SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 11, No. 4, (2025), pp. 744-750
Open Access. Online & Print

DOI: 10.5281/zenodo.11425161

HEALTH DATA IN THE DIGITAL AGE: LEGAL RESPONSES TO THE USE OF AI AND METAVERSE IN MEDICAL SERVICE

Tareck Alsamara[1], Farouk Ghazi[2]

[1]Prince Sultan University, Saudi Arabia, https://orcid.org/0000-0003-0202-0024
[2]Badji Mokhtar Annaba University, Algeria, https://orcid.org/0000-0002-3797-8737

Received: 11/11/2025
Accepted: 18/12/2025

ABSTRACT

This article addresses the issue of personal data protection related to medical services in light of recent technological developments. The global medical system is witnessing a major digital transformation toward artificial intelligence and the Metaverse. The article uses a scientific approach based on diagnosing technological developments and linking them to the current legal framework through an analytical approach. The article concludes that the traditional contractual relationship between doctor and patient has undergone radical transformations, with the entry of third parties that manage artificial intelligence systems, such as Metaverse and other digital platforms and cloud spaces. Therefore, there are justifiable concerns regarding the threat to the confidentiality of the doctor-patient relationship on the one hand, and the privacy of personal data resulting from the use of these systems on the other. Furthermore, there is a need to give national legislation a transnational dimension to ensure that patients' rights to the protection of their personal data are not violated.

KEYWORDS: Health Data - Digital law -Technological Innovation - Medical Service.

1. INTRODUCTION

The integration of artificial intelligence and the virtual world into healthcare services is reshaping the digital ecosystem, creating new forms of interaction, data exchange, and identity representation. Traditionally, the doctor-patient relationship has been simple and straightforward, but it has become more complex with the introduction of technology to guide, examine, and treat patients. Although humans have not been replaced in the healthcare field, the introduction of technology has sparked significant legal debate. This technology contributes to the generation of massive data related to patients' identities, behaviors, and lifestyles. This raises questions about how to protect this data. This technological development has made transnational digital platforms a reason to rethink the principle of territoriality in personal data protection laws and to activate international cooperation between countries in ensuring the protection of patients' personal data. However, all currently existing personal data protection laws were enacted at a time before the emergence of artificial intelligence systems and metaverse programs; hence, there is a noticeable gap in this area.

Perhaps one of the most significant issues raised in this article relates to the emergence of new forms of data, through the concept of digital avatars and virtual identities, and how these challenge traditional definitions of "data subject" in law.

This article aims to identify and address the legal issues associated with protecting personal data when using AI and Metaverse systems in healthcare, and how patient consent and compliance by operators of these platforms play a significant role in data protection.

2. METHOD

The article uses a scientific approach that is appropriate for studying the subject from the point of view of legal sciences, as it relies on the analytical approach in order to analyze the texts of national laws of countries and international law. It also relies on the descriptive approach in describing the laws in order to diagnose them in terms of the extent to which they keep pace with the developments taking place in this field. The article also relies on the comparative approach in order to compare the various laws of different countries.

3. RESULTS AND DISCUSSION

3.1. Definition Of Personal Data

Personal data, also known as personal information, is essentially a set of information, regardless of its source, that identifies or makes a person identifiable, based on elements related to the person, such as their body, biometric data, and even their behavior. (Bygrave, 2010; Stalla-Bourdillon & Knigh, 2016). In French law, "personal data," is information relating to an identified or identifiable natural person (e.g., last name, first name, social security number, address, telephone number, email address, photo, fingerprint, geolocation data, IP address, or online identifier).A person is said to be identified when their identity is known. A person is identifiable when they can be identified, even if their first and last name remain unknown, by cross-referencing a set of data (e.g., a woman living at a given address, born on a given day, and a member of a given association) (Department of Legal and Administrative Information, 2024) . In UK law, "personal data" is defined under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as any information relating to an identified or identifiable living individual ("data subject"). According to the terms of the Act, an individual is identifiable if they can be identified, directly or indirectly, by reference to identifiers such as a name, identification number, location data, online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. This definition emphasizes the broad scope of what constitutes personal data, covering both obvious identifiers (like names) and less direct ones (like IP addresses or behavioral characteristics) (Warren, 2002; Wallace et al, 2014). The Algerian legislation defines personal data or information in Article 03, Paragraph 01 of Law 18-07 as: "Any information, regardless of its source, relating to a known or identifiable person, referred to below as 'the person concerned', directly or indirectly, particularly by reference to an identification number or one or more elements specific to his physical, physiological, genetic, biometric, psychological, economic, cultural or social identity."

