Cristian Dumitru Miheș*

Original Scientific Paper
DOI: 10.47152/ns2025.16

THE RIGHT TO HEALTH AND AI TECHNOLOGIES IN MEDICAL PRACTICE: ETHICAL AND MEDICAL DILEMMAS AND CRIMINAL IMPLICATIONS

The right to health ensures equitable access to safe and effective medical services, protecting patients' physical and mental integrity. Advanced technologies such as artificial intelligence, telemedicine, and surgical robotics offer faster diagnoses and personalized treatments. However, integrating these innovations raises issues around liability, data security, and the governance of automated decision-making. The main challenges stem from a lack of algorithmic transparency – which can produce hard-to-explain diagnostic errors – and from biases in training data that may lead to discriminatory care. Overreliance on automated systems and cybersecurity vulnerabilities further heighten the risk of unforeseen malfunctions and unauthorized access to sensitive information.

Criminal liability may fall on physicians, software developers, healthcare institutions, or malicious third parties. A doctor might face charges for bodily harm or involuntary manslaughter if they rely exclusively on flawed automated recommendations. Algorithm creators risk fines and other sanctions for failing to provide adequate warnings or for marketing non-compliant solutions.

Gathering evidence requires thorough auditing of IT systems, log analysis, and specialized expert evaluations. AI decision metadata and medical-device logs become crucial proof to determine the root cause of an error. Collaboration between investigators, cybersecurity specialists, and technology-law attorneys ensures accurate attribution of responsibility and the identification of compliance gaps.

In case law, incidents of robotic-assisted malpractice and software failures in monitoring devices have led to significant convictions and penalties. Hackers who illegally access medical records or sabotage smart

* Associate Professor, Faculty of Law, University of Oradea, Romania, email: cristian.mihes@uoradea.ro; ORCID: 0000-0003-4615-4737.

equipment are prosecuted for cybercrimes and extortion. These precedents highlight the necessity of clear regulations and rigorous enforcement.

To protect patients and mitigate criminal risk, it is recommended to establish an AI governance framework that includes periodic audits, human-in-the-loop protocols when errors are flagged, and full compliance with GDPR and healthcare legislation. Ongoing training for medical staff in the ethical use of technology and impact assessment further bolsters safety and transparency.

Keywords: *new technologies, medicine, legal implications, criminal law.*

***

1. The Right to Health in the Digital Age

1.1. The Right to Health. The Classification of the Right to Health in International Law

The right to health is a fundamental human right, (often misunderstood) indispensable for the exercise of other human rights and for living a life of dignity. As enshrined in international instruments such as Article 25.1 of the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights, this right place a three-tiered obligation on states: to respect, to protect, and to fulfil. The obligation to respect requires states to refrain from interfering with the right to health. The obligation to protect requires states to prevent third parties from interfering with it. The obligation to fulfil requires states to take proactive legislative, administrative, and judicial measures toward its full realization.

The international legal and ethical consensus does not frame it as a right to be healthy, an unattainable guarantee of a specific biological state. For example we have within our Constitution – "The right to healthcare" as regulated by the Romanian Constitution under article 34: "*Right to health care."*[1]

This critical distinction places a specific kind of burden on the state. It shifts the state's duty from ensuring an outcome to ensuring the conditions, systems, and policies necessary for individuals to pursue the highest possible level of health.

[1] Art. 34 Constitution of Romania: (1) The right to health care is guaranteed. (2) The state is obliged to take measures to ensure public hygiene and health. (3) The organization of medical care and the social insurance system for illness, accidents, maternity, and recovery, the control of the practice of medical professions and paramedical activities, as well as other measures for the protection of the physical and mental health of the person shall be established in accordance with the law.

A widely accepted, though sometimes debated, framework for classifying human rights is the "generational" theory. This framework places civil and political rights in the "first generation" and social, economic, and cultural rights in the "second generation" (Manual for Human Rights Education with Young people, (n.d.). First-generation rights where the most important is the right to life considered inviolable (Kostić, J., 2024: 222) and protected in various forms (Pavlović, Z., 2024: 201-220), and other rights such as freedom of speech or the right to vote, primarily impose a *negative obligation* on the state, meaning the government must refrain from infringing upon these liberties.

Conversely, second-generation rights, which include the right to education, social security, and, most importantly for this report, the right to health, impose a *positive obligation* on the state (Lindsey Reid, 2019). This requires the government to take active, tangible measures to create the conditions and infrastructure necessary for these rights to be fulfilled for all citizens. A state's failure to adequately regulate new medical technologies, ensuring their safety, efficacy, and equal access, could be interpreted as a failure to meet this positive obligation under international human rights law.

