorisation du patient).

Ainsi, la violation du secret médical constitue un **délit autonome**, indépendamment du préjudice

Cette autonomie traduit la **valeur éthique et sociale** conférée au secret médical, qui dépasse le simple cadre individuel du patient pour représenter un **enjeu de confiance** collectif dans le système de santé.

Le caractère autonome de ce délit traduit aussi sa **fonction préventive** : la loi punit la révélation pour **empêcher la banalisation de la divulgation**.

La pénalisation vise donc le **maintien d'une vigilance permanente** et le rappel du fait que le secret médical n'est pas une simple formalité administrative, mais plutôt une **obligation absolue de réserve**.

b. La loi 131-13 relative à l'exercice de la médecine et le code déontologie médical

La **loi n° 131-13** du 19 février 2015, relative à l'exercice de la médecine, renforce la portée déontologique du secret.
Elle impose à tout praticien de **protéger la confidentialité des données de santé**, même après la mort du patient.
pour sa part l'article 4 du nouveau **Code de déontologie médicale de 2022** rappelle que « le secret professionnel s'impose à tout médecin dans les conditions établies par la loi » et s'étend à « tout ce qui a été vu, entendu ou compris ».

Cette règle s'applique quel que soit le support de l'information : papier, numérique, image ou fichier audio.

Ainsi, le passage vers la version numérisée de la **santé** n'allège en rien la responsabilité du praticien.

c. La loi 09-08 relative à la protection des données à caractère personnelles et la CNDP

Promulguée en 2009, la **loi n° 09-08** sur la protection des données personnelles marque une étape essentielle dans la reconnaissance juridique de la **donnée médicale**. Son article 1er qualifie les données relatives à la santé comme étant des **données sensibles**, et leur traitement requiert une **autorisation préalable** délivrée par la **Commission nationale de contrôle de la protection des données à caractère personnel (CNDP)**.

La CNDP veille au respect de la conformité des traitements des données, et la délivrance des autorisations des transferts internationaux de ces données, et toute violation aux principes de la loi 09.08 expose les organismes fautifs à de lourdes sanctions
Cependant, on note que la mise en application de cette loi demeure parfois limitée dans le domaine de la santé, par manque de culture numérique et de moyens de contrôle.

3. Le cadre international : de la confidentialité au droit à la protection des données

Le Maroc, en tant que partenaire privilégié de la rive euro-méditerranéenne ne peut ignorer ces engagements internationaux, et de ce fait il s'inspire profondément du **modèle européen de protection des données** en matière de protection des données

a. Le RGPD (Règlement général sur la protection des données)

Adopté par l'Union européenne en 2016, le **RGPD** érige la protection des données personnelles comme étant un **droit fondamental**.
Son article 9 interdit en principe le traitement des données de santé, sauf le cas des exceptions prévues par ce règlement notamment en matière de soins, de recherche et dans le cadre du respect de l'intérêt public.
les Objectifs clés du RGPD sont :

1. Le Renforcement des droits des personnes par la réglementation du droit d'accès, de rectification, d'opposition, à l'oubli, à la portabilité, à la limitation du traitement.
2. La Responsabilisation des acteurs qui assurent le traitement des données
3. L'Uniformisation des règles dans l'UE, au sin de l'union européen un seul règlement est généralisé à l'ensemble des 27 pays membres, mettant un terme à la directive européenne initiale de 1995.
4. La répression des manquements aux principes de ce règlement par de lourdes sanctions avec des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel des auteurs de l'infraction.

Ces principes inspirent de plus en plus les réformes des partenaires de l'union européen, le Maroc ne fait pas l'exception à travers une coopération entre la **CNDP** marocaine et les autorités européennes (CEPD).

b. Le modèle américain : la loi HIPAA (1996)

Pour ce qui est des États-Unis, la Health Insurance Portability and Accountability Act (HIPAA) est le texte réglementaire qui fixe les standards stricts à respecter afin d'assurer la sécurité et la confidentialité des données médicales électroniques.
Elle impose aux établissements de santé, assureurs et prestataires techniques de fournir les garanties afin de sécuriser le stockage et la transmission des informations relatives à la santé. Toute violation des conditions de recueil , de stockage et de transfert des données de santé expose les contrevenants à de lourdes sanctions administratives et pénales renforçant ainsi la culture de conformité.

c. Les instruments internationaux

La **Déclaration de l'OMS sur la santé numérique (2018)** et la **Stratégie mondiale de cybersécurité en santé** (2020) ont poussé les États signataires à intégrer la protection du secret médical dans leurs politiques publiques de transformation digitale.

