Mario Caterini[*]
Marianna Rocca[**]

Original Scientific Paper
DOI: 10.47152/ns2025.14

THE CRIMINAL LIABILITY OF THE PHYSICIAN IN THE AGE OF ARTIFICIAL INTELLIGENCE: BETWEEN ALGORITHMIC AUTONOMY AND THE DUTY OF CARE

The advent of artificial intelligence in the healthcare sector necessitates a renewed reflection on the criminal liability of the physician. This contribution analyzes the impact of the use of intelligent systems in diagnostic and therapeutic activities, with particular attention to the limitations in assessing negligence in the presence of autonomous and opaque technologies (black box medicine). The traditional criteria for the imputation of liability are examined in light of Art. 590-sexies of the Italian Criminal Code, as well as the repercussions on the duty of care and the principle of reliance. The profiles of liability of the actors involved in the adoption of artificial intelligence in healthcare are also explored, highlighting the issues related to the so-called responsibility gap. From a de jure condendo perspective, a cooperative human-machine model is proposed, and the need for specific regulatory protocols is emphasized, aimed at ensuring algorithmic transparency, patient safety, and the protection of fundamental rights.

Keywords: *health; e-health, artificial intelligence; AI; legal medicine; medical liability.*

[*] University of Calabria, Full Professor and Director of the Institute of Criminal Law Studies "Alimena" (www.ispa.unical.it), email: mario.caterini@unical.it, ORCID: 0000-0002-8766-9908.

[**] University of Calabria, Honorary fellow in Criminal Law,
email: mariannarocca1997@gmail.com

1. The advent of artificial intelligence in medicine and the challenge to the criminal liability of the physician

Artificial intelligence (AI) is one of the most disruptive technological innovations of our time, capable of radically redefining production processes and human interactions, marking an epochal evolution comparable to the advent of the steam engine or electricity. Its ability to operate autonomously and interact with its surroundings without direct human control has generated a progressive shift from automation to autonomy, with profound and all-encompassing implications for every branch of the legal system. The law, as a social and human science, cannot avoid confronting the challenges posed by this "fourth industrial revolution".

The medical-healthcare sector, in particular, has undergone a true "Copernican revolution," defined as Healthcare 2.0 or *e-Health*. This transformation is not limited to a simple modernization of existing practices, but introduces a new epistemology of medical knowledge, based on the development of innovative care paradigms. Such paradigms are made possible by the availability of a growing mass of data (so-called big data), originating from heterogeneous sources such as electronic health records, scientific literature, clinical trials, pharmaceutical registries, smartphones, and wearable devices (Colaruotolo, 2022: 300). The use of AI in medicine is destined for exponential expansion, driven by population growth, increasing demand for medical assistance, staff shortages, and the high costs of care. Already today, a significant part of the healthcare industry, especially overseas, makes extensive use of forms of AI.

However, the integration of AI in the medical field raises a plurality of ethical, political, and socio-economic questions and critical issues, with clear legal repercussions. One of the most salient problems is the intrinsic opacity of algorithms and AI systems, often described as black box medicine. This opacity makes it extremely difficult, if not impossible, for the human operator to understand the logical path underlying the decisions and recommendations provided by the AI (Salvadori, 2021: 89). The era of *diagnosis by software* imposes a dual challenge on the jurist: on the one hand, to establish whether these new technologies should be considered mere products or whether they can be granted some form of legal personality (the so-called "electronic personhood") (Hajdú, 2020: 589); on the other, to identify a criterion for imputing liability in the event of harmful events.

The introduction of artificial intelligence and robotics in the healthcare context accentuates the complexity of the doctor-patient relationship, traditionally founded on trust (Amore, Rossero, 2024: 76-77). In the absence of clear regulation – despite Bill No. 1146 on artificial intelligence ("AI Bill"), aimed at harmonizing Italian national

legislation with the European Regulation 1689/2024 ("AI Act") (Romano, 2024: 410) – such innovations risk undermining citizen trust in the healthcare system, and the diffusion of intelligent systems may be compromised.

