Tulio Felippe Xavier Januário*
Renata Da Silva Rodrigues**

Review Paper
DOI: 10.47152/ns2025.15

FROM HIPPOCRATES TO ALGORITHMS: *CRIMINAL LAW AND THE RIGHT TO HEALTH IN THE AGE OF ARTIFICIAL INTELLIGENCE IN PORTUGAL*[1]

The present paper aims to investigate, in the light of the Portuguese legal system, the issue regarding medical criminal liability in cases in which AI systems are applied and end up causing harm. In other worlds, we will address the following questions: should criminal law intervene in those cases? How to determine authorship and causality, bearing in mind the multitude of actors involved in the development, programming, production, distribution and use of these technologies? Can we consider criminal liability of legal entities in the field of medical criminal law? Are there individual persons criminally responsible in those situations? For that, we will initially analyze the concept and functioning of AI and how it can be effectively applied in the medical sector. Subsequently, we will study the risks inherent to that use that may have criminal consequences for the individuals and legal entities involved in the case. At the end of the investigation, based on a deductive methodology applied to the analysis of theoretical models of criminal responsibility proposed for situations with the intervention of AI, we will demonstrate some of the difficulties in determining, in these cases, the authorship of the crime and the limits of the allowed risk in the conduct of the intervening parties.

Keywords: *right to health; artificial intelligence; medical law; criminal law; portuguese Law; medical criminal law*

* PhD Candidate (University of Coimbra – Portugal). Professor of Criminal Procedure (Mackenzie Presbiterian University – Brazil), email: tuliofxj@gmail.com, ORCID: 0000-0003-0400-1273.

** University of Vale do Sapucaí – UNIVAS/Brazil, with a scholarship from the "PROUNI" Program, email: renatarodrigues042@gmail.com, ORCID: 0009-0004-5334-2693.

[1] This investigation was carried out within the scope of the project entitled "Autoria e responsabilidade em crimes cometidos através de sistemas de inteligência artificial", funded by the Fundação para a Ciência e a Tecnologia – FCT(2020.08615.BD). For a broader and more in-depth analysis of the topic in question, see: Januário, Rodrigues, 2024, Januário, 2022, Januário, 2020.

Introduction

Among the main sectors influenced by the evolution of science and technology, healthcare proves to be one of the most paradigmatic. The progressive development of Artificial Intelligence (AI), driven by big data and machine learning processes, has made it possible to envisage, in the near future, the full operation of diagnostic support programs, autonomous mechanisms for monitoring and assisting patients, robotic tools for aiding surgical procedures, and even suicide-prevention algorithms through social networks (Januário, 2020: 37ff).

Although the benefits arising from the use of AI in medicine are almost certain, the risks posed by this new technology, and, all the more so, the challenges it imposes on legal practitioners in normative, preventive, and especially liability-related terms, are undeniable. With regard specifically to criminal law, further reflection and possible adjustments will be required to both its general part and some types of offences within its special part, in order to address this imminent reality.

In light of this, the aim of this article is to analyze some of the main legal and criminal implications of using AI in healthcare, with particular regard to the attribution of possible criminal liability for harm arising from interactions with AI. To do so, we will first seek to clarify what can effectively be considered artificial intelligence and how it relates to the concepts of big data and machine learning. This brief discussion is necessary because, although these terms are increasingly present on the agenda of legal discussions, legal practitioners often face natural difficulties in dealing with these new, complex topics that originate in fields traditionally distant from our discipline.

Once these clarifications have been made, the second section will explore some of the main ethical and legal issues that regulation must confront due to the application of AI mechanisms in healthcare. Examples include difficulties related to safeguarding patient privacy concerning their personal data and ensuring transparency in AI procedures.

Since, despite the high level of applied technology, AI will inevitably remain subject to failures and errors, the final section will address the central question of this investigation: how criminal liability can be assessed in a context of such uncertainty and unpredictability, a situation made particularly complex by the introduction of systems that, although endowed with reasoning and decision-making capacities independent of human will, are nonetheless not themselves subject to criminal liability.

1. Possible applications of AI in the healthcare sector

There is currently much discussion about scientific advances in the field of AI and how this technology will affect various sectors of society. Indeed, literature, cinema, and television have long portrayed (albeit as a distant dream) vehicles operating without human drivers, intelligent domestic assistants, and especially robots working in various areas, such as medicine and public safety.

Although we have not yet reached the level imagined by screenwriters, it is certain that we are now witnessing tools equipped with “sector-specific” AI, capable of performing certain tasks autonomously. This is the case, for example, with Apple’s intelligent virtual assistant “Siri” and Amazon’s “Alexa.” In the transport sector, experiments with autonomous vehicles have also been conducted, leading to the first recorded accidents involving this type of automobile.

For the purposes of this article, it is important to highlight that healthcare has consistently proven to be one of the most promising fields for the application of AI. According to Luiz Carlos Lobo, this application involves the use of computers to solve medical problems through the analysis of large volumes of data and the implementation of algorithms defined by experts in the field (Lobo, 2017). However, as we will demonstrate, the possible intersection between AI and medicine is much broader. Its main current and future applications include not only clinical decision-making support, but also patient monitoring and general care, as well as the use of autonomous equipment to assist in surgical procedures. More recently, there has even been discussion about the possibility of monitoring social networks to assess potential health risks among their users. In this context, André Dias Pereira argues that, among the main topics likely to revolutionize healthcare services, bioethics, and medical law, are those related to big data, AI, and the digitization and robotization of medicine (Pereira, 2009: 30).

The term artificial intelligence dates back to 1955, when computer scientist John McCarthy published *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. At the time, AI was defined as “the science and engineering of making intelligent machines, especially computer programs,” related to “the similar function of using computers to understand human intelligence,” but not limited to “biologically observable methods” (McCarthy et al., 2006: 12ff; McCarthy, 2007: 2).