En effet dans sa déclaration l'OMS exhorte les ministères de la santé « à évaluer leur utilisation des technologies numériques pour la santé [...] et à donner la priorité, comme il se doit, au développement, à l'évaluation, à la mise en œuvre, à l'intensification et à l'utilisation accrue des technologies numériques

Pour ce qui est de la stratégie mondiale de cybersécurité en santé, elle met l'accent sur le fait que les données sanitaires doivent être classées comme des données personnelles sensibles, ou des informations permettant d'identifier une personne, lesquelles imposent une norme de sécurité élevée.

Par conséquent, elle souligne la nécessité de disposer d'une base juridique et réglementaire solide afin de protéger la vie privée, la confidentialité, l'intégrité et la disponibilité des données ainsi que le traitement des données sanitaires personnelles, et de gérer les questions de cybersécurité, d'établissement de relations de confiance, de responsabilisation et de gouvernance, d'éthique, d'équité, de renforcement des capacités et de connaissances, en veillant à ce que des données de bonne qualité soient collectées et ensuite partagées pour appuyer les efforts en matière de planification, de mise en service et de transformation des services.

4. Le passage du secret individuel à la gouvernance des données de santé

L'ère du numérique a modifié profondément la nature classique du secret médical. Autrefois ce secret était circonscrit entre le médecin et le patient, de nos jours on assiste à l'extension de ce dernier à de nouveaux acteurs (prestataires de services numériques, hébergeurs, sociétés de télémédecine, chercheurs, et même assureurs.)

Le secret devient dès lors un objet de gouvernance collective, et sa garantie ne relève plus seulement du respect déontologique, mais plutôt de la sécurisation technique et de la traçabilité des accès aux données.
Les institutions comme la CNDP, la **DGSSI** et les **autorités sanitaires** sont dans l'obligation d'établir un cadre de coordination clair, afin de prévenir les fuites et les abus.

Cette mutation appelle à une **évolution conceptuelle** : le secret médical n'est plus seulement une **obligation de silence**, mais un **système de garanties juridiques et technologiques** au service de la dignité humaine

Partie II – Les nouveaux défis éthiques, juridiques et technologiques

1. Les enjeux éthiques : consentement, autonomie et confiance numérique

L'entrée de la médecine dans l'ère numérique bouleverse la conception classique du secret médical.
Le **consentement éclairé**, qui constitue l'un des fondements de l'éthique biomédicale, se trouve mis à l'épreuve par la complexité croissante des systèmes numériques et des algorithmes de traitement des données.

Au Maroc, la **loi 131-13** a consacré le droit fondamental du patient à l'information sur son état de santé, toutefois la dématérialisation du dossier médical soulève les difficultés au sujet de la compréhension réelle du recueil , du stockage et de l'usage des données.
Lorsqu'un patient donne son accord pour qu'une application mobile surveille son rythme cardiaque, ou qu'un hôpital partage ses examens pour l'entraînement d'un algorithme d'intelligence artificielle, peut-il réellement comprendre l'étendue du traitement et les risques associés ?

Cette opacité engendre clairement une atteinte au consentement libre et éclairé.
L'éthique médicale doit donc s'adapter à ce nouvel environnement par la promotion de la transparence algorithmique et la traçabilité des décisions automatisées.
Le concept de *consentement dynamique* par renouvellement régulier et contextualisé de ce dernier pourrait être une réponse adaptée, inspirée des réflexions du Comité international de bioéthique de l'UNESCO (2021).

On assiste à une redéfinition de la relation de confiance entre le médecin et le patient qui n'est plus uniquement interpersonnelle, mais médiée par des technologies.
De ce fait le patient doit faire confiance non seulement à son praticien, mais aussi aux plateformes numériques, aux hébergeurs de données et aux institutions qui en assurent le contrôle.
Ainsi, le secret médical se transforme en écosystème de confiance numérique, reposant sur la responsabilité partagée de tous les acteurs.

