Vol. 05, No. 01, pp. 362-376 | june 2025
DOI: https:// DOI 10.34118/jskp.v5i01.4260

Article history (leave this part):
Submission date: 27-11-2024
Acceptance date: 24-05-2025
Available online: 30 - 06- 2025
Keywords:
Artificial Intelligence, Legal Regulation, Health Sector, Security Sector, Rights Protection
Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Competing interest:
The author(s) have declared that no **competing interests** exist.
Cite as (leave this part):
Ouafi , H. (2024). Artificial Intelligence and the Challenge of Protecting Personal Data in Light of European Directive EC/9/96 on the Legal Protection of Databases . Journal of Science and Knowledge Horizons, 4(01), 589-605. https://doi.org/10.34118/jskp.v4i01.3888

Journal of Science and Knowledge Horizons
ISSN 2800-1273-EISSN 2830-8379

The Legal Perspective on Artificial Intelligence in Health and Security Sectors between Innovation and Rights Protection

Dr. Tourkia Rebhi *, Civil status system laboratory, University of Khemis Miliana (Algeria)

dr.rebhi1996@gmail.com

https://orcid.org/0009-0001-5341-8991

Abstract:

Artificial intelligence has now become integral to both the security and healthcare industries, delivering revolutionary technologies for the purpose of improving service delivery and efficiency. With increased usage of AI come monumental legal hurdles, most notably privacy, responsibility, and protection of human rights. This presentation aims to analyze the legal framework that governs AI in the two industries crucial to society, examining the models of regulation attempting to balance technological advancements with safeguarding human rights. In the health sector, AI is revolutionizing patient care, right from diagnosis to treatment protocols, and raising eyebrows about the proper use of data, transparency of decision processes, and responsibility of AI enabled medical devices. And also, the security industry is faced with the dilemma of balancing AI's potential to enhance public safety while risking infringement upon personal freedoms, privacy, and civil liberties. This presentation analyzes existing legal frameworks, determines the differences between how AI is regulated in health and security, and compares their effectiveness at mitigating the risk and complexity posed by these technologies.

Vol. 05, No. 01, pp. 362-376 | june 2025
DOI: https:// DOI 10.34118/jskp.v5i01.4260

Résumé:

L'intelligence artificielle est désormais un pilier incontournable dans les secteurs de la santé et de la sécurité, en apportant des technologies innovantes destinées à améliorer l'efficacité et la qualité des services. Toutefois, son intégration massive soulève d'importants défis juridiques, notamment en matière de vie privée, de responsabilité et de respect des droits fondamentaux.

Dans le domaine de la santé, l'IA transforme les soins aux patients, du diagnostic aux protocoles thérapeutiques, tout en soulevant des questions critiques sur l'utilisation des données, la transparence des décisions automatisées et la responsabilité des dispositifs médicaux intelligents. Parallèlement, dans le secteur de la sécurité, l'IA promet un renforcement de la sûreté publique, mais engendre également des risques potentiels d'atteinte aux libertés individuelles, à la vie privée et aux droits civils. Cette présentation propose une analyse comparative des cadres juridiques encadrant l'IA dans ces deux domaines essentiels, en mettant en lumière les modèles de régulation adoptés, leurs différences, et leur efficacité dans la gestion des risques et des enjeux complexes posés par ces technologies

Mots-clés : *Intelligence artificielle, Réglementation juridique, Secteur de la santé, Secteur de la sécurité, Protection des droits*

*****Dr. Tourkia Rebhi*

I. Introduction:

Artificial intelligence technology is one of the most seen technological advancements of the twenty first century, significantly contributing to performance and efficiency improvement across many areas, particularly healthcare and security. But this rate of development raises profound legal and ethical concerns. While AI improves the ability of institutions to provide better services, it also raises fears regarding privacy, accountability, and its impact on the rights of individuals. The key issue is to design sound regulatory legal frameworks that allow for the safe and responsible use of this technology, especially in scenarios that directly impact individuals' well-being and health.