The "promise" of medical AI is to reduce errors, but not to eliminate them entirely, as harmful events are inevitably destined to occur even with the use of emerging technologies. The challenge for the interpreter is, therefore, to understand the various forms of civil and criminal liability for the use of intelligent systems in healthcare among the various actors involved: the physician, the healthcare facility, and the manufacturer of the medical device. This contribution analyzes the impact of artificial intelligence on the criminal liability of the physician, with particular reference to its use in diagnostic, therapeutic, and surgical fields. The investigation focuses on the critical issues of traditional models of imputation and on emerging perspectives, highlighting the need to balance technological innovation with the protection of fundamental rights.

2. Artificial intelligence as a medical tool: typologies, functioning, and levels of autonomy

Artificial intelligence has found wide and fruitful application in the medical sector, where clinical, rehabilitative, and assistive robotics have contributed to improving the quality and safety level of healthcare services. To fully understand the resulting liability profiles, it is essential to outline the different ways AI is used in medicine, distinguishing between its various forms and levels of autonomy.

The applications of AI in medicine can be classified into three main macro-areas (Lagioia, 2020: 22-42).

- **Clinical robotics.** This category includes the use of robotic systems and AI techniques that directly support "care" and "care processes". It includes applications in diagnosis, treatment, surgical and pharmacological interventions, as well as in emergency healthcare. These systems are generally managed by qualified clinical personnel.
    - Diagnostics*:* AI is particularly advanced in this phase. As early as the 1970s, expert systems like *Mycin* were able to identify bacteria and suggest pharmacological treatments. Today, robotic micro-systems such as *smart medical capsules* (endoscopic microcapsules with cameras for diagnosing intestinal pathologies) and nano-robotics (miniature diagnostic devices injectable into the bloodstream) are used for increasingly precise diagnoses. Advanced neural networks such as IBM's *Watson for Oncology* and Google's *DeepMind* are used to interpret radiological or histopathological findings, diagnose neoplastic

forms with accuracy equal to or greater than that of specialists, and support clinical decisions. These systems process extraordinary volumes of data (clinical records, scientific literature, clinical studies) to provide predictions and recommendations based on statistical analyses. Even in complex fields such as in vitro fertilization, AI has found application in embryo selection: by analyzing static and moving images, artificial intelligence extracts specific characteristics of the embryos and, through advanced neural network models, classifies them based on genetic quality, thus guiding clinical choices towards an optimal outcome (Januario, Rodrigues, 2024: 420).

  - Robotic surgery*:* automated technologies have made it possible to develop less invasive surgical practices, with clear advantages for the patient (less pain, reduced complications, lower risk of bleeding and infections, shorter hospital stays). Examples include the PUMA 560 system for brain biopsies, the NeuroArm robot to limit operator tremors, and ROBODOC for hip and knee surgery. The most famous is the *Da Vinci Surgical System*, an advanced robot for minimally invasive surgery, controlled by a surgeon who manipulates mechanical arms from an external console, eliminating tremor and allowing for precision movements (e.g., 360-degree rotations). Telesurgery, which allows for remote interventions, represents a further application (Torres, Maynes, 2025: 25-27).

- **Rehabilitative and prosthetic robotics.** This area is crucial in the treatment of physical and cognitive disabilities, with applications both in specialized facilities and in the home setting. Examples include robotic exoskeletons like Lokomat for recovering lower limb mobility and "intelligent prostheses" that recognize the patient's intentional movements. Robots like PARO (a robotic seal) are used to interact with elderly patients with dementia or autistic children, reducing anxiety and agitation (Chen, 2023: 653).
- **Assistive robotics.** This includes automated systems that perform routine nursing tasks, such as monitoring vital signs, patient hygiene, or wound dressing. These robots were particularly useful during the SARS-CoV-2 emergency, lightening the workload of healthcare personnel and limiting contact with contagious patients (Baldassare, Sasanelli, 2021: 14-28).