Currently, an AI system is understood as one capable of capturing and analyzing surrounding information, learning from it, and selecting the most appropriate response, without substantial human interference (Steibel et al., 2019: 53-56). Its primary characteristics are therefore: (i) autonomy, reflected in the ability to perform tasks without constant human guidance; and (ii) adaptability, meaning the ability to learn from past experiences and improve performance (Jesus, 2019: 43-45).

To provide greater precision, the European Commission's High-Level Expert Group on Artificial Intelligence (2019: 6) has proposed dividing the concept into two groups: (i) AI as a system, understood as software or hardware developed by humans that operates in physical or digital environments, and which, to achieve a specific goal, perceives its surroundings through data collection, interpretation, and processing, and identifies the best decision to make based on predefined "symbolic rules" or by "learning" an appropriate numerical model. These systems are also capable of adapting their behavior after analyzing environmental changes caused by their own previous actions; and (ii) AI as a scientific discipline, encompassing and integrating various techniques and methodologies, such as machine learning, automated reasoning, and robotics, into "cyber-physical" systems.

Based on the COMEST Report on robotics ethics (2017: 48), Susana Aires de Sousa (2020: 62) also distinguishes between deterministic robots (technological systems preprogrammed to perform specific tasks) and cognitive robots (capable of making choices and carrying out tasks for which they were neither designed nor anticipated by their programmers). This distinction is significant because, while deterministic algorithms are "trained" to respond to specific questions or situations, cognitive systems possess self-learning capabilities and constant evolution, making it impossible to reliably predict their responses in advance.

In this latter case, according to Kaplan and Haenlein (2019: 17), AI uses the Internet of Things and big data as input to identify rules and patterns, and through machine learning can acquire knowledge for which it was not originally programmed. As Caitlin Mulholland and Isabella Frajhof (2019: 265) explain, machine learning systems enable entirely autonomous decision-making without human interference. By processing massive amounts of data (input), the system generates results (output) based on deductive procedures and statistical analyses associated with AI.

In medicine, data collected and processed by these systems may come from various sources, such as electronic medical records, medical literature, private insurance data, prescriptions, and even information gathered from smartphone applications. Using machine learning techniques, which involve learning the rules and methods necessary to detect patterns within vast big data sets, algorithms can be developed to make predictions and classify patients into groups (Price II, 2017: 2).

Specifically regarding AI in medicine, we can highlight, by way of example, tasks related to: (i) clinical decision-making support; (ii) personalized medicine; and (iii) robotics for surgeries, treatments, patient monitoring, and diagnostics.

Regarding this last domain, it is important to note that, while healthcare systems fully integrated with AI have yet to be realized, expectations for the next years are promising, especially if AI development is accompanied by sufficient data and well-structured systems, according to the report *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence*, published by Stanford University. Whereas physicians currently rely on patients to verbally describe their symptoms and mentally correlate them with known pathologies, in the future an automated assistant may perform this task, albeit under physician supervision. The physician's expertise will remain crucial to feeding data into the system and evaluating its output (Stone et al., 2016: 26), especially given the inability to explain precisely *why* or *how* conclusions are reached, creating what Price II calls a "medical black box". This situation is exacerbated when AI systems can incorporate new data, redefine previous predictions, and even modify their own algorithms (Price II, 2017: 2).

In robotic surgery, due to its complexity and implications, this field is expected to evolve into specialized niches, each developed by different companies that will face the challenge of building comprehensive systems for data analysis, detection, automation, and enhancement (Stone et al., 2016: 28).

According to Laura Terrizzi's classification, there are three macro-areas in which AI and robotics may prove beneficial: (i) clinical applications: facilitating, for example, less invasive surgeries (with benefits in precision, reduced patient pain, lower risk of complications, and shorter recovery times, as well as reduced strain on medical staff) and intelligent medical capsules (for detecting precancerous lesions and tumors in the intestinal tract); (ii) rehabilitation, particularly with "intelligent prosthetics"; and (iii) patient assistance, including routine logistical support in clinical and hospital settings (Terrizzi, 2023: 70-76).

As already noted, not all robotic tools are equipped with AI, as many simply reproduce preprogrammed commands, albeit with remarkable precision. However, when devices are capable of acquiring and processing data, autonomously "learning" from them, evolving, and making independent decisions, albeit in limited contexts, they may be considered AI-enabled products, subject to the same legal questions analyzed here.

Wearable devices also deserve mention; according to Stanford University's report, these are increasingly promising and commercially viable (Stone et al., 2016: 27). They allow for continuous patient data collection, such as blood glucose and ECG, which can trigger automated actions, like insulin injections, subcutaneous defibrillator shocks, or medication adjustments for Parkinson's disease patients (Lobo, 2017: 187).

Clinical Decision Support Systems (CDSS) appear to be more advanced, with operational programs such as IBM's Watson Health and DeepMind (acquired by Google in 2014 and now integrated into Google Health). Both process oncology-related information stored in the cloud, along with risk assessments and patient progress records. They catalog cases with diagnostic frameworks, prescribed treatments, and outcomes, thereby expanding medical knowledge and suggesting actions based on probabilistic data (Lobo, 2017: 189)

As Laura Terrizzi (2023, 77-86) explains, CDSS can be either "knowledge-based" or learning-based. Knowledge-based systems consist of three core technological levels: (i) a medical knowledge base, composed of hundreds of thousands of medical publications; (ii) an inference engine, developed through "if-then" rules distilled from the literature based on clinical relevance and case characteristics (such as patient age or therapy type); and (iii) a user interface for input and output.

Learning-based systems, which rely on machine learning and deep learning, can autonomously learn from past cases and experiences to identify clinical patterns. According to Terrizzi (2023: 84), the leading approaches include support vector machines, neural networks, and genetic algorithms.

Thus, the growing storage capacity of big data is crucial for these technologies' increasing presence in healthcare, particularly for disease prevalence, incidence, and progression data, which enable statistical modeling to predict epidemics and guide preventive actions. Patient data, combined with reported symptoms, diagnostic tests, treatments, and outcomes, create essential databases to refine clinical practices (Lobo, 2017: 190).