2. Les défis juridiques : le vide normatif et les limites du cadre actuel

Si le droit marocain a consacré la protection du secret médical, il n'a pas encore pu intégrer le caractère spécifique **des données de santé numériques**.
La **loi 09-08**, bien qu'avancée pour son époque, demeure centrée sur les données personnelles en général, sans distinction claire des données médicales ni exigence technique spécifique
De même, la **loi 05-20** relative à la cybersécurité traite la question de manière globale, sans approche sectorielle.

Ce vide normatif engendre plusieurs conséquences :

Le flou sur la responsabilité juridique : qui répond en cas de fuite de données ? Le médecin, l'établissement, l'hébergeur, ou le fournisseur de service numérique ?

L'absence d'obligation d'hébergement sécurisé : contrairement à la France, où les hébergeurs de données de santé doivent être certifiés HDS, le Maroc ne dispose pas encore d'un dispositif équivalent.

Le non-encadrement du Transfert international : certaines données médicales hébergées sur des serveurs étrangers échappent à la juridiction marocaine.

Si le Règlement général sur la protection des données (RGPD) européen impose des obligations strictes de sécurité, de notification et de traçabilité, la HIPAA, exigent la désignation d'un *privacy officer* et la tenue d'audits réguliers dans le contexte américain, le cadre juridique marocain reste malheureusement fragmenté et incomplet, notamment en matière de santé numérique et d'intelligence artificielle médicale.

Dans un contexte où les hôpitaux marocains optent pour l'adoption des solutions numériques étrangères, l'absence de législation claire fragiliserait la **souveraineté des données de santé**. La mise en place d'un **cadre légale unifié** apparaît désormais indispensable.

3. Les défis technologiques : cybersécurité, intelligence artificielle et interopérabilité

La vulnérabilité technologique constitue aujourd'hui l'un des principaux risques qui menace le secret médical.
on assiste à une multiplication des cyberattaques qui ciblent les hôpitaux et les cliniques à l'échelle international, entraînant des violations massives de données sensibles.
En 2023, plusieurs établissements hospitaliers européens ont été paralysés par des rançongiciels, et le Maroc n'est pas à l'abri de tels incidents.

La Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), à travers son cadre réglementaire et ses guides de sécurité, recommande aux institutions publiques l'adoption des normes de cybersécurité (ISO 27001, cryptage, authentification forte).
Cependant, dans le secteur privé, notamment les cliniques et laboratoires, la mise en application de ces recommandations laisse encore à désirer

Le développement de l'intelligence artificielle médicale soulève d'autres défis :

Comment garantir la confidentialité des données d'entraînement des algorithmes ?

Qui contrôle la qualité éthique des systèmes prédictifs ?

Comment prévenir la reconstruction d'identités à partir de données anonymisées ?

Les chercheurs (Mougeot, 2022 ; Parance, 2023) soulignent la nécessité d'un cadre de gouvernance algorithmique fondé sur la transparence, la supervision humaine et l'audit indépendant, et en l'absence de tels mécanismes, l'IA peut devenir un facteur amplificateur du risque de violation du secret médical.

Enfin, la question de l'interopérabilité des systèmes d'information reste centrale.
Le partage des dossiers médicaux électroniques entre hôpitaux, cliniques et praticiens libéraux suppose des standards communs et des protocoles sécurisés.
Une interopérabilité mal maîtrisée, sans normes de chiffrement robustes, constitue une menace directe pour la confidentialité.

Ainsi, loin de la neutralité attribuée à la technologie, elle doit être considérée comme un acteur du droit.
Elle impose au législateur de penser la protection des données dès la conception (*privacy by design*), et au praticien de développer une compétence numérique éthique

4. La gouvernance éthique et institutionnelle : vers une responsabilité partagée

L'enjeu majeur de la santé numérique réside dans la reconstruction d'une gouvernance du secret médical adaptée à la complexité des technologies.

En recourant à la santé numérique, on ne peut plus imaginer le secret comme une simple obligation individuelle du médecin, mais on doit définir une responsabilité collective, impliquant tous les acteurs du système de santé.