The issue in this case concerns achieving a balance between technological advancement and development on the one side and the preservation of individual and communal rights on the other side. This challenge involves an exhaustive consideration of how legal systems deal with the utilization of AI within these sectors, security, and health. **In what ways can legal systems respond to the issues raised by the increasing use of AI, including risks associated with algorithmic bias, use of personal data, and decisions with consequences for individuals' health and safety?** For example, while regulations such as the EU AI Act are focused on transparency and safeguarding the rights of users in the healthcare sector, those in the security sector are centered on data and societal protection from potential hazards. Therefore, the analysis of diverse legal frameworks and the revelation of discrepancies and congruences between the various fields are pivotal in establishing their efficiency in confronting current and future challenges. In this presentation, we compare legal frameworks for AI in security and healthcare, illustrating how each sector responds to challenges introduced by technology and evaluating how well these frameworks succeed in protecting people's rights and encouraging responsible use.

1 Analysis of the Legal Frameworks for Artificial Intelligence in Different Sectors

The adoption of artificial intelligence in diverse industries has ushered in revolutionary possibilities and enormous legal hurdles. As AI transforms fields such as healthcare and security, the law has to adapt to its consequences. This chapter discusses regulatory strategies used to manage AI, highlighting the specific requirements and dangers intrinsic to each field

1.1 The Health Sector

Due to the rapid development occurring within the global health care sector, there has been a great enthusiasm for the introduction of artificial intelligence technologies as an effective and novel tool in the sector. Such an introduction has been behind the reshaping of the nature of care that medical professionals provide to patients. Despite the continuous rise in the use of these advanced technologies, we have witnessed several cases where artificial intelligence has acted to enhance precision, effectiveness, and individualized care In introducing artificial intelligence into various roles within the healthcare industry, the aim is not only to create independent tools that can replace practicing physicians but also to provide tools that assist doctors in maximizing their processes to be as efficient as possible and to deliver individualized care to each patient.

Since the general shortage of physicians across the world, artificial intelligence has enabled processes to be accelerated and duties to be assigned to tools and platforms that utilize this technology, thus giving more time to medical practitioners to dedicate to their everyday tasks. The following are examples of how artificial intelligence is bringing about change in healthcare, since its use in medicine makes the work more effective and precise, and in many cases, adds a personal touch (How Artificial Intelligence is Transforming Healthcare,).

- Assistance in Diagnosis

Artificial intelligence is applied in the analysis of medical images, such as X-rays or MRIs, and these technologies are employed in the diagnosis of illnesses such as cancerous tumors, retinal diseases, and pneumonia, among others. Artificial intelligence technologies have also been employed in the diagnosis of heart diseases, where deep learning is employed to diagnose heart attacks in a way similar to that of cardiologists. In certain cases, artificial intelligence networks are instructed using clinical pictures to diagnose skin illnesses and classify skin lesions exactly. Artificial intelligence has been proven through experiments to be able to perform diagnostic work equivalent to or even superior to that of human experts, in addition to possessing better accuracy and speed (Pillai, 2023).

- Robotic-Assisted Surgery

Another novel application of medical artificial intelligence is its ability to support the provision of the correct surgical decisions before, during, and after surgical procedures. This is achieved through the aggregation of information from various data sources, such as research outcomes and surgical guidelines. In some instances, robotic surgical systems with artificial intelligence capabilities can help

surgeons perform operations more precisely. Besides that, robotic surgery advantages patients in numerous aspects, including shorter hospital stays, quicker recovery, and generally lower pain levels (p. p723)

1.2 AI in Healthcare: Key Statistics

This table highlights the transformative impact of artificial intelligence on the healthcare sector, focusing on diagnostic accuracy and robotic-assisted surgery (World Economic Forum, 2023) (Grand View Research, 2024)