3.2. Legal Protection of Personal Data in International Conventions

Many international conventions and agreements stipulate the protection of personal data. Among these conventions is the Universal Declaration of Human Rights, Article 12 of which states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." Everyone has the right to the protection of the law against such interference or attack (Lim and Junhyoung, 2025). The OECD Convention on Consumer Protection in Electronic Commerce also includes provisions on privacy risks, security, payment protection, and the safety of goods. The OECD Recommendation on Privacy Protection and Cross-Border Flows of Personal Data includes key principles, including those related to limiting data collection, data quality, security safeguards, individual participation, accountability, and more (Qin et al, 2025; Shaik & Poojasree, 2021).At the European Union legislative level, we find the General Data Protection Regulation (GDPR) of 2016, which provides a strong framework for the protection of personal data in the European Union (Sarabdeen & Mohamed, 2025).

3.3. Legal Protection of Personal Data in National Law

National law defines the processing of personal data as any operation or set of operations carried out by automated or non-automated means on personal data, such as collection, recording, organization, storage, adaptation, modification, extraction, access, use, communication, by transmission, publication, or any other form of availability, approximation, or environmental connection, as well as blocking, encryption, erasure, or destruction (Bouker, 2024). The Algerian legislation also obligates the person responsible for processing personal data and information to take appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, loss, publication, or unauthorized access, especially when processing requires sending data over a specific network, as well as protecting it from any form of unlawful processing, as processing must include taking an appropriate degree of security measures in view of the risks (Meramria & Bouadjila, 2024).

3.4. New Challenges

3.4.1. The Use of the Metaverse in Healthcare Services

The integration of the Metaverse into healthcare services represents a paradigm shift in the current era, providing immersive, interactive environments for medical training and teaching, remote consultations, mental health treatment, and patient education. Through virtual reality (VR) and augmented reality (AR), healthcare professionals can simulate surgical procedures, collaborate across borders, and provide real-time care in 3D virtual clinics (Jeong & Lee, 2025; Chaddad & Jiang, 2025). Furthermore, the Metaverse is currently being used to train specialists and students to perform virtual surgeries. Virtual laboratories are interactive digital simulations of activities typically performed in physical laboratory settings. These virtual laboratories mimic the tools, equipment, tests, and procedures used in various medical, engineering, chemistry, physics, and other disciplines to create a realistic scenario. Recent global studies have demonstrated how educational activities that resemble real-world work conditions enhance learning transfer (Marwa, 2025; Burlacu et al, 2025).

It is important to note that this innovation enhances the accessibility and efficiency of medical care, particularly for remote or underserved populations. However, the Metaverse poses downsides related to privacy challenges. The immersive nature of these environments means that users generate large amounts of sensitive biometric, behavioral, and health data. Unlike traditional telemedicine platforms, the Metaverse collects real-time inputs, such as facial expressions, eye movements, voice patterns, and physiological responses. This information is often classified as personal data by law and can potentially reveal highly personal information. Ensuring compliance with data protection laws, such as the General Data Protection Regulation (GDPR), becomes increasingly important. Therefore, developers of these programs must consider how to ensure their programs comply with legal rules related to the protection of personal data (Adil et al, 2025, Pasa, 2025). There is also a legal debate surrounding the ownership of data generated by the use of virtual reality software. The involvement of developers and virtual reality service providers raises concerns about data ownership. Software developers must incorporate patient consent and combat unauthorized access. Strong encryption must be adopted to ensure transparent privacy and strict access controls to prevent the theft of patient data or access to their identity (Bayaraa et al, 2025, Adeyinka & Adeyinka, 2025).

3.5. The Use of AI In Healthcare Services

There are several risks associated with using AI in healthcare, including the potential for misuse that violates human rights to privacy and personal data protection laws. AI systems can collect information on patient healthcare and behavior. This is sensitive information protected by national law (Corfmat et al, 2025; Wilhelm et al, 2025; Meskic et al, 2022; Hassan et al, 2021). AI systems can meet personal data laws by implementing data processor obligations as defined in the law, which are principles that define what a data processor must do, such as restricting use, obtaining consent, and working with only necessary data (Zahra, 2025). The information most at risk is personal data, patient records, biometric data, mental health information, and finally, patient behavior and lifestyle. Although AI developers in the healthcare field are making significant strides in anonymizing patients, concerns remain about whether they are sufficiently anonymous and are protected from hacking and unauthorized access (Zainab et al, 2025). The most vulnerable types of patients when processed by AI technologies include those with chronic illnesses, mental health conditions, genetic disorders, or rare diseases, as well as elderly individuals and children. These groups often have more detailed and sensitive health record (Abdulai, 2025; Joshi, 2025).