The so-called "personalized medicine" approach has gained significance through AI advances. As André Dias Pereira (2019: 32) explains, big data enables the development of individualized medical models based on phenotype and genotype analysis, aiming to design personalized therapeutic strategies at the right time. This allows for the early detection of predispositions and preventive interventions, leading to earlier diagnoses, reduced treatment costs, and better-tailored therapies, including lifestyle recommendations to prevent or mitigate disease.

Indeed, as Eric Hilgendorf (2019: 193) notes, medicine increasingly aims not only to cure but to enhance healthy individuals. Examples of this paradigm shift include cosmetic surgery and advances in genetic engineering. Hilgendorf argues that, in the near future, scientific progress may allow for "optimization" of traits in future generations.

With developments in reproductive medicine and genetics, another level of "enhancement" could, theoretically and considering ethical, moral, and legal implications, become feasible. In some countries, eliminating genetically impaired embryos is already a common practice in assisted reproduction; such selection could eventually extend to traits such as sex, physical appearance, or even personality. This raises the prospect of designing "desired children", made plausible by combining artificial insemination with genetic modification (Hilgendorf, 2019: 195)[2].

However, AI-related predictions are not limited to identifying diseases through predictive genetic diagnosis, made increasingly feasible by advances in genomic research (Hilgendorf, 2019: 196-198). There is also interest in using AI for suicide prevention. Marks (2019: 104-108) categorizes this field into two groups: *medical suicide prediction*, which analyzes patients' medical histories and may be carried out by physicians, public health researchers, government agencies, and health systems; and *social suicide prediction*, which involves analyzing individuals' behavior and interactions on social media, apps, and other platforms outside the healthcare system. Unlike the former, social suicide prediction relies on tech companies such as Facebook, Crisis Text Line, and Objective Zero. Its goal is to mitigate suicide risk by analyzing users' digital traces. For instance, posts containing terms such as "sad" or "very sad" can trigger concern.

From this section's analysis, the potential of AI in medicine becomes evident, extending well beyond the examples presented here and likely to expand further. At the same time, this emerging but promising integration gives rise to numerous ethical, moral, and, ultimately, legal issues that demand urgent evaluation so that the law can effectively respond to this new reality through regulatory, preventive, and punitive measures.

2. Possible Legal Issues Arising from AI in the Healthcare Sector

To illustrate the potential problems arising from the use of AI in healthcare, its application to suicide prevention (particularly through social network monitoring) proves paradigmatic. As Marks (2019: 102) explains, despite its undeniable advantages in identifying high-risk individuals and, consequently, preventing suicides, these techniques inherently involve serious violations of users' right to privacy, as well as other ethical and legal concerns. Among these are questionable categorizations (based on imprecise criteria) of individuals as suicidal or non-suicidal, potentially leading to marginalization, stigmatization, and trauma for vulnerable individuals, which could paradoxically worsen their clinical conditions and suicide risk.

[2] For a more detailed analysis of the ethical and legal issues arising from this matter, see: Januário, Rodrigues, 2024: 425ff. On the relevance of discussions on the protection of the rights of unborn children, see: Pavlović, 2022.

In analyzing these risks, Marks (2019: 111) classifies them into three groups: (i) security risks; (ii) privacy risks; and (iii) autonomy risks. The first category includes cases of false negatives, which would leave potential suicide victims without necessary assistance, and false positives, which may result in partial treatments administered against a patient's will, or unexpected police interventions. In the latter case, risks are not limited to potential law enforcement overreach but may also lead to criminal proceedings and even imprisonment in jurisdictions that criminalize suicide attempts.

Privacy risks, in turn, may involve unauthorized data access or sale and transfer of patient information to third parties, potentially resulting in discrimination, stigmatization, and exploitation. As for autonomy, particularly in AI-driven suicide prevention, risks relate to possible censorship, unnecessary confinement, involuntary civil commitments, and even criminal sanctions in some legal systems (Marks, 2019: 111)[3].

Although this section uses AI-based suicide prevention as an example and mentions only three categories of risks, it is clear that other applications of AI may raise comparable concerns. One of the key issues is the lack of transparency, which seems inherent to AI technologies. Marks, for instance, criticizes Facebook's *social suicide prediction* system for bypassing independent ethical review and failing to disclose its methodologies, which remain confidential (Marks, 2019: 109). Yet this transparency deficit is not unique to this example; as Price II explains, AI algorithms are often so complex that deciphering them is extremely difficult, turning AI systems into genuine "black boxes" (Price II, 2017: 2).

In this context, Miriam Wimmer (2019: 15ff) highlights the "opacity" of AI systems, given the immense difficulty of tracing the criteria underlying their outputs, which raises undeniable concerns about transparency, explainability, and verifiability. On opacity, Jenna Burrell (2016: 1) observes that when algorithms process input data to generate outputs, the rationale behind their decisions is often unknowable, and in many cases, even the input data remain obscure. In the medical context, Wimmer (2019: 16ff) questions how patients can be expected to place their trust in a "black box" diagnosis when physicians themselves cannot justify a treatment decision beyond the inference produced by a big-data-based AI system.

This opacity is closely tied to issues in data collection and analysis, which also raise significant privacy concerns – especially in healthcare, where sensitive personal data are constantly used (Souza, Oliveira, 2019: 67-69). Alexandre Libório Dias Pereira (2018: 60) stresses that those responsible for processing such data bear a heightened duty of care,

[3] For a detailed analysis of autonomy in its most varied facets, see: Heberling, 2021: 595.

including technical and organizational measures to protect against destruction, loss, alteration, dissemination, or unauthorized access. Illustrating this, Eric Hilgendorf (2019: 198-199) emphasizes the importance of safeguarding genetic data: if an individual's predisposition to a disease is identified, public disclosure could lead to employment discrimination or denial of insurance coverage.