1.2. The Right to Health in the Romanian Legal Order

The Romanian legal system provides a robust foundation for the right to health, which is enshrined in the Constitution and further detailed in key pieces of legislation. Article 3 Law 46/2003 on patient rights, published in the Official Gazette of Romania no. 51 din 2003.01.29 states that "Patients have the right to the highest quality medical care that society can provide, in accordance with available human, financial, and material resources." Article 2 of this law explicitly states that patients have a right to medical care "of the highest quality available to society, in accordance with human, financial, and material resources" (Ibidem). This provision serves as a legal anchor for the integration of modern medical technologies, as it obligates the state and its healthcare providers to utilize the best available resources, which today increasingly includes AI and digital health platforms. The law also establishes a principle of non-discrimination, the right to information regarding proposed medical interventions (Art. 6), and the necessity of obtaining the patient's consent (Art. 13).

Complementing this, Law 95/2006 on health reform, published in the Official Gazette of Romania no. 652 din 2015.08.28, defines public health assistance as an "organized effort of society" to protect and promote the population's health, a definition that directly reflects the state's positive obligation under international law. In a forward-looking step, amendments to this law have begun to directly address the emergence of new medical technologies.

For instance, the law now defines and recognizes "personalized medicine," a data-intensive approach to care, as a patient right (Art. 36^2). It also establishes the legal framework for "telemedicine" (Art. 30^1), which includes services like teleconsultation, tele-expertise, and telemonitoring. A critical aspect of these new provisions is the requirement for informed consent and strict adherence to data protection and security measures for all services delivered via telemedicine (Art. 30^8 and Art. 30^9). These legislative updates demonstrate a legal evolution to accommodate technology, but as will be shown, they also introduce new complexities that are not fully resolved by the existing legal framework.

2. Legal and Ethical Challenges of Technological Integration

The advent of AI and telemedicine fundamentally redefines this obligation to "fulfil" the right to health (Januario, T.F.X. & Rodrigues, R.S., 2024:415). Traditionally, this duty involved the provision of physical infrastructure, such as hospitals and clinics, and ensuring a sufficient number of medical professionals. However, in the digital age, a state's responsibility extends to the digital layer that now underpins healthcare delivery. The effective use of telemedicine, for instance, is dependent on the availability of robust digital infrastructure, including broadband and mobile networks, as well as the widespread availability of digital hardware like computers and mobile phones. A state cannot fully realize the right to health if a significant portion of its population, particularly those in rural or underserved areas, is unable to access remote care due to poor connectivity or a lack of digital literacy. Consequently, the state's obligation evolves from merely providing physical healthcare resources to actively creating and maintaining a robust and equitable digital health ecosystem. This includes ensuring that new technologies are not just theoretically available, but are truly accessible and usable by all citizens, without discrimination.

The integration of digital technologies also introduces new complexities that challenge the very principles of non-discrimination and patient autonomy. The right to non-discrimination, a core component of the right to health, is threatened by implicit biases that can be inadvertently designed into technologies (Sun, N., Esom, K., Dhaliwal, M. & Dhaliwal, M. 2020:21-32). These biases can stem from non-representative training data or a lack of input from diverse socioeconomic and racial backgrounds during the development of AI systems. The result is that AI models may perform poorly for certain patient subgroups, thereby perpetuating and worsening existing health inequalities (Sun, N., Esom, K., Dhaliwal, M. & Dhaliwal, M. 2020:21-32). For a state to fulfil its duty to

protect against third-party interference, it must proactively address these algorithmic biases.

The patient-doctor relationship, a cornerstone of medical law and ethics, is also being fundamentally altered by this technological shift. The traditional model, where a patient orients themselves entirely to the doctor, is not fully applicable in the case of AI (Ungureanu, A.M., Matei, S.C. & Malita, D., 2025:230). This raises profound questions about trust, informed consent, and accountability. Patients now have a new set of imperatives that demand protection, including the right to an explanation for an AI-generated diagnosis or treatment plan, the right to contest an AI's output, and the right to withdraw from AI-supported care altogether (Ploug, T., Jørgensen, R.F., Motzfeldt, H.M., Ploug, N. & Holm, S., 2025). A patient cannot provide truly informed consent to a "black box" system whose internal workings are opaque (Ploug, T., Jørgensen, R.F., Motzfeldt, H.M., Ploug, N. & Holm, S., 2025). A new legal framework is therefore necessary to not only address technical liability but also to codify these new patient rights, thereby restoring trust and maintaining the integrity of the medical relationship in the digital era (Ploug, T., Jørgensen, R.F., Motzfeldt, H.M., Ploug, N. & Holm, S., 2025). Last, but not least, we must understand that certain categories of persons will not understand the mechanisms of new technologies, such as elderly people who often experience social exclusion (Stănilă, L., 2023: 112) or persons with certain disabilities (Onica-Chipea, L., 2019: 107-113).