Category	Statistic	Details
Diagnostic Accuracy	AI improves the accuracy of medical imaging diagnostics (e.g., X-rays, MRIs) by up to 95%.	This statistic reflects AI's contribution to accurate diagnostics in healthcare.
Robotic-Assisted Surgery	A 26% growth in robotic-assisted surgeries was recorded in 2023, driven by AI adoption in surgery.	Highlights the expanding use of AI-driven robotics in surgical procedures.
Efficiency in Diagnosis	AI reduces the time required for diagnostic imaging analysis by 20%-30%, improving early detection.	Emphasizes AI’s efficiency in speeding up diagnostic processes.
AI in Drug Discovery	AI reduces drug discovery time from 5-6 years to 1 year.	Demonstrates AI’s role in accelerating drug development.

Source: Compiled from World Economic Forum and Grand View Research reports

1.3 Legal Frameworks Regulating the Use of Artificial Intelligence in Healthcare

European Union Artificial Intelligence Act: This law, under Article 10, mandates risk evaluations for AI and transparency in applying it in the health sector. The act obligates healthcare AI companies to provide explanations regarding how they handle data and reports required for protecting users and patients. This law is all about highlighting the importance of transparency and accountability, with the mandate compelling organizations to implement good mechanisms to track AI technologies' performance and reliability and thus gain confidence in their application among their constituents (Gerke, 2023, p. 233).

U.S. Food and Drug Administration (FDA) Regulations: The FDA provides regulatory standards for devices and applications that use artificial intelligence in the healthcare sector. Article 3 (Health Risk Assessment) states that the new technologies must be safe and effective before approval for clinical use, but highlights the importance of continuous evaluation and monitoring after deployment so that the technologies continue to meet to standards of safety and efficacy. Prioritizing privacy and safety, the FDA ensures that AI applications do not interfere with patient confidentiality and health (p. 234).

General Data Protection Regulation (GDPR): Article 9 of this European Union legislation aims at protecting personal data in health apps. Article 9 puts strict limitations on the processing of sensitive data, including health data, and makes patient consent mandatory (Article 9, 2016), thus, their privacy is ensured. Not only does this article reconfirm organizations' obligation to ensure personal data is secured, but it also empowers patients' rights because they can decide how their information is used. Also, the GDPR sets large fines for non-compliance, hence encouraging healthcare organizations to prioritize data protection and ethical considerations when adopting AI technologies (Article 9)

While such regulatory systems provide necessary legal frameworks, they are by no means flawless. Among the main problems that continue to linger is the ethical dimension of deploying AI in medicine, a discipline that finds itself on a middle ground between law and ethics. Transparency, bias of algorithms, and explainability of AI decision are not invariably addressed through existing legislation. For example, a machine learning based diagnostic tool may be more precise than a physician, but if the decision process is opaque, both physicians and patients will have difficulty trusting or questioning its results. In addition, regulations lag behind technological progress, making it difficult for lawmakers to keep up with the rapid pace of development of AI capabilities. Even with strong frameworks like the GDPR or the FDA guidelines, enforcement can be spotty, especially in the case of cross-border digital health platforms. These lacunae reflect the need for more flexible, dynamic legal systems that align with ethical norms to ensure that AI is not only effective but also compatible with core human values of dignity, autonomy, and justice