It is essential to distinguish between AI systems based on different levels of autonomy. At present, medical robotics is almost always incapable of treating patients without the direct intervention of human operators. Most healthcare technologies fall into the

category of weak AI or artificial narrow *intelligence*, designed for specific tasks and requiring human supervision. The physician, in this context, acts as an intermediary of the technology, maintaining a central role in medical practice. The model of "independent" artificial intelligence remains largely hypothetical, whereas the "auxiliary" model is well-established and divided into two subcategories: technical support AI and intellectual support AI. The former are tools designed to enhance the physician's executive capabilities, comparable to any traditional medical device. The latter, by contrast, are characterized by a significant degree of decision-making autonomy, assisting the physician in diagnostic reasoning and the formulation of therapeutic solutions. In this context, the physician is called upon not only to use the technology but also to exercise rigorous critical judgment over the generated outputs. Criminal liability in such cases proves to be more complex (Amore et al., 2024: 3-4). However, there are also cognitive robots capable of self-learning and continuous evolution, whose behavior is not always predictable. This unpredictability, combined with black box medicine (the inability to understand the "why" or "how" of the AI's conclusions), raises problems of transparency and verifiability.

The European Commission, through its High-Level Expert Group on Artificial Intelligence, has proposed dividing the concept of AI into two groups: AI as a system (software or hardware that acts in a physical or digital environment, perceiving the environment and choosing the best decision) and AI as a scientific discipline (which includes techniques such as machine learning, automated reasoning, and robotics). A further distinction is between deterministic robots (pre-programmed for specific tasks) and cognitive robots (capable of self-learning and making choices not foreseen by programmers). This distinction is crucial: while deterministic robots have predictable behavior, cognitive robots can modify their algorithms based on experience, making their behavior not perfectly predictable (Januario, Rodrigues, 2024: 369).

The critical point is that, with the development of AI and autonomous artificial systems, the operator no longer has entirely safe means to predict the behavior of these new entities. Society thus finds itself in the uncomfortable position of having to choose whether to forgo the use of highly advanced technologies or to find solutions to bridge this "responsibility gap".

3. The criminal liability of the physician in the use of AI systems: the model of negligence, the *lex artis*, and the limits of black box medicine

The criminal liability of a physician in Italy is primarily governed by Arts. 589 (involuntary manslaughter) and 590 (negligent personal injury) of the Criminal Code,

with particular reference to Art. 590-sexies c.p., introduced by Law No. 24/2017 (Romano, 2019: 1-13). This law established that healthcare professionals must adhere to the recommendations provided by guidelines and good clinical-assistive practices. Art. 590-sexies, para. 2, of the Criminal Code provides for a cause for non-punishability for negligence due to lack of skill if the guidelines appropriate to the specific case have been respected.

The use of AI in the healthcare sector requires questioning the qualification of the medical activity performed by the professional. Although this is generally considered an obligation of means, liability for its breach is assessed according to the criterion of negligence, based on professional diligence (Art. 1176, para. 2, of the Civil Code) and compliance with guidelines (Terrosi Vagnoli, 1999: 189). From the perspective of negligent liability, it must be excluded that the physician can be held responsible for the malfunction of an AI system that is beyond his control, due to its high degree of autonomy and opacity. The physician's liability remains limited to only those cases where the damage is a consequence of incorrect use of the machine, attributable to his own negligence. For example, healthcare personnel may be held responsible without adequate training or understanding of its functioning, for having used an intelligent system while being aware – or culpably unaware – of its defectiveness or its limits; for not having detected the erroneousness of the indications provided by the machine, where such an error was recognizable through diligent verification in accordance with the *lex artis* (Lanzi, 2025: 7).

A part of the doctrine has proposed the application of special forms of non-contractual civil liability (Arts. 2049, 2048, 2052, 2050, 2051 of the Civil Code), but these approaches are generally considered inadequate. The norms in question were conceived for natural intelligence (human or animal) and are difficult to transfer to the context of artificial intelligence (Faccioli, 2024: 3). In particular, the classification of medical activity as a hazardous activity under Art. 2050 of the Civil Code appears implausible when the use of advanced technological solutions contributes to increasing the accuracy and safety of care. Furthermore, Art. 590-sexies, para. 3, of the Criminal Code explicitly refers to the paradigm of liability for negligence (Art. 2043 of the Civil Code) for the physician acting as an auxiliary of the healthcare facility, precluding interpretations aimed at applying more stringent regimes.