Currently, AI systems cannot be held civilly liable for breaches of the law, because AI does not have legal personality (Azis, 2025; Alsamara & Farouk, 2025). Rather, the human operator of AI systems is liable under civil law. For example, under the French Civil Code, in the absence of specific provisions governing specific categories of objects, Article 1242 Paragraph 1 applies. Its general scope covers a wide range of cases. This provision therefore applies to all movable and immovable objects, moving and moving, dangerous and non-dangerous. This general approach to operator liability for objects is rooted in the nature of Article 1242, which seeks to establish a framework for civil liability arising from the use of objects regardless of their characteristics. In short, Article 1242 of the Civil Code, which reiterates the provisions of the previous Article 1384, constitutes a central mechanism for personal liability associated with objects. It clearly defines the rules, enshrines exceptions governed by specific regulations, and sets limits on their application, taking into account the inherent characteristics of certain categories of objects. In the absence of special regulations, Article 1242 regulates the general rule that governs a variety of things and circumstances, thus confirming the pivotal and fundamental role of this rule in the field of civil liability (Solaiman & Malik, 2025; Ballell, 2025). This principle could be extended to medical services as well.

At the level of legal precedents, it is worth noting the Meta case before the German courts. On May 23, 2025, the Higher Regional Court in Cologne heard an urgent case filed by the German consumer protection organization (VZ NRW) against Meta, accusing it of violating the General Data Protection Regulation (GDPR) by using historical user data to train artificial intelligence systems without their explicit consent. The organization demanded an immediate halt to model training before the main lawsuit begins. The court refused to issue an interim injunction against Meta, considering that the legal criteria required to prove urgent harm had not yet been met. It emphasized that this decision does not preclude the main case, which will be decided at a later stage (Aitana et al; 2025).

Patient consent plays an important role in protecting their data. Furthermore, hospitals and clinics must implement their legal obligations in the field of data protection by establishing audit and inspection committees (Lekadiret al, 2025; Farouk& Alsamara, 2023). We note that the current legal framework is currently insufficient. For example, there is a single text at the European Union level that discusses the issue in detail, but legislation, including European legislation, still lacks clear provisions specifically for artificial intelligence (Judge et al, 2025; Alsamara & Ghazi, 2024). From a technical standpoint, the principle of privacy-by-design remains the greatest guarantee for the protection of personal data (Del-Real et al, 2025). In addition, artificial intelligence impacts the confidentiality of the doctor-patient relationship. Previously, the relationship was direct, without an intermediary, but through applications, the intervention of a third party has impacted this confidentiality. Algorithms and cloud computing represent a third party that impacts the confidentiality of the relationship between the doctor and their staff on the one hand, and the patient on the other. Since the operator of these cloud spaces cannot be guaranteed to comply, these spaces often cross-national borders, making it difficult to comply with the laws of a single country (Albakjaji & Kasabi, 2021; Alsamara & Farouk, 2024). It is important to note that digital identity management systems for patients enable the reliable management of patient records within a digital environment, allowing control over access to patient data, verification of their identity, and the obtaining of their explicit consent.

3.6. Liability For Damages Caused by Artificial Intelligence and Metaverse Technology

Currently, there are no specific provisions regulating civil liability for damages caused by artificial intelligence and metaverse technology, as this technology does not have legal personality and is therefore subject to the general rules of civil liability for things.

The person who uses or operates this technology is responsible for its errors and the resulting damages. This person may seek to hold the manufacturer liable under the framework of product liability for defective products.

3.7. Criminal Responsibility on the Personal

Data Violation:

National law includes criminal provisions to ensure the implementation of personal data protection laws. Algerian law stipulates that, without prejudice to the more severe penalties provided for in applicable legislation, the processing of personal data in a manner that does not respect human dignity and privacy shall be punishable by imprisonment from two (2) to five (5) years and a fine of 200,000 DZD to 500,000 DZD. Anyone who processes personal data in violation of the law without the concerned party's consent shall be punished by imprisonment from one (1) to three (3) years and a fine of 100,000 DZD to 300,000 DZD. The same penalty shall be imposed on anyone who processes personal data despite the person concerned's objection, when such processing is intended, in particular, for commercial advertising or when the objection is based on legitimate grounds. Finally, anyone who carries out or orders the processing of personal data without respecting the condition of prior authorization by the national authority shall be punished with imprisonment from two (2) to five (5) years and a fine from 200,000 DZD to 500,000 DZD.