1.4 The Security Sector

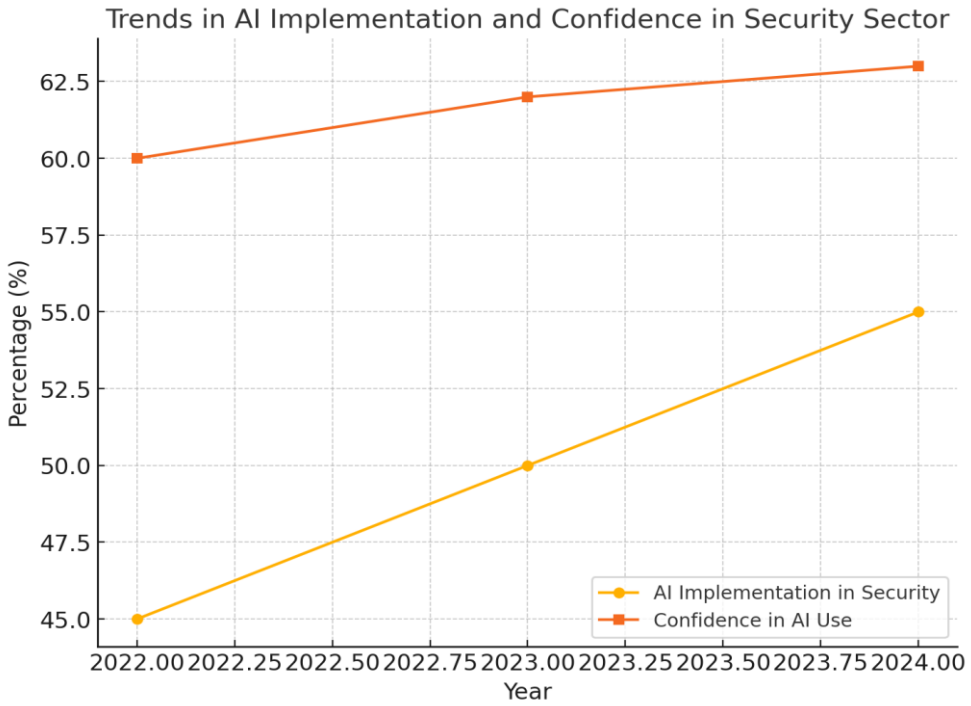
Artificial intelligence is one of the technologies that enables states to boost levels of security and devise new means of fending off increasing security threats. Modern security mechanisms greatly rely on AI to increase efficiency and

accuracy in decisions. AI makes it possible to rapidly and precisely process vast volumes of data, which enables authorities to identify potential threats before they are realized, examine behavior patterns, and predict security breaches (Rebhi, 2023).

The AI practical uses in the security industry are diverse because it is utilized in industries such as intelligent surveillance video, analysis of intelligence data, face recognition, and response systems. For instance, machine learning algorithms are used to process surveillance videos (Rebhi, p. Ibidem), facilitating illegal or suspicious behavior in public areas to be easier to detect. AI systems are also employed to aggregate information from various sources, such as social networks, allowing security agencies to get the overall picture and predict potential threats. These uses have posed numerous ethical and legal issues, such as privacy and human rights. The application of AI in security must ensure that there is a legal framework established that will handle the balance between security gains and the observance of the essential rights of individuals. Therefore, legal and regulatory frameworks appropriate to the same need to be developed due to the increasing utilization of the technology in public security operations (Nguyen, 2023).

The following chart illustrates trends in the implementation of Artificial Intelligence in the security sector and the growing confidence in its use from 2022 to 2024 (p. Ibidem). The data reflects percentages of organizations reporting active implementation of AI solutions and the confidence levels among security professionals.

AI Implementation and Confidence Trends in the Security Sector (p. Hypothetical data inspired by research trends from WEF and CSA)



Sources: Author's own work and data compiled based on various references

1.5 Legal Frameworks Governing the Use of Artificial Intelligence in Security

Within the framework of deploying artificial intelligence into security fields, the role played by legal institutions regulating the mode in which the technology is to be applied remains significant to ensure the protection of fundamental rights. Globally, the International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly in 1966 (Rebhi T. , 2024), forms the fundamental legal system for the establishment of human rights. For instance, Article 17 states that "no one shall be subjected to arbitrary or unlawful interference with his privacy." (The International Covenant on Civil and Political Rights, 1966) Any application of artificial intelligence technologies to public security surveillance must be per the regulations enshrined in this covenant, whereby whatever technology is used for surveillance must be an urgent need and proportionate to security targets (ouafi, 2024)