2.1. Algorithmic Bias and Discriminatory Care

The introduction of AI into medical decision-making introduces the significant risk of algorithmic bias, which can lead to discriminatory care. AI systems are not inherently neutral; their outputs are a reflection of the data on which they were trained. If this historical data is not representative of the broader population – for example, if it is drawn predominantly from a specific gender, race, or socioeconomic group – the AI model may perpetuate or even amplify existing biases. This can lead to misdiagnoses, inadequate treatment recommendations, or unequal access to care for underrepresented populations.

In the Romanian legal context, this directly conflicts with the fundamental patient right to non-discrimination, as stipulated in Article 3 of Law 46/2003. The law defines discrimination as *"the distinction made between people in similar situations based on race, sex, age, ethnic origin, national or social origin, religion, political options or personal antipathy."*

An AI system that makes biased recommendations, whether intentionally or unintentionally, effectively creates a distinction in care based on these very factors. The legal challenge, therefore, lies in extending the concept of non-discrimination from a human-to-human interaction to a human-to-algorithm interaction. The current constitutional

framework prohibits a person from discriminating, but it does not explicitly address discrimination facilitated by an automated system. In this respect, we have Article 16 of Constitution of Romania – "Equality of Rights": *"(1) Citizens are equal before the law and public authorities, without privileges and without discrimination. (2) No one is above the law."* This gap suggests that new regulations are needed to hold the creators and operators of such systems accountable for their discriminatory outcomes.

2.2. The Black Box Problem – The Lack of Algorithmic Transparency and Explainability

Many advanced AI systems, particularly those based on deep learning, are notoriously opaque. Their internal decision-making process is so complex that it cannot be easily understood or explained by human experts. This is often referred to as the "black box problem."

On the other hand, in medicine, where clinical accountability is dominant, this lack of transparency presents a profound legal and ethical challenge.

According to medical malpractice principles, a physician has a professional duty to independently apply the standard of care. This duty requires them to critically evaluate any recommendations or information, including those from an AI system. If a physician relies exclusively on a flawed automated recommendation and it leads to patient harm, they could face criminal charges for bodily harm or involuntary manslaughter (Bodea, R. & Bodea, B., 2008: 41-49; Udroiu, M., 2024: 89-168), or civil charges of malpractice (Morozan, F., 2014: 208-2015).

However, without algorithmic transparency, it becomes nearly impossible for a doctor to understand *why* the AI made a certain recommendation, let alone to critically assess its validity.

This leaves a physician in a difficult position: if they cannot understand the reasoning behind an AI's output, they cannot fulfill their duty to question it, yet they may be held liable for its errors. This fundamental conflict creates a liability vacuum, making it difficult to attribute fault and potentially deterring the adoption of useful technologies.

2.3. Cybersecurity and Data Privacy Vulnerabilities

The large-scale deployment of AI and telemedicine systems requires the collection, storage, and processing of vast amounts of sensitive health data, making them high-value targets for cyber threats. These threats range from data breaches and unauthorized access to ransomware attacks and the deliberate sabotage of medical devices. The legal and ethical implications of these vulnerabilities are twofold, involving both individual

privacy rights and national security concerns (Mihăilă, C. O., Mihăilă, M., 2023: 189-222).

At the individual level, data privacy in the EU and Romania is governed by the GDPR and its national implementation law, Law 190/2018. This framework classifies health data as a "special category of personal data" subject to a higher level of protection. The law imposes stringent requirements for data processing, mandating specific technical and organizational measures to ensure confidentiality and security (Popescu, C., 2025). It also provides a legal basis for patient rights, such as the right to refuse automated decision-making and the right to seek compensation for damages caused by data breaches.

At the institutional and national level, the Romanian legal framework is also evolving to address these risks. Law 58/2023, regarding the cyber security and defense of Romania, as well as for the amendment and completion of certain normative acts published in the Official Gazette of Romania no. 214 din 2023.03.15, explicitly includes healthcare IT infrastructure as "critical information infrastructure of national interest". This designation elevates cybersecurity from a matter of individual data protection to a national security priority. Consequently, authorities are tasked with actively preventing and counteracting cyber incidents and attacks on these systems.