A crucial aspect is *black box medicine*. The algorithms are so complex that deciphering them becomes an arduous task, transforming AI systems into true "black boxes". Such opacity raises significant issues regarding informed consent (Morana et. al, 2022: 127-151), which requires the patient to be aware of the use of the technology and its contribution to the diagnosis or treatment. However, Italian jurisprudence has downplayed the criminal impact of invalid consent, stating that criminal liability exists only in

the presence of a violation of the *lex artis* that is causally relevant to the occurrence of the harmful event.

It should also be noted that it may be difficult for physicians to deviate from the indications provided by an AI system, even if they do not agree with its conclusions. The fear is that failure to comply with the information provided by the equipment could expose the professional to liability, aggravated by the impossibility of refuting the algorithm due to its opacity. Medical AI will in the near future become part of the standard level of care, with liability of the healthcare operator in case of omitted use. This implies that the physician must not only know how to use AI, but also be able to critically evaluate its indications, even without being able to fully understand its internal workings. The challenge lies in balancing the principle of reliance on technology with the duty of supervision and control, which remains with the human professional.

In summary, the criminal liability of the physician in the age of AI focuses on his negligent conduct in the use of the instrument, but it clashes with the difficulty of assessing negligence in a context of algorithmic autonomy and opacity. The *lex artis* will have to evolve to include diligence in the interaction with AI, but without imposing an unrealistic burden on the physician to understand or predict algorithmic behavior.

4. The liability of the manufacturer and the healthcare facility: damage from a defective product, safety obligations, and the chain of responsibility

The introduction of artificial intelligence in medicine not only redefines the role of the physician but also extends and complicates the chain of responsibility, significantly involving the manufacturers of AI systems and healthcare facilities. The complexity of the healthcare system, understood as a socio-technical system, with its interactions between human, technological, and procedural components, generates complex problems that require articulated responses in terms of liability (Ruffolo, 2023: 14-15).

AI systems used for diagnostic purposes are, first and foremost, a type of software. The European Commission has clarified that software is considered a "product" for the purposes of Directive 85/374/EEC on liability for defective products. Furthermore, Regulation (EU) 2017/745 on medical devices defines diagnostic software, including those based on AI, as "medical devices". Since there is a genus-species relationship between products and medical devices, it follows that diagnostic AI systems are products. If an AI system, as a product, causes harm (death or personal injury) that falls within the criminal offenses of Art. 590-sexies of the Criminal Code, it can establish liability for product damage on the part of its respective creators. This is because negligent conduct

(commissive or omissive) attributable to the system can only derive from a prior negligent active or passive behavior of one of the professionals involved in its creation.

The obligations incumbent on the creators of AI systems (manufacturers, developers, programmers, *domain experts*) derive mainly from Regulation (EU) 2017/745 and the proposed regulation on artificial intelligence (AI Act). These obligations include the following points.

- **Establish, document, implement, and maintain a risk management system:** this system must identify and analyze known and foreseeable hazards, estimate and evaluate risks, eliminate or control them, and assess the impact of information from the production and post-market surveillance phase. The residual risk associated with each hazard, as well as the overall residual risk, must be considered acceptable.
- **Ensure product conformity:** manufacturers must ensure that their products are designed and manufactured in accordance with essential safety and performance requirements.
- **System updates:** AI systems, especially those applied to diagnostics, require continuous updates, as they are based on current human knowledge and do not devise innovative solutions. The obligation to update arises upon the discovery of any new medical law, corroborated by authoritative, independent, reliable, and scientifically rigorous studies. *Domain experts* are required to follow the evolution of the most promising medical studies to proceed promptly with the updating of AI systems.
- **Post-market surveillance:** suppliers must inform distributors and competent authorities in case of non-compliance or serious risks, immediately adopting corrective measures. They must also establish and keep up-to-date a system for recording and reporting incidents and safety corrective actions.