At the European level, the General Data Protection Regulation (GDPR), which became effective in 2018, is one of the strictest pieces of legislation for the safeguarding of personal data. Article 5 demands that personal data must be processed lawfully and in a fair manner regarding the rights of the individual. Article 6 makes it necessary to process personal data in the performance of a task carried out in the public interest or official authority. The suggestion is that

security agencies are supposed to use artificial intelligence technology under these laws, so they are spurred to take steps towards data transparency and accountability for collection and use (Walters, 2021). Nationally, many countries have enacted specialized legislation concerning the use of artificial intelligence for security. In the United States, for example, the Data Privacy Protection Act, enacted in 2018, mandates government agencies to examine the risks of employing artificial intelligence technologies. Article 3 of this law requires agencies to conduct serious assessments before taking up any new technology to ensure that the use of artificial intelligence does not violate people's fundamental rights (all, 2021).

The National Security Law of the United Kingdom, 2019, amended, has articles on the use of artificial intelligence for security surveillance operations. Article 10 envisages a complete impact analysis of the use of artificial intelligence in national security on how to safeguard the rights and liberties of individuals. Some Arab countries, such as the United Arab Emirates, have also legislated a legal framework for the use of artificial intelligence (Kingdom, 2019). In 2020, the government launched the UAE Artificial Intelligence Strategy, and it contains provisions that require adherence to privacy and protection of data in all artificial intelligence security applications. Article 8 of the strategy identifies the need to follow ethical principles when utilizing data (Pillai, p. 26).

2 Comparison of Legal Standards between Sectors and Their Consistency

The legal principles governing the use of artificial intelligence technologies in security and health have become central subjects of research in contemporary law. Both of these areas, although differing in their specific requirements and character, are united by their dependence on AI to enhance efficiency and decision-making in such vital fields as data protection and medicine. Despite sector-specific problems, there are vast spaces of convergence between the legal frameworks (p. 26), particularly concerning core principles such as privacy, transparency, and assurances of safety. But the establishment of elevated legal norms extending to such principles for both sectors is fraught with countless challenges. This section attempts to investigate areas of concordance between the legal systems of the security and health sectors and the obstacles toward attaining general legal concordance between the two fields.

2.1 Points of Agreement between Sectors

The standards of law in both the security and health sectors demonstrate certain points of commonality that reflect agreement about the cardinal principles under which artificial intelligence technologies are to be implemented. There is conclusive evidence that safety guarantees, privacy, and transparency are all cardinal attributes in either sector, as each of them entails adequate mechanisms for safeguarding personal information as well as information security.

Privacy: Law in both sectors recognizes the importance of protecting individual data. The General Data Protection Regulation (GDPR) law within the EU, adopted in 2018, for instance, outlines how to process data in a manner that protects privacy and maintains individuals' rights. Article 5 in the law identifies the "need to process data legally, fairly, and transparently" as a way of showcasing the importance of privacy in both health care and security.

Transparency: Legal standards in both industries require transparency in data collection and usage processes. In the security sector, the Personal Data Protection Act in the United States requires that individuals be informed about the use of their data. In contrast, in the health sector, U.S. Food and Drug Administration (FDA) rules highlight that information related to the use of artificial intelligence in healthcare needs to be disclosed, with the firms required to clarify how data is being processed. Both sectors require strong guarantees to make individuals and society safe. Legislation around National Security in most countries requires implementing security measures to protect information, whereas Public Health Laws center on the guarantee of the safety of medications employed, such as those supported by artificial intelligence technologies (Lupo, 2022).