Personalized medicine also poses potential challenges to individual autonomy. Before symptoms manifest, AI systems may impose recommendations or restrictions that are difficult for the general population to follow, especially in the absence of resources to contest or ignore such guidance (Pereira, 2021: 247).

Further reflection is also required regarding how much information patients should receive and its potential psychological impact. While advances in predictive medicine are invaluable for early diagnosis, some patients may prefer not to know their genetic predispositions. Even when they choose to be informed, consideration must be given to their potential reaction and its effects on family members.

In line with these developments, discussion of the scope and limits of information disclosure to patients is necessary, especially to preserve their "right not to know" (Pereira, 2019: 33).

Despite the technological sophistication of AI systems, they are far from infallible, and errors may cause significant harm to third parties. As Jason Chung (2017: 37-38) notes, IBM's Watson system, for example, has been found to contain errors stemming from programmer oversight, physician input errors during training, or the inherent unpredictability of algorithmic data processing.

Steven Gouveia (2019: 173-176) highlights this unpredictability as a central dilemma: as AI and autonomous systems advance, operators lose the ability to reliably anticipate their behavior. Society faces the uncomfortable choice of either abandoning highly advanced tools or developing solutions to this "responsibility gap". As Gouveia explains, machines no longer operate strictly under human direction but may decide their own course of action, learning from experience and altering their operating rules.

Hilgendorf (2019: 199-200) similarly emphasizes that when robots can independently learn, incorporate new experiences, and draw new conclusions, questions of civil and criminal liability become increasingly complex. While liability allocation in medical law has always been challenging, introducing an AI "agent" complicates matters further: should blame fall on the programmer, the user, or the robot itself?

These difficulties are exacerbated by the lack of regulatory frameworks. In the U.S., for instance, Mason Marks (2019: 105) explains that while *medical suicide prediction* is regulated by multiple standards, such as the Health Information Portability and

Accountability Act (HIPAA), which imposes civil and criminal penalties for privacy violations, and the Federal Common Rule governing human research, *social suicide prediction* falls outside these regimes, as it is conducted outside the healthcare system.

Debates about whether AI should be strictly regulated are not limited to this field. Kaplan and Haenlein (2019: 22) note that while some advocate immediate, proactive national and international regulation, others fear this would stifle progress in such a rapidly evolving field.

Beyond regulatory challenges, liability allocation in cases of AI system failures remains a major concern. As Price II (2017: 3) observes, while clinical trials and scientific testing are designed to ensure safety and efficacy, these methods are ill-suited to "black box" medicine because machine learning algorithms often cannot explain their reasoning, or their explanations are so complex that they are practically incomprehensible. Moreover, some algorithms generate highly personalized predictions that make standardized testing infeasible, while others are capable of self-modification, requiring ongoing validation.

Another pressing issue is the difficulty for physicians to disregard AI recommendations, even when they disagree with them. Depending on the legal framework, ignoring AI-generated guidance may expose practitioners to liability (Marks, 2019: 113). Additionally, given algorithmic opacity, professionals may lack the expertise to understand or challenge AI conclusions, making rebuttal extremely difficult.

This opacity also complicates informed consent. Patients must be fully informed about the technology and its role in diagnosis and treatment (Allain, 2013: 1063), but will healthcare providers be able to explain the basis for a diagnosis or why alternatives were excluded? How can informed consent be reconciled with the "black box" nature of AI systems? What legal and criminal implications might arise if patients refuse treatments recommended or performed by these systems?

Among the numerous legal questions raised by AI's integration into healthcare, the issue that draws particular attention, and will be addressed in the next section, is the potential for criminal liability arising from harm caused by intelligent artificial "agents."

As Price II notes, if harm results from a flaw in an algorithm's development, liability could be assigned to its programmers. But could direct users of AI tools, such as physicians or healthcare staff, also be held accountable? Should they rely blindly on these systems, or are they expected to evaluate their quality? If so, are they capable of doing so, and would this expectation undermine the very benefits these technologies provide? (Price II, 2017: 4)

3. Implications of AI for Criminal Responsibility in the Healthcare Sector

As demonstrated, AI can be applied to healthcare in a wide range of ways, from personalized and predictive medicine to diagnostic tools, suicide prevention systems, and robotic instruments for patient care and surgical procedures.

However, despite the highly advanced scientific development required and achieved by these technologies, AI systems are not infallible. They remain vulnerable to various types of errors, whether stemming from flaws in the system's design and production or from misinterpretation of inputs, potentially resulting in incorrect outputs.

It is undeniable that these technologies not only process extremely sensitive personal data but also directly affect the most fundamental legal interest: human life[4]. Consequently, any failure could lead to serious harm, ranging from improper disclosure of personal information to diagnostic or operational errors that compromise patients' physical integrity or even their lives.

The atribution of criminal liability in the medical field has always been a complex topic (Fidalgo, 2009: 417-418). The integration of AI systems capable of interpreting and learning from uncertain data through complex and rarely verifiable methods further complicates this task, introducing new challenges rooted in the inherent unpredictability of these technologies.

Hypothetically, if an AI system endangered a patient's life, body, or health by employing techniques during a procedure that deviated from *leges artis*, or if such measures were performed without proper informed consent, could the medical team or the hospital or clinic involved be held criminally liable? Similarly, if a patient suffered harm to their life or physical integrity because of a procedure carried out by an AI system beyond the scope of their consent, would this constitute a criminal offense? If so, who would be liable? The algorithm's developer or programmer? The members of the medical team? The hospital or clinic? Or the AI itself? These emblematic questions illustrate the pressing need for discussion about the medical criminal law in the near future.

According to Chung (2017: 38-39), there is currently no clear legal or regulatory framework for determining liability in cases of harm caused by AI system failures, such as those involving Watson. While, as Steven Gouveia (2019: 176-177) notes, a less advanced technology might not challenge traditional concepts of liability, part of these new tools' appeal lies precisely in their ability to replace human oversight, facilitated by the rapid advancement of algorithmic learning.

[4] On the difficulties in defining what we can understand as life: Ćorić, 2021.