5. Future scenarios and *de jure condendo* perspectives: the responsibility gap, human-machine interaction, and the need for new paradigms

The evolution of AI in the medical-diagnostic sector requires a reflection on the repercussions in the criminal law field, especially regarding subjective imputation. Three main models are envisaged:

1. **AI as an aid to the physician**, devoid of autonomous legal relevance (Iagnemma, 2020: 458). In this perspective, the recommendations provided by the AI – even if inaccurate or harmful – would not be capable of determining profiles of direct criminal liability, not even if they mislead the physician who uses them. This reconstruction is, however, subject to criticism, both on a logical

and a legal level. From a logical point of view, the assimilation of AI to traditional consultative tools, such as manuals or scientific texts, appears problematic: while the latter are limited to providing static data and general information, AI systems operate through machine learning mechanisms and process solutions in an at least partially autonomous way, replicating – albeit imperfectly – human clinical reasoning. From a legal point of view, the approach under examination raises questions regarding the identification of responsible subjects. Excluding from the outset the liability of the designers or developers of the systems – despite the concrete impact of the algorithm on the physician's diagnostic orientation – entails the risk of an unjustly exclusive imputation to the healthcare professional. Attributing all responsibility to the latter, even in the presence of an error caused (or significantly influenced) by the indications provided by the system, is disproportionate and likely to frustrate the fundamental principles of negligence and subjective imputation.

2. **AI as an autonomous decision-maker**: although this evolution promises greater efficiency and standardization, it poses significant questions regarding the imputation of liability for any damage resulting from erroneous decisions of the system. If the system acts without human intervention, the problem of the responsibility gap arises (Lombardi, 2024: 72), that is the impossibility of attributing criminal liability in the absence of human intent or negligence. Excluding human responsibility altogether would, in fact, amount to a form of de-responsibilization that is unacceptable on both ethical and legal grounds. The only path consistent with the principles of the legal system would then be to attribute criminal liability to those who have participated, in any form, in the design, development, or dissemination of the AI system, applying the general rules governing complicity in crime.
3. **Cooperative model**: this conceives of human-machine interaction as teamwork (Risicato, 2013: 31-39), in which both the physician and the subjects involved in the creation of the AI could be held responsible according to the logic of negligent cooperation (Art. 113 of the Criminal Code), due to the functional interdependence between their respective conducts (Consulich, 2022: 1032). This has significant consequences: for example, in the case of negligent personal injury prosecutable upon complaint, a complaint against the healthcare professional would also extend its effects to the material co-perpetrators of the event.

Despite the significant progress in the cognitive and operational capabilities of artificial intelligence systems, the prevailing doctrine continues to exclude the possibility of recognizing direct criminal liability for them, believing that criminal law presupposes

a subject endowed with consciousness, reproachability, and motivatability, elements ontologically absent in artificial agents. The parallel with the liability of legal persons also proves unpersuasive, since it is in any case based on organizational faults attributable to human subjects (Lanzi, 2025: 4). From the point of view of utility, the imposition of a criminal sanction on a machine is devoid of practical meaning: if the system proves to be dangerous, public intervention should consist in modifying the software or withdrawing it from the market, rather than in a punitive reaction.

Thus, the so-called responsibility gap manifests itself, that is, the vacuum of responsibility that occurs when the system has causally contributed to the production of the illicit event, in the absence of intentional or negligent conduct attributable to programmers or users (Lombardi, 2024: 73). The current criminal law framework thus proves inadequate to guarantee effective protection, making *de jure condendo* solutions necessary. Among the most significant proposals are:

- **Strengthening standards of diligence.** If AI systems are called upon to perform activities typical of the medical profession, it becomes necessary to update the standards of skill required of healthcare professionals. The use of advanced systems, such as *Watson*, entails the need for the physician to develop critical skills of interaction with the algorithm, including understanding the limits, biases, and functioning of the AI. In these contexts, artificial intelligence acts as a technical partner whose input must be critically assessed, interpreted using proper clinical and scientific standards, and integrated into the wider therapeutic decision-making process. In this scenario, it is the doctor who plays a key and active role, taking responsibility for balancing the different factors involved: on one side, the added value of the algorithm's diagnostic and predictive abilities; on the other, the essential ethical, professional, and legal requirements that protect the patient's right to health (Vallini, 2024: 3).
- **Proactive regulation and specific precautionary obligations.** A regulatory framework capable of anticipating the risks associated with the use of AI is hoped for, through technical protocols and precautionary obligations. The AI Act of the European Union, through the classification of high-risk systems and the provision of specific obligations for developers and users, represents a first significant step. However, the excessive delegation to large companies in defining the area of permitted risk is criticized. Alternatively, the establishment of an independent administrative authority with technical-scientific expertise is proposed, tasked with setting objective safety standards and precautionary measures, overcoming the current self-regulatory model.

- **Theory of normative agents.** To regulate the possible emergence of 'criminal' phenomena related to the conduct of autonomous intelligent agents, the best solution could be the adoption of the theory of normative agents. These agents, both norm followers and capable of "intelligent violations" of the norms, have a role in harmonizing the behaviors of AI. In the case of unjustifiable illicit conduct, but without intent or negligence on the part of human programmers or users, recourse to criminal law should be avoided, favoring corrective interventions on the system, aimed at preventing reiteration. The goal is not to punish the machine, but to restore a correct functional setup.
- **Informed consent and transparency.** The patient has the right to be adequately informed about the use of AI in the diagnostic and therapeutic process. The principle of transparency, also enshrined in Article 52, paragraph 1, of the AI Act, requires that the information be understandable, balanced, and proportionate to the cognitive capacity of the interested party.

In conclusion, the integration of AI into the medical-diagnostic sector requires a profound revision of the relationship between human and machine. In the initial phase, AI may be considered a mere auxiliary tool, with liability imputed exclusively to the physician. However, with the increasing refinement of systems and their ability to develop more accurate solutions than the average human operator, the exclusive attribution of liability to the healthcare professional will become unsustainable. The imputation must therefore extend to the manufacturers and distributors of the software, in order to prevent significant cases of malpractice from falling outside the criminally relevant area. The role of scientific research conducted by human beings will nevertheless remain essential, as the primary source of medical knowledge that feeds artificial intelligence. The legislator's challenge will be to reconcile with technological evolution, preparing a regulatory framework consistent with the principles of liability, safety, and justice.

References

Amore, N., Rossero, E. (2024). Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità. Una ricerca sociologica e giuridico-penale. Bologna: Il Mulino.

Amore, N., Cioni, A., Corti, D., Lippi, M.E., Sestieri, M., Vallini, A. (2024) Policy Paper. Buone pratiche e modelli di regolamentazione per l'impiego della IA nella diagnostica per immagini. La legislazione penale, pp. 1-27.

Baldassarre, M., Sasanelli, L. (2021). Socially Assistive Robotics ed educazione inclusiva: prospettive teoriche e applicazioni pratiche nella disabilità intellettiva. QTimes – webmagazine, n. 1, pp. 14-28.

Chen, M. (2023) Exploring the potential of robocare in anti-agesim and protecting human rights for elderly people in long-term care settings. Elderly people and discrimination: prevention and reaction, pp. 643-661.

Colaruotolo, A. (2022) Intelligenza artificiale e responsabilità medica: novità, continuità e criticità. Responsabilità Medica, n. 3, pp. 229-310.

Consulich, F. (2022) Flash offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti. Rivista Italiana di Diritto e Procedura Penale, fasc. 3, pp. 1015-1061.

Faccioli, M. (2024) Responsabilità medica per danni cagionati dall'intelligenza artificiale, available at: https://www.eclegal.it/responsabilita-medica-danni-cagionati-intelligenza-artificiale/, accessed on 30.06.2025.

Hajdú, J. (2020) Dignity of elderly persons and digitalised social care. Yearbook Human Rights Protection, n. 3, pp. 570-595.