Cette gouvernance suppose, d'abord la coordination institutionnelle entre la CNDP, le ministère de la Santé, la DGSSI et l'Ordre des médecins ; la création de comités d'éthique du numérique en santé, chargés d'évaluer les projets d'IA et de télémédecine ; et l'adoption de chartes internes de confidentialité numérique dans chaque établissement de santé.

Sur le plan éthique, la transparence et la reddition des comptes doivent être les deux piliers de cette gouvernance.
Chaque acteur doit pouvoir démontrer, à tout moment, la traçabilité des traitements et le respect du consentement du patient.
Le secret médical devient alors un droit collectif à la protection numérique, garantissant la confiance dans le système de santé.

Comme le souligne Alain Supiot (2020) dans son ouvrage sur la gouvernance par les nombres, l'éthique des technologies ne consiste pas seulement à limiter leurs excès, mais à « réintroduire la responsabilité humaine dans les dispositifs techniques ».
C'est à cette condition que la santé numérique pourra se développer sans sacrifier les valeurs fondamentales de la médecine

Partie III – Perspectives et recommandations pour le Maroc

1. Vers un cadre législatif unifié pour la santé numérique

L'analyse des dispositifs actuels montre que le Maroc dispose d'un socle juridique solide, à travers les lois 09-08 sur les données personnelles, loi 131-13 sur l'exercice de la médecine, loi 05-20 sur la cybersécurité, Code pénal (art. 446) ; toutefois ce cadre reste éclaté et parfois inadapté aux exigences de la santé numérique.
Aucune de ces lois ne définit clairement la donnée de santé ni ne fixe des normes d'hébergement, d'audit ou de certification spécifiques.

Une des premières recommandations est donc l'adoption d'une loi-cadre sur la santé numérique, articulée autour de trois objectifs :

- Définition des catégories de données de santé et des obligations de sécurité correspondantes ;
- L'obligation de l'obtention d'une certification des hébergeurs de données médicales et des plateformes de télémédecine ;
- La Création d'un régime de responsabilité partagée entre les professionnels de santé, les établissements et les prestataires techniques.

Ce cadre légal pourrait s'inspirer du modèle européen de régulation sectorielle, tout en respectant les spécificités marocaines : la sacralité du secret médical, le rôle du Conseil de l'Ordre des médecins et le respect de la dignité humaine.
L'adoption d'une telle loi renforcerait la sécurité juridique pour les praticiens et encouragerait la confiance des citoyens dans la digitalisation du système de santé.

2. Renforcer les institutions de gouvernance et de contrôle

Le développement de la santé numérique exige le renforcement de la coordination institutionnelle.
Actuellement, la CNDP assure la supervision du traitement des données personnelles, tandis que la DGSSI encadre la cybersécurité.
Mais ces deux institutions agissent selon des mandats distincts, parfois sans articulation opérationnelle.

Il est donc recommandé la création d'un Comité national de gouvernance de la santé numérique, qui implique: la CNDP, pour la régulation des données personnelles, la DGSSI, pour la sécurité technique, le Conseil national de l'Ordre des médecins, pour la déontologie et les représentants du secteur privé et universitaire, pour la recherche et l'innovation.

Ce comité aurait la charge de définir des référentiels nationaux de sécurité pour les systèmes d'information hospitaliers, d'élaborer des chartes d'éthique du numérique en santé et d'assurer la supervision de la formation continue des professionnels.

Un tel organe favoriserait une gouvernance intégrée, essentielle pour concilier les impératifs de sécurité, de secret et de développement technologique.

3. Promouvoir une culture numérique éthique et juridique

La réussite de la transition numérique dans le domaine de la santé ne dépend pas seulement des lois, mais également des comportements et de la culture professionnelle.

La formation aux enjeux de protection des données et de secret professionnel numérique au profit des praticiens les gestionnaires et les informaticiens de santé est une pièce angulaire dans la réussite du chantier de transition numérique médicale

Les facultés de médecine et de droit devraient intégrer des modules d'éthique et de droit du numérique en santé dans leurs cursus, afin de préparer les futurs professionnels aux responsabilités qui les attendent.
De même, les établissements hospitaliers devraient instaurer des formations obligatoires sur la sécurité des systèmes d'information et la confidentialité des données.