2.2 Difficulties in Establishing a Coherent Legal Approach

Although there are several points of convergence between health and security legal requirements, the possibility of a fully harmonized legal framework for artificial intelligence is a remote one, due to a range of complex and overlapping problems. They include inconsistencies in national regulatory frameworks, data governance gaps, and growing concerns about individual rights, all of which have a direct impact on the reliability, safety, and ethical use of AI technologies in both sectors. AI regulations are fragmented or nonexistent in most countries, particularly in the security sector, leading to legal uncertainty and the absence of harmonized standards. Even in regions of the world with more developed regulatory systems, such as the United States and the European Union, there remains a balance to be struck between the impulse for technological

innovation and the imperative to protect fundamental rights and freedoms (Nguyen, p. 8). AI systems increasingly rely on the collection and analysis of enormous datasets, but the existing legal frameworks are often insufficient to address the complexity of modern data use. The shortfall is especially problematic where algorithms operate with minimal human intervention, raising questions of privacy, consent, and accountability. Also, the use of AI has introduced new threats to individual rights, including the threat of biased or discriminatory outcomes that can stem from prejudiced data sets or opaque decision algorithms. With a lack of definite legal rules and unmistakable concepts of liability, individuals who are adversely affected by such decisions have limited recourse (p. ibidem). Adding to the difficulty is the incongruence of national and global legal systems that creates hurdles for cross-border collaboration, particularly in domains like public health and national security, where synchronized action is essential. By way of example, divergent privacy standards between European and non-European states consistently hinder data sharing, rendering collaborative efforts to regulate and manage the use of AI in an effective and ethically sound manner more challenging. All of these factors contribute to a challenging legal environment that requires not only amendments to existing laws but also a reframing of how legal systems can themselves keep up with the pace of technological innovation in a manner that upholds human dignity and trust (p. Ibidem).

In Algeria, these universal challenges are also being aggravated by the lack of specific national legislation dedicated to regulating artificial intelligence. While the country has made significant advancements in the field of digital transformation and demonstrated interest in the adoption of emerging technologies, the legal system has not kept up with technological advancements. Current data protection laws remain limited in scope and are, in most instances, outdated, offering insufficient safeguards against the likely harms of AI systems, especially in high risk areas like security and healthcare. The absence of clear legal definitions, regulatory agency bodies, and enforceable ethical standards means that the use of AI in Algeria operates in a widely unregulated field. Such a void in the law not only leaves people open to violations of their rights, such as invasion of privacy or biased algorithmic decisions, but institutions too, because there are no systems of accountability. As well, Algeria's efforts in international cooperation regarding AI related matters are tainted with the incompatibility of its domestic legal system with international norms, particularly the European Union's General Data Protection Regulation; (Rebhi T. , 2025) which has evolved

into a benchmark for data protection and AI ethics. Closing this gap will require a complete transformation of law, institution-building, and a national strategy that aligns technological innovation with legal responsibility, transparency, and respect for human rights.

2.3 Legal Harmonization Opportunities

Even as the challenges to harmonizing legal standards across the security and health fields are significant, there are also possible chances of achieving more alignment and congruence in legal frameworks governing artificial intelligence. These chances include where there are shared principles that can be integrated to maximize legal coherence, allow cooperation, and reduce regulatory fragmentation (AllahRakha, 2023, p. 35).

One such opportunity to enhance consistency across industries is the development of universal legal frameworks that can be used extensively across different industries, both security and health. These frameworks would be able to make demands for transparency, data protection, and accountability consistent, thereby simplifying the process of moving through different regulations in each industry (AllahRakha, p. 36). For example, the implementation of broad rules such as the European Union's GDPR might serve as a model for the two sectors, offering uniform standards for data security and protection that might be used across a variety of circumstances. Another option is to encourage collaboration among the two industries to create shared ethical standards for the application of AI. Both the health and security industries have similar issues regarding bias, discrimination, and privacy concerns when using AI technologies (p. Ibidem). Through collaboration, the two industries' stakeholders, like legal experts, policymakers, and technology designers, can develop shared ethical standards that ensure responsible use of AI across industries. This collaborative framework can help resolve shared concerns while ensuring consistency in the regulation of such technologies. In addition to initiatives at the national level, international cooperation is at the heart of ensuring consistency of laws across industries. Governments, regulatory bodies, and international organizations can collaborate to create global standards for the regulation of AI that ensure a balance between innovation and the protection of rights (Rebhi T. , p. 108). By balancing regulative approaches in areas such as data protection, transparency, and accountability, countries can create a more standard and predictable legal environment for the application of AI. This balance would make cross-border cooperation more

effective, particularly in areas such as cyber security and international health programs, where AI applications are increasingly taking place.