Much of the debate over programmer liability for AI systems centers on their potential unpredictability and the harmful consequences this may cause. Susana Aires de Sousa (2020: 64) explains that what distinguishes autonomous machines from "conventional information systems for data collection and processing" is their ability to make decisions (often contrary to legal norms) independently of their programmers, based solely on the data they process and the experience they accumulate.

For this reason, some scholars advocate attributing criminal liability directly to AI systems. This is the solution proposed by Chung (2017, 38-39), who argues for granting AI systems a form of legal personality akin to that of medical students, making them directly liable for medical negligence and reducing the scope of liability for developers. According to Chung, this approach would make the liability regime in this field more predictable, thereby guiding technological development.

Gabriel Hallevy (2010: 174ff), in turn, proposes three distinct models of criminal liability for AI: (I) *Perpetration-through-Another Liability*, which assumes that AI systems lack human attributes, treating offenses committed through AI as those committed by legally irresponsible actors used as instruments for crime. In such cases, liability falls on the developer or user. This model applies when AI capabilities are underutilized or when systems are obsolete. However, it is not suitable for offenses stemming from the AI's independent knowledge or experience; (II) *Natural-Probable-Consequence Liability*, which applies when neither programmer nor user intends to commit a crime, nor foresees harm, but harm arises as a natural and probable consequence of their actions. According to Hallevy, such cases reflect negligence by the programmer or user, who should have anticipated the risk. If the AI functioned merely as an innocent agent, liability would not extend to it; however, if it acted independently, the system itself could bear direct responsibility; (III) *Direct Liability (Strict Liability)*. Hallevy argues that criminal liability of any agente (human, corporate, or AI) requires both an external element (*actus reus*) and an internal element (*mens rea*). While the external element is straightforward in AI (e.g., mechanical movements), Hallevy maintains that AI systems can also exhibit *mens rea*-like features. Through sensors, they can collect and interpret data (knowledge) and act intentionally to achieve specific goals (specific intent).

Sabine Gleß and Thomas Weigend (2014: 570-579) also address AI's potential liability, arguing that the key questions concern whether these entities possess the "capacity for conduct" and culpability. Although no definitive answers exist today, they suggest that future developments could make this possible, particularly if AI systems become capable of evaluating their behavior in moral terms, which could justify recognizing criminal capacity. Similarly, Paz Mercedes de la Cuesta Aguado (2015: 92-94) predicts that, depending on AI's level of autonomy, it may eventually be possible to attribute culpability to these systems.

However, in our view, neither legal norms nor the functions of punishment provide sufficient justification for granting AI systems any form of legal personality, regardless of their autonomy. Ontologically, humans and AI systems differ fundamentally: AI systems cannot contextualize decisions within social and ethical frameworks or adapt to contingent, unforeseen circumstances (Picotto, 2023: 54-55).

As Barresi (2023: 292-294) observes, AI systems operate mechanistically; their "decisions" are direct and immediate outputs of algorithms, devoid of freedom, consciousness, or will. Regarding "intention," Lacaze and Walther (2023: 165) note that AI does not act out of greed, hatred, or lust, but solely through rational and logical processes. In other words, AI decisions are not driven by conventionally understood motivations.

Furthermore, even the most advanced AI systems are incompatible with the legal concept of culpability and, consequently, with the principle of guilt in criminal law (Grandi, 2023: 68).

Punishing AI systems would also undermine the goals of criminal sanctions, as deterrence is meaningless without self-awareness or autonomy (Picotti, 2023: 54-55). Traditional penalties, such as imprisonment, restriction of rights, or monetary fines, would have no practical impact on entities without legal standing or property rights (Lacaze, Walther, 2023: 171).

Unlike corporations, where sanctions have reputational and financial consequences, AI systems would not be meaningfully affected (Magro, 2020: 9). This raises the question of whether alternative regulatory mechanisms outside criminal law might better safeguard legal interests in light of these emerging risks.

That said, corporate criminal liability remains an important topic within this contexto (Rodrigues, Sousa, 2021: 203ff). Until the enactment of Law Nº. 94/2021 of 21 December, Article 11th of the Portuguese Penal Code allowed corporate liability for only a limited set of healthcare-related offenses, such as Article 144-B (organ trafficking), Article 168 (non-consensual artificial reproduction), and Article 283 (spreading diseases, falsifying medical tests or prescriptions), as well as aggravated forms of Articles 285, 152-A (maltreatment), and 152-B (breach of safety rules). However, the legislative amendment expanded liability to include, among others, Articles 150 (medical-surgical interventions and treatments) and 156 (arbitrary medical-surgical interventions). Non-codified provisions also permit corporate liability for crimes under Law Nº. 32/2006 on medically assisted reproduction.

The increasing complexity of medicine is mirrored by a growing complexity of potential offenses, a reality likely to intensify with AI integration. When algorithmic, robotic, or AI systems cause risks or harm to life, physical integrity, or privacy through unauthorized disclosure of sensitive data, misconduct may originate from large organizations. In some cases, harmful outcomes may result not from isolated incidents but from internal corporate policies.

Political-criminal arguments for expanding corporate liability in this field go beyond these points. As previously highlighted, medical law's dependence on technological and scientific developments makes it inherently dynamic, frequently confronted with novel challenges (Hingeldorf, 2019: 3). AI law is similarly tied to technological advances, giving the intersection of these areas distinct contours.

In this context, criminal law should play a subsidiary role, reinforcing primary sectoral norms, such as ethical codes, professional conduct rules, *leges artis*, and industry-specific regulations. These norms collectively guide evaluations of whether conduct by individuals or corporations is lawful or criminally negligente (Frisch, 2004: 128-129; Januário, 2018: 15ff).

Article 150 of the Portuguese Penal Code, addressing medical-surgical interventions, reflects this dynamic approach. As a clear "blank criminal norm," it refrains from specifying what constitutes "the state of medical knowledge and expertise," deferring instead to evolving *leges artis*.