La CNDP, en partenariat avec les universités, pourrait élaborer un label de conformité éthique pour les acteurs respectant les bonnes pratiques de protection des données.
Cette labellisation, à la fois préventive et valorisante, renforcerait la confiance du public et favoriserait l'exemplarité.

4. Encourager l'innovation responsable : IA, Blockchain et souveraineté numérique

Le Maroc a vocation à devenir un acteur régional majeur de la santé numérique, mais cette ambition doit reposer sur une innovation responsable.
Les technologies émergentes telles que l'intelligence artificielle, la blockchain, le cloud souverain doivent être intégrées dans un cadre éthique et sécurisé.

L'intelligence artificielle peut améliorer le diagnostic, la prédiction et la gestion hospitalière, mais elle ne doit pas devenir une « boîte noire » échappant au contrôle humain.
Le principe de supervision humaine des décisions automatisées, inspiré du RGPD, devrait être inscrit dans le droit marocain.

La blockchain, quant à elle, offre des opportunités inédites de traçabilité et de sécurisation des données médicales.
Son adoption dans les systèmes hospitaliers marocains pourrait garantir une transparence accrue sans porter atteinte au principe de respect du secret médical.

Enfin, la création de centres de données nationaux sécurisés permettrait d'assurer la souveraineté numérique du Maroc, en évitant la dépendance à des serveurs étrangers et en favorisant la recherche locale sur les données de santé anonymisées.

5. Vers une charte marocaine de la santé numérique

En parallèle à l'élaboration du cadre législatif, il nous parait opportun d'élaborer une Charte marocaine de la santé numérique, et qui serait adoptée conjointement par la CNDP, le ministère de la Santé et l'Ordre des médecins.
Cette charte aurait pour but le rappel des principes éthiques fondamentaux du secret médical ; l'énonce des droits numériques des patients (information, consentement, portabilité, rectification) ; et la définition des obligations des établissements et prestataires en matière de sécurité et de transparence.

Un tel instrument, à la fois normatif et pédagogique, permettrait la diffusion d'une culture nationale de la confiance numérique en santé.

Il placerait le Maroc dans une trajectoire conforme aux standards internationaux, tout en préservant son identité juridique et éthique.

Conclusion

Le **secret médical**, principe fondateur de la pratique médicale et pilier de la confiance entre le médecin et son patient, connaît aujourd'hui une transformation profonde sous l'effet de la **révolution numérique.**
La dématérialisation des données, la télémédecine, les objets connectés et l'intelligence artificielle ont fait émerger de **nouveaux défis éthiques, juridiques et technologiques** qui transcendent les frontières traditionnelles du secret professionnel.

Au Maroc, malgré l'existence d'un cadre juridique protecteur notamment le **Code pénal,** la **loi 131-13,** la **loi 09-08**, et **loi 05-20** , la réglementation demeure **fragmentée** et inadaptée à la complexité des traitements numériques.
Le **vide législatif** relatif à la santé numérique fragilise la sécurité juridique et la confiance du patient, notamment face aux risques de piratage, de fuite ou de réutilisation non autorisée des données de santé.

Les comparaisons internationales montrent que des dispositifs comme le **RGPD** européen ou la **HIPAA** américaine offrent des garanties plus cohérentes, articulant **sécurité, responsabilité et transparence.**
Le Maroc gagnerait à s'en inspirer pour concevoir une **loi-cadre sur la santé numérique**, harmonisant les obligations des acteurs publics et privés et intégrant la **gouvernance des données de santé** dans une vision éthique et souveraine.

Sur le plan éthique, le secret médical doit désormais s'appréhender comme un **principe de gouvernance numérique** : il ne se limite plus à une obligation de silence, mais s'étend à la conception même des systèmes technologiques, selon le principe de *privacy by design*.
La préservation du secret suppose donc une **responsabilité partagée** entre les praticiens, les établissements, les ingénieurs, les hébergeurs, et les institutions publiques.