Tunisian law also includes provisions to guarantee the protection of personal data, stipulating a prison sentence of two to five years and a fine of five thousand to fifty thousand dinars for anyone who transfers personal data outside the country. Attempts are punishable by two years' imprisonment and a fine of ten thousand dinars for anyone who processes data related to crimes. The same penalties apply to anyone who processes personal data without the concerned party's consent. Anyone who induces a person to consent to the processing of their personal data by deception, violence, or threats is punishable by one year's imprisonment and a fine of ten thousand dinars. Anyone who intentionally transmits personal data for the purpose of achieving a benefit for themselves or others or to cause harm to the person concerned shall be punished with one year's imprisonment and a fine of five thousand dinars. Anyone who intentionally processes personal data without submitting the declaration stipulated in Article 7 or obtaining the license stipulated in Articles 15 and 69 of the Data Protection Law, or who continues to process data after the processing has been prohibited or the license has been withdrawn, or who publishes personal data related to health despite the prohibition of the authority stipulated in the second paragraph of Article 65 of the Data Protection Law, or who transfers personal data abroad without the authorization of the National Authority, shall also be punished with one year's imprisonment and a fine of five thousand dinars.

4. CONCLUSION

The article highlights a legislative deficiency in the field of personal data protection and reliance on artificial intelligence and the metaverse. At the national legislative level, there are no specific laws on the subject. Therefore, software developers are called upon to formulate professional ethical rules and codes to fill the legal gap. The general rules contained in personal data laws and civil law remain applicable to the interference of third parties in the traditional bilateral relationship between doctor and patient. States are invited to promote a legal framework for international cooperation to ensure a better protection of personal data. Finally, states are urged to develop an international treaty that clarifies responsibilities regarding the use of Artificial Intelligence and the Metaverse in the medical field, including aspects related to personal data protection. Governments should commit to incorporating this treaty into their national legislation.

Acknowledgements: The authors are thankful to Governance and Policy Design Research Lab (GPDRL) and Prince Sultan University for providing APC for this publication.

REFERENCES

Abdulai, A. F. (2025). Is Generative AI Increasing the Risk for Technology-Mediated Trauma Among Vulnerable Populations?. Nursing Inquiry, 32(1), e12686.

Adeyinka, K. I., & Adeyinka, T. I. (2025). Data Security. Navigating AI and the Metaverse in Scientific Research, 363.

Adil, M., Song, H., Khan, M. K., Mastorakis, S., Farouk, A., & Jin, Z. (2025). Metaverse in Health Care: Security Challenges and Pathways for Future Research. IEEE Systems, Man, and Cybernetics Magazine, 11(1), 95-106.

Aitana PA et al. (2025). Meta AI: German Court did not grant interim injunction. Final decision will be taken in main procedure. German DPAs issued urgency procedure. Noyb. Published: https://noyb.eu/en/meta-ai-german-court-did-not-grant-interim-injunction-final-decision-will-be-taken-main-procedure

Albakjaji, M., & Kasabi, M. (2021). The right to privacy from legal and ethical perspectives. Pt. 2 J. Legal Ethical & Regul. Isses, 24, 1.

Azis, M. A., Rahman, N., & Putri, R. A. K. (2025). Between the future or just utopia: a critical analysis of the legal personhood of artificial intelligence on the claim as a patent inventor. Critical Legal Review, 1(1), 56-81.

Ballell, T. (2025). Mapping Generative AI rules and liability scenarios in the AI Act, and in the proposed EU liability rules for AI liability. In Cambridge Forum on AI: Law and Governance (Vol. 1, p. e5). Cambridge University Press.

Bayaraa, B., Bataa, N., Baatar, O., Gankhuyag, D., & Damba, G. (2025). Jurisdictional Challenges in Metaverse. In Tech Fusion in Business and Society: Harnessing Big Data, IoT, and Sustainability in Business: Volume 2 (pp. 229-239). Cham: Springer Nature Switzerland.

Bouker, R. (2024). Recent Developments in the Concept of Protecting the Right to Privacy: A Study in Light of Latin and Anglo-Saxon Legislation. 628-619 ,(1)7. .Journal of economic and legal study

Burlacu, A., Brinza, C., & Horia, N. N. (2025). How the Metaverse Is Shaping the Future of Healthcare Communication: A Tool for Enhancement or a Barrier to Effective Interaction?. Cureus, 17(3).