For these reasons, many scholars favor regulatory flexibility in this area. Price II (2017: 4) identifies scientific research and clinical testing as key to ensuring AI safety and effectiveness in medicine, advocating a flexible regulatory framework coupled with rigorous oversight during development and production (particularly in data quality and validation) and robust post-market surveillance. Kaplan and Haenlein (2019: 22) likewise propose collaborative standard-setting to avoid constant legal revisions, emphasizing customary norms that incorporate minimum transparency and testing requirements.

Given this field's dynamic and complex nature, the definition and implementation of sectoral primary norms to reduce risks is crucial. Compliance programs thus emerge as promising tools at the intersection of medical law and AI.

Broadly, compliance programs are mechanisms within corporate governance enabling entities, under state-granted autonomy, to self-regulate and self-monitor. Their immediate goals include fostering ethical culture, regulatory adherence, and preventing, investigating, and addressing unlawful practices, while their long-term objectives encompass reputation management, profitability, and protection of organizations and representatives from liability (Januário, 2019: 85-86, Januário, 2023: 378).

Among their various elements (spanning program design, implementation, and consolidation) (Engelhart, 2012: 712ff) risk identification and management procedures are particularly vital in complex fields like healthcare. Proactive identification of risks allows organizations to act within socially necessary and legally permissible limits (Bock, 2011: 43). From this, behavioral standards can be established internally or collectively through statutes, administrative provisions, or industry-wide guidelines, defining benchmarks for what constitutes a “reasonably prudent organization” (Lascuraín, 2013: 125-126).

In the context of AI in healthcare, risk management mechanisms may prove essential for monitoring scientific advancements in medicine and AI, as well as related legislative and regulatory changes. This would enable concrete definitions of permissible conduct and risk thresholds.

Such standards should be codified in ethical and conduct codes, which function as foundational norms binding an organization’s employees and representatives (Lascuraín, 2013: 125-126). These codes articulate corporate values, ethics, and policies and may extend beyond a single organization, being developed by international organizations, stakeholder groups, or industry associations (Navas Mondaca, 2013: 113-119).

These ethical codes should be regarded as *pre-legal standards of care*[5], incorporated into the category of “primary risk-reduction standards,” and factored into criminal law assessments of conduct[6]. Corporations and industry bodies, rather than states, are often better positioned to identify and mitigate risks posed by emerging technologies, establishing procedures and acceptable standards of behavior.

Thus, compliance programs, including internal guidelines and rules, serve not only as tools to assist the state in preventing, investigating, and prosecuting offenses but also as essential benchmarks for defining permissible risk in evaluating potentially criminal conduct in healthcare AI applications.

Marc Engelhart (2018: 22-30) proposes six levels of state involvement in corporate self-regulation, ranging from pure self-regulation (level 1) to mandatory compliance programs for organizations above a certain complexity (level 6). While this highest level

[5] Wolfgang Frisch (2004: 105-106) proposes a classification according to which, in addition to the limitation of risks through criminal law, there are behaviours governed by (I) ‘pre-legal’ norms – risk-reduction programmes, lex artis, ethical guidelines; (II) ‘pre-criminal-law’ norms – such as road traffic codes and medical codes of ethics; and (III) those not regulated within standards of care.

[6] According to Wolfgang Frisch (2004: 126), when the agent acts in accordance with the standard of diligence, and this can be considered, from an ex ante perspective, sufficient and appropriate to reduce the concretely relevant risks, the conduct cannot be regarded as typical.

is rarely implemented, Engelhart argues that the most effective way to promote compliance adoption is to offer exculpatory provisions for corporations that implement effective programs (level 5).

However, this approach faces two challenges in Portugal: (i) corporate liability does not cover some healthcare offenses; and (ii) Portugal's model of corporate criminal attribution places limited emphasis on compliance programs, restricting their role to the narrow provisions of Article 11(6) of the Penal Code.

Nevertheless, Law No. 94/2021 introduced significant changes regarding compliance programs' effects on sentencing. Amending Article 90-A of the Penal Code, it allows for: (I) Sentence mitigation for corporations that adopt effective compliance programs prior to an offense (Art. 90-A(4)); (II) The imposition of compliance-related obligations as an accessory penalty when necessary (Art. 90-A(5)); and (III) Replacement of fines with alternative penalties that adequately achieve punishment goals, considering compliance measures (Art. 90-A(6)).

In other words, although compliance programs have limited impact on establishing corporate criminal liability in Portugal (except in the narrow context of Article 11(6)), they can mitigate penalties. These conclusions directly apply to healthcare criminal law, particularly for offenses where corporate liability exists.

However, in the field of AI, it is not only through incentives for the adoption of compliance programs that the model of corporate criminal liability may exert influence. In legal systems where the attribution of criminal acts to collective entities still depends, to a greater extent, on the identification of conduct attributable to a natural person, one tends to encounter obstacles that are, in a certain sense, analogous to those found in cases of individual criminal liability for offenses involving AI systems.

As we have discussed elsewhere, the prevailing view is that Portugal follows a "mixed model" of corporate liability: Article 11(2)(a) reflects a model of "vicarious liability", while (2)(b) reflects a model closer to "self-liability" (Canestraro, Januário, 2018: 275, Januário, 2018: 201). The 2021 amendments did not fundamentally alter this interpretation.In both scenarios, liability is tied to human conduct, whether directly attributable to a leader or a subordinate acting under their authority. However, AI's involvement complicates identifying individuals responsible for harmful or dangerous outcomes, as well as establishing causation.

First, corporate criminal liability in Portugal is limited by Article 11, which excludes liability for negligent homicide and bodily harm. Furthermore, Articles 150 and 156 limit perpetrators to physicians or individuals legally authorized to perform medical procedures, excluding programmers, manufacturers, or developers, whether natural or legal persons. The inclusion of these offenses in Article 11 suggests that only clinical institutions could face liability for violations.

Second, the development, programming, production, and use of AI systems involve multiple actors, making it difficult (if not impossible) to pinpoint whose actions or omissions caused harm (Diamantis, 2021: 149).