The interplay between these two legal domains means that healthcare providers face a dual responsibility: to protect individual patient data under GDPR and to secure national critical infrastructure under cybersecurity laws. A breach of these systems is no longer just a privacy violation; it is a threat to the functioning of the state's healthcare and defense networks.

3. The Framework of Legal Liability in Romania

3.1. Civil Liability for Malpractice (Title XVI of Law 95/2006)

The foundation of civil liability in Romanian medical law is laid out in Law 95/2006, regarding the reform in the field of health – Republication, published in the Official Gazette of Romania no. 652 din 2015.08.28, Title XVI Article 653 defines "malpraxis" as a professional error that causes prejudice to the patient, including errors resulting from "*negligence, imprudence, or insufficient medical knowledge*". This definition is broad and applies to all medical personnel. A critical challenge arises, however, when this definition is applied to new technologies.

Article 654 of the same law provides that medical personnel are not liable for damages caused by "hidden defects of medical materials, equipment and medical devices". This provision, intended for physical medical products, creates a complex legal challenge for AI.

The central question becomes: is a faulty AI algorithm a "hidden defect" of a medical device, or does a physician's reliance on its flawed recommendation constitute a professional error? If it is a hidden defect, liability would fall on the developer or manufacturer (Art. 657). If it is deemed a professional error, the physician is held liable under the theory of "insufficient medical knowledge" or "imprudence" for failing to identify and correct the AI's mistake. This legal ambiguity leaves a significant gap in the accountability chain. It creates a perverse incentive for physicians to be overly cautious in using new technologies, fearing liability for errors they cannot foresee or explain. For developers, it may lead to a reduced focus on creating transparent, explainable systems, as a lack of clarity could potentially obscure their liability.

3.2. Criminal Liability in Technology-Induced Harm

When technological errors result in (severe) patient harm or death, the question of criminal liability arises. The Romanian Penal Code contains provisions that could be applied in such cases. For instance, bodily harm ("vătămare corporală") and involuntary manslaughter ("omor din culpă") are defined and punished under Articles 194 and 195, respectively (Bodea, R. & Bodea, B., 2008: 41-49; Udroiu, M., 2024: 89-168). The core of these offenses is the element of negligence ("culpa") (Pătrăuș, M. 2025:. 106-117*;* Mirișan, V. & Domocoș, C, 2019: 151–164).

The complexity lies in proving negligence in a context involving AI, and from this complexity derive at least two questions: 1. Can a doctor be found criminally negligent for trusting a flawed automated recommendation, or for failing to anticipate a technological failure? 2. Can a software developer be held criminally liable for a design flaw or biased algorithm that results in a death?

The legal framework lacks a clear standard for what constitutes "due diligence" when interacting with an AI system. Proving the causal link between a specific algorithmic decision and a patient's death is a forensic and legal challenge that current laws are not equipped to handle.[13] This uncertainty makes criminal prosecution difficult and highlights the urgent need for a more specific legal framework that addresses the unique nature of AI-related harm.

3.3. Evidentiary Challenges and the Role of Digital Evidence

The investigation of malpractice cases involving AI and telemedicine fundamentally changes the nature of evidence. The traditional focus on physical evidence and personal testimony is shifting toward digital forensics (Miheș, C. & Alămoreanu, S., 2020: 200-204). Critical evidence now includes AI decision metadata, system logs, patient data

access logs, and network traffic records. The legal system must be prepared to handle these new forms of evidence.

The Romanian legal system has some existing mechanisms for technical expertise in a legal context, such as the judicial technical expertise ("expertiză tehnică judiciară"). However, the specific standards for the collection, preservation, and legal admissibility of digital evidence in medical cases are not yet formalized. The user query highlights the need for thorough auditing of IT systems and the importance of AI decision metadata and medical-device logs as crucial proof.

While Romania does have an official List of IT Auditors ("Lista auditorilor IT"), its application in medical malpractice investigations needs to be explicitly defined and standardized. Without clear rules on how this digital evidence is collected, verified, and presented in court, its legal value could be challenged, making it difficult to establish a clear chain of causation and hold the responsible parties accountable. This is one of the present important challenges of theory, law and practice.

3.4. The Role of the Commission for Monitoring and Professional Competence for Malpractice Cases

The Commission for Monitoring and Professional Competence in Malpractice Cases" ("Comisia de monitorizare și competență profesională pentru cazurile de malpraxis"), established by Law 95/2006 (Art. 679), is the primary body for investigating malpractice claims in Romania. Its composition includes representatives from medical colleges, the public health directorate, and medico-legal experts. This structure is designed for traditional medical errors, where the cause of harm can be determined by medical and forensic experts.