Enfin, l'avenir du secret médical au Maroc repose sur la capacité des acteurs à instaurer une **culture de la confiance numérique,** fondée sur la formation, la transparence et l'innovation responsable.
Le défi consiste moins à résister à la transformation numérique qu'à l'accompagner, en faisant du secret médical **un instrument de protection et non un obstacle à l'innovation.**
La conciliation entre progrès technologique et respect de la dignité humaine demeure, plus que jamais, la condition d'une médecine éthique et durable.

Bibliographie

Textes législatifs et réglementaires :

- Code pénal marocain, art. 446 et suivants.

- Loi n° 131-13 relative à l'exercice de la médecine, Bulletin officiel du 19 février 2015.
- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (2009).
- Loi n° 05-20 relative à la cybersécurité (2020).
- Code de déontologie médicale marocain (2022).
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD).
- Health Insurance Portability and Accountability Act (HIPAA), U.S. Department of Health & Human Services, 1996.
- Lignes directrices de l'OMS : recommandations sur les interventions numériques pour le renforcement des systèmes de santé [WHO guideline : recommendations on digital interventions for health system strengthening]. Genève, Organisation mondiale de la Santé, 2022. Licence : CC BY-NC-SA 3.0 IGO
- Stratégie mondiale pour la santé numérique 2020-2025 [Global strategy on digital health 2020-2025]. Genève : Organisation mondiale de la Santé ; 2021. Licence : CC BY-NC-SA 3.0 IGO

Ouvrages et articles :

- Carbonnier, J. (2016). *Droit civil : Introduction, les personnes, la famille, les incapacités*. PUF.
- Parance, B. (2023). *Les données de santé à l'épreuve du numérique : enjeux éthiques et juridiques*. Revue de droit sanitaire et social, 59(2), 145-163.
- Mougeot, M. (2022). *Éthique et intelligence artificielle médicale : entre transparence et responsabilité*. *Médecine & Droit*, 194(4), 201-212.
- Supiot, A. (2020). *La Gouvernance par les nombres, Paris, Fayard, 2015, 2nde éd. coll. Pluriel, 2020*.
- Rouvillois, F. (2019). *Le secret médical à l'heure de la e-santé*. *Revue française d'éthique appliquée*, 6(2), 87-101.
- Béatrice Parance, B., & Lachièze-Rey, P. (2021). *Bioéthique et droit de la santé*. Dalloz.
- Organisation mondiale de la santé (OMS). (2018). *Stratégie mondiale sur la santé numérique 2020-2025*. Genève.
- UNESCO. (2005). *Déclaration universelle sur la bioéthique et les droits de l'homme*. Paris.
- UNESCO. (2021). *Rapport du Comité international de bioéthique sur les implications éthiques de l'intelligence artificielle dans la santé*.
- OCDE. (2020). *Principes de gouvernance responsable des données dans la santé*. Paris.
- CNDP. (2021). *Guide pratique sur la protection des données de santé au Maroc*. Rabat.
- DGSSI. (2022). *Cadre national de cybersécurité et bonnes pratiques pour le secteur de la santé*. Rabat.
- Loukili, O. (2025). *L'intelligence artificielle et le secret médical : état des lieux et perspectives au Maroc*. *Revue marocaine du droit de la santé*, 12(3), 45-67.
- Tscheulin, D., & Drevs, F. (2020). *Digital health and patient trust: Ethical considerations in medical data sharing*. *Journal of Medical Ethics*, 46(9), 621-628.
- Freeman, T., & Kennedy, A. (2019). *Enacting corporate governance of healthcare safety and quality*. *Sociology of Health & Illness*, 41(2), 284-302.
- European Data Protection Board (EDPB). (2022). *Guidelines on health data processing under the GDPR*. Bruxelles.

- Conseil national de l'Ordre des médecins du Maroc. (2023). *Charte de déontologie numérique en santé (projet de consultation)*.
- Haute Autorité de Santé (HAS). (2021). *Référentiels éthiques et certification des systèmes d'IA en santé*. Paris.
- Revue marocaine de bioéthique et droit médical. (2024). *Numéro spécial sur le secret médical et la transformation numérique*.
- OECD Health Division. (2023). *Digital governance in healthcare: Policy lessons for emerging economies*. Paris.