If that were not enough, it is important to remember that, depending on the specific case and the type of offense under which it is analyzed, it will not always be possible to identify a human perpetrator who committed the act. This is because, despite the various theories seeking to determine the criminal-legal institution of the perpetrator and to distinguish it from forms of complicity, we must not forget that, at its most basic logical-grammatical level, the perpetrator is the one who performs the action – that is, who carries out the conduct corresponding to the meaning of the action described in the criminal offense, to be identified accordingly based on the interpretation of the typical verb[7].

When harm or danger arises not from deliberate misuse, design flaws, or human error but from the AI system's autonomous learning and decision-making, there may be no natural person who fulfills the actus described in criminal statutes (e.g., "injuring another person," "killing," or "endangering life or safety").

We do not advocate treating AI systems as criminally responsible entities. Rather, these gaps highlight the need to develop offenses tailored to today's AI landscape, encouraging heightened diligence during development, programming, production, use, and oversight.

The challenges in attributing human conduct as a basis for liability also affect corporate liability, particularly under vicarious models (Rodrigues, 2021: 127; Rodrigues, Sousa, 2021: 203ff). In systems linking corporate actions to those of leaders or subordinates, courts must identify the human act and its author to establish liability. This will not always be possible in AI contexts.

Consequently, self-liability models may better address these cases. In an ideal framework, courts would assess organizational defects (Januário, 2016: 175ff, Gómez-Jara Díez, 2015: 73) independently of AI flaws, evaluating policies, procedures, testing, supervision, transparency, and continuous improvement to determine whether an organization created excessive risk leading to harm or danger.

[7] From the theory of meaningful action adopted herein, and from the abstraction of the search for a "superconcept" of action, it inevitably follows the deconstruction of a general concept of the perpetrator, which will always depend on the specific type of crime and its interpretation (Canestraro, Januário, 2021: 225ff).

It remains too early to predict how Portuguese courts will approach corporate liability in AI-related cases under Article 11(2)(b), especially regarding "failures of supervision or control" by leaders. It is conceivable that these obligations could extend to algorithms and AI systems used or marketed by organizations. A more complex question, requiring further reflection, is whether courts will demand identification of an "intermediate human act" between the AI's harmful conduct and the leader's supervisory breach.

As for individual liability, AI introduces additional challenges due to its inherent unpredictability and opacity. These systems can autonomously interpret human actions, modify their own algorithms, and act in ways unforeseen by programmers, manufacturers, or users.

Legally, this unpredictability complicates causation and fault assessments. If neither programmers, manufacturers, nor users could reasonably foresee the AI's harmful conduct, the foreseeability requirement for establishing criminal liability may not be met (Januário, 2021: 160ff). As Roxin (2008: 1000-1001) notes, when an outcome is entirely unforeseeable or unavoidable, there is no legally relevant risk or causal link. Similarly, Figueiredo Dias (2007: 901) emphasizes that even in negligence, liability requires that harmful outcomes be at least foreseeable, which is often not the case with AI.

Opacity also raises difficulties regarding informed consent. As Flávia Siqueira (2020: 23) explains, patient autonomy includes "the right to make personal decisions about medical interventions," encompassing: (I) The right not to undergo treatment against one's will or without consent; (II) The right to choose treatments; (III) The right to refuse treatments, even if life-saving. The patient's free will is expressed through the indispensable free and informed consent, which not only legitimises the medical intervention but also creates for these professionals the duty not to obstruct the patient's will and not to interfere with their bodily integrity without providing all the necessary information for them to make an autonomous decision (2019: 128).

In the case of the Portuguese legal system, pursuant to Article 150 of the Penal Code, medical intervention for therapeutic purposes, when consented to, is not even deemed to constitute a criminal offence, as consent represents a genuine agreement between doctor and patient (Albuquerque, 2015: 573, Andrade, 2012: 457ff). Conversely, medical or surgical intervention carried out without valid and effective consent, although atypical from the perspective of personal injury, is addressed under Article 156, which, by establishing the offence of arbitrary medical and surgical interventions and treatments, clearly protects a specific dimension of personal freedom, namely the individual's right to self-determination over their own body (Andrade, 2020: 62-63).

However, what constitutes adequate information for valid consent? As previously noted, machine learning inputs and methods are rarely verifiable, and even when they are, their complexity makes it difficult for physicians (and especially patients) to understand them.

María del Carmen Gómez Rivero (2003: 83) argues that it is neither practical nor necessary to communicate every procedural detail, but only those essential for informed decision-making. Hilgendorf similarly states that clarifications should "enable the patient to assess the risks and benefits of the intervention and to make a self-determined decision based on the information provided to them" (Hilgendorf, 2019: 53). Article 44 of the Code of Ethics of the Portuguese Medical Association appears to follow a similar approach, providing that the duty of clarification must cover the diagnosis, therapy, and prognosis of the illness, and should, whenever possible, be carried out on a probabilistic basis and include the information necessary for the patient to make an informed decision. Likewise, the Portuguese Penal Code, in Article 157, stipulates that clarification will only be valid "when the patient has been duly informed of the diagnosis and of the nature, extent, and possible consequences of the intervention or treatment".

In cases where diagnosis or medical intervention is carried out through or with the assistance of AI, it appears essential that the patient be informed of such use, of the risks already known (Iagnemma, 2020: 443), and, insofar as possible, of the procedures applied by the AI. As Flávia Siqueira (2020: 29) explains when addressing the effects of the (non-)medical indication on the necessity of consent, its impacts are limited to the intensity of the duty of clarification, meaning that the less indicated a given intervention is, the greater the physician's obligation will be to share information and clarifications regarding contraindications and possible harmful effects.

If no further information is available regarding the reason for a particular diagnosis, or even regarding the hypotheses excluded by the algorithm, patients must be informed of this state of uncertainty, together with the potential benefits and possible adverse effects of the technology and the indicated treatment. The absence or insufficiency of such clarification undermines the validity of the patient's consent, constituting an arbitrary medical intervention or treatment, falling within the scope of Article 156 of the Portuguese Penal Code.