The inclusion of complex AI systems, however, challenges the commission's existing expertise. The commission, in its current form, may not have the technical knowledge to properly evaluate an AI algorithm's function or a system's cybersecurity vulnerabilities. The legal framework for this commission must be updated to explicitly grant it the authority to engage specialized technical experts, such as IT judicial experts, to analyze digital evidence and provide a technical report that can inform its final decision. Without this specialized expertise, the commission's ability to accurately attribute responsibility in cases involving advanced technology would be severely limited.

3.5. Comparative Regulatory Approaches in Key Jurisdictions – The European Union Approach: Risk, Regulation, and Rights

The EU has adopted a proactive and comprehensive strategy to regulate AI in all sectors, including healthcare. The EU AI Act, which entered into force in 2024, classifies AI systems based on their potential risk to fundamental rights and safety. AI systems used in medical devices are automatically designated as "high-risk" (Apostle, J. & Sharrow, D., 2024). This classification triggers a series of stringent obligations for both the developers and users of these systems. Key requirements for high-risk AI include a mandatory pre-market conformity assessment, rigorous data governance, comprehensive risk management, and the implementation of a "human-in-the-loop" protocol to ensure human oversight (de Lacy-Brown, N. 2024).

This regulatory approach is layered on top of the already robust data privacy framework established by article 4 from the General Data Protection Regulation (GDPR), which imposes strict rules on the processing of sensitive health data and automated decision-making. The GDPR requires explicit patient consent for using health data for profiling or automated decisions. Furthermore, the Network and Information Systems 2 (NIS2) Directive, which came into force in 2024, designates the health sector as critical infrastructure and imposes enhanced cybersecurity obligations (Food and Drug Administration, USA. (n.d.). This creates a comprehensive, harmonized framework that addresses AI from multiple perspectives: safety, data privacy, and cybersecurity.

The EU's philosophy is to anticipate and mitigate risks before they can cause harm, balancing innovation with the protection of fundamental rights. However, there (were) are opinions that criticize the EU approach to this matter(s), stating that it is a legal barrier towards technical progress, and in time, it will increase the distance between EU and other competitors as regarding the integration of technology with the consequences of losing the efficiency as regarding the medical act – also in medical field.

3.6. Comparative Regulatory Approaches in Key Jurisdictions – The United States Approach: Market-Driven and Tort-Based

In contrast to the EU, the United States lacks a single, overarching federal law for AI regulation in healthcare. Instead, its approach is more fragmented, relying on existing regulatory bodies and legal doctrines.

The Food and Drug Administration (FDA) regulates AI as a type of medical device, particularly as "Software as a Medical Device" (SaMD) (Food and Drug Administration, USA. (n.d.). The FDA's regulatory paradigm was not designed for adaptive AI, but it is attempting to adapt by publishing guidance and using its existing pre-market review pathways. This has resulted in a case-by-case, reactive regulatory system. (Food

and Drug Administration, USA. (n.d.)). Patient data privacy is primarily governed by the Health Insurance Portability and Accountability Act (HIPAA), which establishes standards for handling Protected Health Information (PHI) (Food and Drug Administration, USA. (n.d.)). AI developers and healthcare providers must be HIPAA-compliant, often through complex contracts known as Business Associate Agreements (BAAs) (HHS. (n.d.). *Telehealth policy*). A key challenge in the US system is the fragmented regulatory landscape for telemedicine, with licensure requirements varying at the state and cross-state levels (G, Maliha., Gerke, S., Cohen, I.G. & Parikh, R.B. 2021: 629-647).

Liability for AI-related harm is largely addressed through tort law. Physicians remain the primary point of accountability under medical malpractice theories (Kay, C. 2025). Courts and legal analysts suggest that a physician who relies on a faulty AI recommendation may still be held liable for failing to independently apply the professional "standard of care" (Maliha G, Gerke S, Cohen IG, Parikh RB., 2021). This "human-in-the-loop" model places a heavy burden on the individual clinician. For AI developers, liability may be pursued under products liability law, but this area is considered legally "unsettled" (Maliha G, Gerke S, Cohen IG, Parikh RB., 2021).

The US model prioritizes market innovation and relies on existing legal systems to resolve disputes, with liability as a key mechanism for encouraging safe practices.

3.7. Comparative Regulatory Approaches in Key Jurisdictions – The China Approach: State-Led and Pro-Innovation

China's approach to AI in healthcare is characterized by a strong state-led agenda that balances a fervent push for technological advancement with a top-down system of control and accountability. National policies, such as the "Healthy China 2030" blueprint, actively encourage the integration of AI to enhance efficiency and reduce costs (Healthy China 2030 (from vision to action).