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. Scandinavian studies in law, 56(8), 165-200.

Chaddad, A., & Jiang, Y. (2025). Integrating Technologies in the Metaverse for Enhanced Healthcare and Medical Education. IEEE Transactions on Learning Technologies.

Corfmat, M., Martineau, J. T., & Régis, C. (2025). High-reward, high-risk technologies? An ethical and legal account of AI development in healthcare. BMC Medical Ethics, 26(1), 4.

Del-Real, C., De Busser, E., & van den Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. International Review of Law, Computers & Technology, 1-32.

Department of Legal and Administrative Information. (2024). Obligations en matière de protection des données personnelles (RGPD). Published on : https://entreprendre.service-public.fr/vosdroits/F24270

Farouk, G., & Alsamara, T. (2023). Legal view on blockchain technologies in healthcare: A European states case study. International Journal of Sociotechnology and Knowledge Development (IJSKD), 15(1), 1-13.

Hassan, S., Dhali, M., Zaman, F., & Tanveer, M. (2021). Big data and predictive analytics in healthcare in Bangladesh: regulatory challenges. Heliyon, 7(6).

Jeong, E., & Lee, D. (2025). Metaverse applications in healthcare: opportunities and challenges. Service Business, 19(1), 4.

Joshi, H. (2025). AI and Chronic Diseases From Data Integration to Clinical Implementation. In Generative AI Techniques for Sustainability in Healthcare Security (pp. 17-40). IGI Global Scientific Publishing.

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. Policy and Society, 44(1), 85-97.

Lekadir, K., Frangi, A. F., Porras, A. R., Glocker, B., Cintas, C., Langlotz, C. P., ... & Starmans, M. P. (2025). FUTURE-AI: International consensus guideline for trustworthy and deployable artificial intelligence in healthcare. *bmj*, *388*.

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. IET Information Security, 2025(1), 5536763.

Marwa, R. (2025). Using the metaverse to train specialists and students to perform virtual surgeries, https://egyptiangeographic.com/ar/news/show/690

Meramria, B., & Bouadjila, N. (2024). The Intersection of Law and Technology in Environmental Protection in Algeria. Revue Académique de la Recherche Juridique, 15(1), 483-501.

Meskic, Z., Albakjaji, M., Omerovic, E., & Alhussein, H. (2022). Transnational consumer protection in E-commerce: Lessons learned from the European Union and the United States. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 13(1), 1-15.

Pasa, B., Bernes, A., Gaggioli, A., Tuccari, E., Zollo, F., Vulpiani, G., ... & Cerasa, A. (2025). LawVerse: the legal framework for clinical metaverse content. Journal of Medical Extended Reality, 2(1), 13-19.

Qin, Z., Wang, G., Deng, W., & Hao, Y. (2025). Electronic Commerce and Law. In Introduction to E-Commerce (pp. 377-434). Singapore: Springer Nature Singapore.

Sarabdeen, J., & Mohamed Ishak, M. M. (2025). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). International Journal of Law and

Management, 67(1), 99-119.

Shaik, D., & Poojasree, M. V. (2021, May). Consumer Protection in E-Commerce: A Legal and Compliance Framework in the Digital Market. In 1st International Conference on Law and Human Rights 2020 (ICLHR 2020) (pp. 18-23). Atlantis Press.

Solaiman, B., & Malik, A. (2025). Regulating algorithmic care in the European Union: evolving doctor–patient models through the Artificial Intelligence Act (AI-Act) and the liability directives. Medical law review, 33(1), fwae033.

Stalla-Bourdillon, S., & Knight, A. (2016). Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data. Wis. Int'l LJ, 34, 284.

Wallace, S. E., Gaye, A., Shoush, O., & Burton, P. R. (2014). Protecting personal data in epidemiological research: DataSHIELD and UK law. Public Health Genomics, 17(3), 149-157.

Warren, A. (2002). Right to privacy? The protection of personal data in UK public organisations. New Library World, 103(11/12), 446-456.

Wilhelm, C., Steckelberg, A., & Rebitschek, F. G. (2025). Benefits and harms associated with the use of AI-related algorithmic decision-making systems by healthcare professionals: a systematic review. *The Lancet Regional Health–Europe*, *48*.

Zahra, Y. (2025). Regulating AI in Legal Practice: Challenges and Opportunities. Journal of Computer Science Application and Engineering (JOSAPEN), 3(1), 10-15.

Zainab, H., Khan, A. R. A., Khan, M. I., & Arif, A. (2025). Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases. Global Trends in Science and Technology, 1(1), 63-74.