II. Conclusion

In short, this study of the legal frameworks for artificial intelligence in healthcare and security industries confirms that even though AI can do a great deal to raise efficiency and service quality in the two sectors, its use in all spheres comes with such basic challenges. Such challenges relate fundamentally to safeguarding human rights, transparency in applying AI, and accountability in taking decisions. It becomes apparent that a strong legal framework is necessary to balance innovation with the protection of basic human rights, fostering trust, and making sure that AI technologies are utilized responsibly and ethically in such sensitive areas.

Suggestions:

- There should be continuous training of employees in the security and health industries on how to use AI. This includes learning to handle data in a secure way and learning about the risks associated with AI.
- Such states ought to promote international collaboration to tackle the challenges surrounding the regulation of AI. This is possible through developing worldwide platforms for experience and knowledge sharing and making global standards that facilitate the proper utilization of cutting edge technologies.
- There needs to be an establishment of ethical standards to guide the development and deployment of AI, such as a commitment to human values and respect for human rights.
- It is suggested to invest in research and studies to better grasp the influence of AI and explore the legal and ethical challenges associated with its use.

3 Bibliographie

all, d. A. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology, 3*(23), 505-525.

AllahRakha, N. (2023). AI and the law: Unraveling the complexities of regulatory frameworks in Europe. *International Bulletin of Young Scientist, 1*(2), 35.

Article 9. (2016). *of European Union legislation*.

Gerke, S. e. (2023). *Ethical and legal challenges of artificial intelligence-driven healthcare.* Academic Press.

Grand View Research. (2024). Consulté le Nov 2024, sur AI in Healthcare Market Size, Share & Growth Report, 2024-2030: www.grandviewresearch.com

How Artificial Intelligence is Transforming Healthcare,. (n.d.). Retrieved november 2024, from World Economic Forum: www.weforum.org.

Kingdom, T. N. (2019). Article 10 .

Lupo, G. (2022). The ethics of Artificial Intelligence: An analysis of ethical frameworks disciplining AI in justice and other contexts of application. *Oñati Socio-Legal Series, 3*(12), 620.

Nguyen, M. a. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *nternational Journal of Intelligent Automation and Computing*, *6*(5), 1-12.

ouafi, h. (2024). Artificial Intelligence and the Challenge of Protecting Personal Data in Light of European Directive EC996 on the Legal Protection of Databases. *Journal of Science and Knowledge Horizons, 4*(1), 595.

Pillai, A. (2023). Artificial Intelligence in Healthcare Systems of Low-and Middle-Income Countries: Requirements, Gaps, Challenges, and Potential Strategies. *International Journal of Applied Health Care Analytics*, *8*(3), p23.

Rebhi, T. &. (2023). Challenges and Prospects in Enforcing Legal Protection of Children from Online Sexual Exploitation. *Krytyka Prawa*, *4*(15), 21-33.

Rebhi, T. (2024). Rebhi, Tourkia. "INTERPOL'S GLOBAL EFFORTS TO COMBAT ORGANIZED CRIME. *revue critique de droit et sciences politiques, 1*(19), 99-111.

Rebhi, T. (2025). Combating Financial Corruption and Recovering Illicit Assets Combating Financial Corruption and Recovering Illicit Assets through Modern Technology. *Combating Financial Corruption and Recovering Illicit Assets.* University of Tissemsilt.

The International Covenant on Civil and Political Rights. (1966). Article17. the United Nations General.

Walters, R. a. (2021). Artificial intelligence and law." Cyber security, artificial intelligence, data protection & the law. *Singapore: Springer Singapore*, 39-69.

World Economic Forum. (2023). Retrieved novembre 2024, from How Artificial Intelligence is Transforming Healthcare: www.weforum.org