The regulatory framework is primarily driven by the National Medical Products Administration (NMPA). AI-based medical software is regulated as a medical device, and the classification is tiered based on its "software security level" – mild, moderate, or severe (Li, B., 2025). This approach allows regulators to apply more stringent requirements, including technical evaluations, system inspections, and adverse event monitoring, to higher-risk applications. A core principle of the Chinese regulatory philosophy is the preservation of human oversight; regulations explicitly state that AI is an "assistive tool" and is "not permitted to replace doctors in the delivery of medical diagnosis and treatment services" (For further details please see: Jia, J. & Zhao, S., 2025). Data protection is governed by a comprehensive legal framework, including the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL) (Liao, T.,

Lui, B. & NG, G., 2022). Healthcare data is classified as "sensitive personal information" and requires explicit and separate consent for processing and cross-border transfers. The government also mandates ethics reviews for AI projects that could affect public health and safety (Liao, T., Lui, B. & NG, G., 2022).

In terms of liability, the regulations reinforce the role of the human professional, expecting medical institutions to establish robust internal oversight and placing ultimate responsibility on the licensed healthcare provider (United Nations Development Programme, (n.d.)). China's strategy reflects a centralized, pragmatic effort to leverage technology for public welfare and national interest, while maintaining strong state control over data and accountability.

4. De Lege Ferenda: Legislative and Policy Recommendations for Romania

The analysis of the Romanian legal framework and a comparison with international jurisdictions highlights a clear need for legislative reform to effectively govern the new era of technological healthcare. The following recommendations, proposed *de lege ferenda*, are designed to fill existing gaps, provide legal certainty, and protect patient rights in an increasingly digital medical landscape.

4.1. Establish a National AI Governance Framework for Healthcare

Romania should establish a specialized legal and institutional framework for the governance of AI in healthcare. This could be achieved by creating a new, dedicated agency or by empowering a body like the National Agency for Medicines and Medical Devices (ANMDMR) to oversee the entire lifecycle of AI-driven medical technologies. This framework should adopt a risk-based approach, similar to the EU AI Act, where AI systems are classified based on their potential to cause harm. High-risk systems, such as those used for diagnosis or treatment recommendations, would be subject to stringent pre-market conformity assessments, continuous monitoring, and mandatory human-in-the-loop protocols. This approach would move Romania from a fragmented, reactive legal system to a cohesive, proactive one, ensuring alignment with European standards while addressing unique national needs.

4.2. Codify Legal Liability for AI-Induced Harm

The current legal framework in Law 95/2006 creates ambiguity regarding liability for AI-related harm. The law should be amended to clearly delineate the chain of responsibility. Specifically, the law should distinguish between liability for software defects and negligent use. A software defect, such as a programming error or a biased algorithm, should be considered a form of hidden defect ("viciu ascuns") for which the developer or manufacturer bears civil liability.

Negligent use, on the other hand, would be a professional error on the part of the physician who fails to exercise due professional judgment, over-relies on the AI, or uses it for purposes beyond its validated scope. This clarification would protect diligent medical professionals while incentivizing developers to create safer and more transparent systems, thereby fostering a more accountable technological ecosystem.

4.3. Strengthen Digital Forensic Standards and Expertise

To address the evidentiary challenges in malpractice cases involving technology, Romania must formalize standards for digital forensics. The law should mandate that healthcare providers using AI systems maintain secure, auditable, and unalterable logs of all system interactions. These logs should include AI decision metadata, patient data access records, and timestamps. Furthermore, The Commission for Monitoring and Professional Competence for Malpractice Cases should be granted the explicit authority to call upon certified IT judicial experts and to compel the production of this digital evidence. This would ensure that malpractice investigations can effectively navigate the complexities of digital evidence, leading to more accurate and just attribution of responsibility. Without these standards, proving causation in a technology-driven medical error will remain a significant challenge.

4.4. Mandate Human-in-the-Loop Protocols and Continuous Training

A key lesson from comparative international approaches is the importance of human oversight. Regulations should mandate human-in-the-loop protocols for all high-risk AI systems in healthcare, ensuring that a human professional is always involved in the final decision-making process.

This should be supported by a requirement for continuous training for medical staff on the ethical and practical use of AI. This training should cover how to recognize and mitigate algorithmic bias, understand the limitations of AI systems, and correctly interpret and validate their outputs.

This dual approach reinforces the professional responsibility of the physician while equipping them with the necessary tools and knowledge to fulfill that responsibility in a technologically advanced environment.