Iagnemma, C. (2020) I 'robot medici': profili problematici in tema di alleanza terapeutica e di responsabilità penale. Corti supreme e salute, n. 2, pp. 441-458.

Januario, T.F.X., Rodrigues, R.S. (2024) Intelligenza artificiale e diritto penale della medicina: un'analisi basata sull'ordinamento giuridico portoghese. Corti supreme e salute, n. 1, pp. 366-403.

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. The right to life and body integrity, pp. 415-429.

Lagioia, F. (2020) L'intelligenza artificiale in sanità: un'analisi giuridica. Torino: Giappichelli.

Lanzi, M. (2025) Uso di strumenti a intelligenza artificiale e imputazione della responsabilità penale: difficoltà ricostruttive e prospettive di intervento, available at: https://dirittodidifesa.eu/uso-di-strumenti-a-intelligenza-artificiale-e-imputazione-della-responsabilita-penale-difficolta-ricostruttive-e-prospettive-di-intervento-di-massimiliano-lanzi/, accessed on 30.06.2025.

Lombardi, O. (2024) Responsabilità penale dell'uomo per il danno cagionato attraverso condotte dolose e colpose nell'impiego dei sistemi di intelligenza artificiale. Sistema Penale, n. 12, pp. 57-73.

Morana, D., Balduzzi, T., Morganti, F. (2022). La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione. Federalismi.it, n. 34, pp. 127-151.

Pasceri, G. (2021) Intelligenza Artificiale, Algoritmo e Machine Learning. La responsabilità del medico e dell'amministrazione sanitaria. Milano: Giuffrè.

Pignatiello, G.G. (2021) Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle Digital Authorities?. Federalismi.it, n. 16, pp. 164-185.

Risicato, L. (2013) L'attività medica di équipe tra affidamento ed obblighi di controllo reciproco. L'obbligo di vigilare come regola cautelare, Torino: Giappichelli.

Romano, B. (2024). Il DDL in materia di IA: l'utilizzo nell'attività giudiziaria e in ambito sanitario. Rivista italiana di medicina legale, n. 1-2, pp. 409-416.

Romano, B. (2019) La responsabilità penale dell'esercente la professione sanitaria tra antichi dubbi e nuovi problemi. In: B. Romano (ed.) La responsabilità penale nelle professioni sanitarie. Pisa: Pacini Giuridica, pp. 1–13.

Ruffolo, U. (2023). L'Intelligenza Artificiale nei dispositivi medici e nell'attività sanitaria: per un'analisi interdisciplinare circa responsabilità, controlli preventivi e disciplina dei dati sanitari. Le conseguenti proposte interpretative e normative. In: U. Ruffolo, M. Gabbrielli, eds. Intelligenza Artificiale, dispositivi medici e diritto. Un dialogo fra saperi: giuristi, medici e informatici a confronto. Torino: Giappichelli, pp. 3-20.

Salvadori, I. (2021) Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale. Rivista Italiana di Diritto e Procedura Penale, n. 1, pp. 83-118.

Terrosi Vagnoli, E. (1999) Le linee guida per la pratica clinica: valenze e problemi medico-legali. Rivista Italiana di Medicina Legale, p. 189 ff.

Torres, M., Maynes, E. (2025), Evolution of Robotic Systems Utility in Anatomy and Surgery. International Journal of Cadaveric Studies and Anatomical Variations, n. 6, pp. 25-27

Vallini, A. (2024) Il Progetto IUSTIDIA (buone pratiche e modelli di regolamentazione per l'impiego della IA nella diagnostica per immagini). Una panoramica. La legislazione penale, pp. 1–6.

Legal Sources:

Regulation of the European Parliament and of the Council on Artificial Intelligence of 13 June 2024 (so-called AI Act), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL_202401689

Directive of the European Parliament and of the Council on liability for defective products of 23 October 2024, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202402853

Draft Law on Artificial Intelligence of 20 May 2024, https://www.senato.it/service/PDF/PDFServer/BGT/01418921.pdf

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 June 2017 on medical devices, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R0745