6. Conclusion

The rapid integration of advanced technologies like artificial intelligence (AI) and telemedicine into healthcare is outpacing existing legal and ethical frameworks, calling into question how we protect a foundational human right: the right to health. Traditionally conceived as a socio-economic right requiring active state intervention, the right to health is now being reshaped by innovations that promise faster diagnoses, personalized treatments, and wider access while introducing novel risks. Romania has made initial strides – recognizing telemedicine services and exploring personalized medicine – but critical gaps persist, especially around liability for AI-driven errors, algorithmic bias, and the admissibility of digital evidence in court.

A comparative overview highlights three distinct regulatory philosophies. The European Union's approach, embodied in the forthcoming AI Act and its General Data Protection Regulation (GDPR), adopts a risk-based, rights-centric model that seeks to prevent harm through advance oversight. The United States leans on a reactive, market-driven system that treats emerging technologies as extensions of existing medical tools and emphasizes tort liability for practitioners. Meanwhile, China pursues a state-led, top-down strategy that balances rapid innovation with a tiered regulatory scheme and strict government oversight, reinforcing accountability at every stage of development and deployment.

To bridge these gaps in Romania, this report proposes targeted legislative and policy reforms. First, establish a dedicated national AI governance framework for healthcare that integrates ethical guidelines, certification processes, and enforcement powers. Second, clarify civil and criminal liability by defining the responsibilities of software developers, medical professionals, and healthcare institutions when technology causes harm. Third, formalize standards for digital forensics to ensure that algorithmic decisions and data trails can be reliably examined in legal proceedings. Finally, mandate "human-in-the-loop" protocols and invest in continuous professional training so that practitioners remain adept at interpreting and overseeing AI outputs.

Embracing AI and telemedicine offers an unprecedented opportunity to strengthen healthcare delivery in Romania. Yet without a robust, rights-based legal framework, the promise of better outcomes risks being undermined by new forms of injustice

– ranging from data misuse to algorithmic discrimination. By adopting a balanced regulatory model that draws on best practices from the EU, the US, and China, Romania can safeguard the right to health while fostering innovation. The moment for decisive action is now: only through comprehensive legal and policy reform can we ensure that technology enhances care, preserves patient trust, and upholds the fundamental rights of every individual.

References

Bodea, R. & Bodea, B. (2018). *Drept penal special (Criminal Law Special Part)*. pp. 41-49, București: Editura Hamangiu.

Januario, T.F.X. & Rodrigues, R.S. (2024). Artificial Intelligence and Medically Assisted procreation: An analysis of Preimplantation Genetic Testing (pgt) in the Light of Brazilian Criminal law. In: Z. Pavlović, & I. Stevanović (eds.) *The right to life and body integrity*. Belgrade.

Kostić, J. (2024). Obligations of institutions regarding the protection of the right to life. In: Z. Pavlović & I. Stevanović (eds.) *The right to life and body integrity*. Belgrade.

Miheș, C. & Alămoreanu, S. (2020). Pledoarie pentru Criminalistica, in Miheș, C. (editor) – *"In Honorem Valentin Mirișan"*. pp. 200-204. Bucharest: Universul juridic Publishing House.

Mirișan, V. & Domocoș, C. (2021). *Drept penal general (General Criminal Law),* pp. 151-164. Bucharest: Universul Juridic Publishing House.

Morozan, F. (2014). *Drept civil. Introducere în Drept civil*. (*Civil Law. Introduction in Civil Law).* Oradea: University of Oradea Publishing House.

Pavlović, Z. (2024). Multiple Homicide and The Public Perception. In: Z. Pavlović & I. Stevanović (eds.) *The right to life and body integrity*. Belgrade, p. 201-220

Stănilă, L., (2023) The Status of the Elderly Convicts in the Criminal Justice system of Romania in Zoran Pavlović (editor), *Elderly People and Discrimination: Prevention and Reaction*, Belgrade – Novi Sad, 2023

Udroiu, M. (2024). *Sinteze de Drept penal, Partea special (Syntheses of Criminal Law, Special Part),* 5th Edition, 1st volume. pp. 89-169. Bucharest: C.H. Beck. Publishing House

Online sources

Apostle, J. & Sharrow, D. (2024). *The EU AI Act: What Life Sciences and Digital Health Companies Should Know*. Available at: https://www.orrick.com/en/Insights/2024/09/The-EU-AI-Act-What-Life-Sciences-and-Digital-Health-Companies-Should-Know (Accessed: 8 September 2025).

de Lacy-Brown, N. (2024). *NIS2 Series, Part 1 – Key features of the EU's new cybersecurity law and how it will apply to the life sciences sector | DLA Piper*. Available at:

https://www.dlapiper.com/insights/blogs/cortex-life-sciences-insights/2024/nis2-series-part-1 (Accessed: 8 September 2025).

Food and Drug Administration, USA. (n.d.). *Artificial Intelligence in Software as a Medical Device – FDA*. Available at: https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device (Accessed: 8 September 2025).

G., Maliha., Gerke, S., Cohen, I.G. & Parikh, R.B. (2021). Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation. *Milbank Q*, 99(3), pp. 629-647. Available at: https://doi.org/10.1111/1468-0009.12504.

HHS. (n.d.). *Telehealth policy*. Available at: https://telehealth.hhs.gov/providers/telehealth-policy (Accessed: 8 September 2025).

Jia, J. & Zhao, S. (2025). Ethical and Legal Governance of Generative AI in Chinese Healthcare. *Journal of multidisciplinary healthcare*, 18, pp. 5405–5419. Available at: https://doi.org/10.2147/JMDH.S541271.

Kay, C. (2025). *Examining the Evolving Landscape of Medical AI*. Available at: https://www.theregreview.org/2025/09/07/spotlight-examining-the-evolving-landscape-of-medical-ai/ (Accessed: 8 September 2025).

Li, B. (2025). *China releases 'AI Plus' plan, rolls out AI labeling law*. Available at: https://iapp.org/news/a/china-releases-ai-plus-plan-rolls-out-ai-labeling-law (Accessed: 8 September 2025).

Liao, T., Lui, B. & NG, G. (2022). *China's Data Privacy Laws and Implications for Healthcare Industry*. Available at: https://www.morganlewis.com/pubs/2022/07/china-data-privacy-laws-and-implications-for-healthcare-industry (Accessed: 8 September 2025).

Mihăilă, C. O., Mihăilă, M., (2023) Video surveillance and Artificial Intelligence: How does it affect privacy and intellectual property rights? – (62)100, Zbornik radova Pravnog fakulteta u Nišu, 2023, pp. 189-222. Available at: https://scindeks.ceon.rs/article.aspx?artid=0350-85012300189O&lang=en (Accessed: 12 September 2025)

Onica-Chipea, L., (2019) Theoretical And Practical Aspects Of The Amendments To Law No. 448/2006 On The Protection And Promotion Of The Rights Of Persons With Disabilities By Emergency Ordinance No. 69/2018. (*2)2019. Fiat Justitia Review*, pp. 107-113.

Pătrăuș, M. (2024). The Criminal Offense – Constitutional Challenges and Controversies. (2)2024, pp.16-117. *Journal of Faculty of Law Oradea,*

Ploug, T., Jørgensen, R.F., Motzfeldt, H.M., Ploug, N. & Holm, S. (2025). The need for patient rights in AI-driven healthcare – risk-based regulation is not enough. *Journal of the Royal Society of Medicine*, 1410768251344707. Available at: https://doi.org/10.1177/01410768251344707.

Popescu, C. (2025). *Data protection and cybersecurity laws in Romania – CMS Expert Guide*. Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/romania (Accessed: 8 September 2025).

Reid, L., (2019). *The Generations of Human Rights*. The University of Alabama at Birmingham Available at: https://sites.uab.edu/humanrights/2019/01/14/the-generations-of-human-rights/ (Accessed: 8 September 2025).

Sun, N., Esom, K., Dhaliwal, M. & Dhaliwal, M. (2020). Human Rights and Digital Health Technologies. *Health and Human Rights Journal*, 22(2), pp. 21-32.

Ungureanu, A.M., Matei, S.C. & Malita, D. (2025). Controversies in the Application of AI in Radiology-Is There Medico-Legal Support? Aspects from Romanian Practice. *Diagnostics (Basel, Switzerland)*, 15(2), 230. Available at: https://doi.org/10.3390/diagnostics15020230.

United Nations Development Programme. (n.d.). *Respect for human rights in the provision of Pre-Hospital Emergency Medical Services in the Republic of Moldova*. Available at: https://www.undp.org/ro/moldova/publications/respectarea-drepturilor-omului-prestarea-serviciilor-de-asistenta-medicala-urgenta-prespitaliceasca-din-republica-moldova (Accessed: 8 September 2025).

Legal sources

Law 46/2003 on patient rights, published in the Official Gazette of Romania no. 51 din 2003.01.29.

Law 95/2006 on health reform, published in the Official Gazette of Romania no. 652 din 2015.08.28

Law 286/2009, Criminal Code of Romania in the Official Gazette of Romania no. 510 din 2009.07.24.