It is true that knowing whether most patients will trust the application of artificial intelligence systems in relation to their treatments is something that only empirical experience can reveal. However, with regard to their respective autonomy, the physician must, as far as possible, always clarify matters and allow patients to participate in decisions, since, as Luiz Carlos Lobo (2017: 190) reminds us, they will ultimately bear the consequences of medical decisions. It is for this reason that we do not foresee the complete replacement of this profession by artificial intelligence, even if it were to demonstrate higher success rates than humans, because, while the algorithm may be highly effective in explaining the know-what, the physician remains the only one capable of attempting to explain the know-why to the patient, thereby alleviating their distress.

Conclusion

As demonstrated in this article, artificial intelligence has great potential for application in the medical field, both through clinical and diagnostic support programmes, robotic equipment assisting in surgical interventions, and wearable devices that enable patient monitoring and minor interventions, as well as through the prediction of future illnesses and suicides.

However, while the healthcare sector is among the most promising in terms of applying these new technologies, on the other hand, due to the sensitivity of the data and the interests at stake, it is also one of the areas posing the most complex challenges for legal practitioners, requiring, from now on, careful reflection regarding regulation, patient and data protection, verifiability and transparency of procedures, and liability for any damages caused by AI systems.

Specifically with regard to criminal law, in the final chapter we observed that the opacity and unpredictability of AI, combined with its capacity for autonomous decision-making and the complexity of the sectors in which it is developed and operated, imposes unprecedented challenges on legal doctrine, particularly in terms of identifying the perpetrator and assessing the crime and culpability of natural and legal persons in most offences related to medical criminal law.

Therefore, in light of the expansion of AI in this and other sectors of society, it is necessary to revisit and reflect upon the general part of criminal law, so that some of its classical theories may be adapted in light of the scientific and technological realities expected in the coming decade. The scope and models of criminal liability for legal persons must be reconsidered, so that they are capable of addressing cases involving AI and serve as a tool to effectively promote corporate self-regulation and effective compliance programmes, which can not only collaborate with state activities to prevent, investigate, and repress unlawful conduct, but also, from a clearly privileged position, act in identifying and managing risks in this field and in defining competent action standards for the sector.

The dynamics of this field will put the subsidiary nature of criminal law to the test, with particular attention to primary risk-reduction norms, whether administrative rules, ethical and conduct codes, professional deontological standards, or sector-specific *leges artis*, capable of better monitoring technological and scientific developments and defining, more precisely and objectively, the permissible scope of human participants' conduct.

Finally, it should be noted that the undeniable risks arising from the application of AI in the medical field cannot justify non-compliance with criminal law regarding the act and the principle of culpability. By this, as obvious as it may seem, we mean that physicians, clinical and hospital institutions, and algorithm programmers cannot be held objectively liable solely on the basis of the function or position they occupy, when the damages and hazards in question – often unpredictable – cannot at least be attributed to them as negligence.

References

Albuquerque, P. P. (2015) Comentário do Código Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 3. Ed. Lisboa: Universidade Católica Editora.

Allain, J. S. (2013) From Jeopardy! to Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems, Louisiana Law Review, 73(4), pp. 1049-1079.

Andrade, M. C. (2012) Artigo 150º (Intervenções e tratamentos médico-cirúrgicos). In: Dias, J. F. (ed.) Comentário Conimbricense do Código Penal: Parte Especial: Tomo I: Artigos 131º a 201º, 2. ed. Coimbra: Coimbra Editora.

Andrade, M. C. (2020) Consentimento em direito penal médico – o consentimento informado. In: Estellita, H., Siqueira, F. (ed.) Direito Penal da Medicina. São Paulo: Marcial Pons, pp. 55-78.

Barresi, O. (2023) Italian Report on Traditional Criminal Law Categories and AI, RIDP, 94(1), pp. 269-302.

Bock, D. (2011) Criminal compliance. Baden-Baden: Nomos.

Burrell, J. (2016) How the machine 'thinks': understanding opacity in machine learning algorithms. Big Data & Society, 3(1).

Canestraro, A. C., Januário, T. F. X. (2018) Responsabilidade penal da pessoa coletiva e princípio da culpabilidade: análise crítica do modelo português, Revista da Faculdade de Direito da UFRGS, (39), pp. 261-285.

Canestraro, A. C., Januário, T. F. X. (2020) Concurso de agentes na perspectiva da teoria da ação significativa: um diálogo entre o sistema espanhol e o Projeto de Novo Código Penal Brasileiro, RBCCRIM, 29(178), pp. 213-244.

Chung, J. (2017) What should we do about artificial intelligence in health care?, Health Law Journal, 22(3), pp. 37-40.

Ćorić, D. (2021) Right to Life, Whatsoever Life Is, Yearbook Human Rights Protection: Right to Life, (4), pp. 55-64.

De La Cuesta Aguado, P. M. (2015) Riesgo e imputación: especial consideración de los riesgos derivados de la inteligencia artificial, Revista de Derecho Penal, (2), pp. 69-95.

Diamantis, M. E. (2021) Algorithmic Harms as Corporate Misconduct. In: Antunes, M. J. et al. (ed.) Artificial Intelligence in the Economic Sector: Prevention and Responsibility. Coimbra: Instituto Jurídico. pp. 135-164.

Engelhart, M. (2012) Sanktionierung von Unternehmen und Compliance: eine Rechtsvergleichende Analyse des Straf – und Ordnungwidrigkeitenrechts in Deutschland und den USA. 2. ed. Berlin: Dunkler & Humblot.

Engelhart, M. (2018) The Nature and Basic Problems of Compliance Regimes. Freiburg im Breisgau: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Fidalgo, S. (2009) Responsabilidade penal no exercício da medicina em equipa: o princípio da confiança e o princípio da divisão do trabalho. In: Andrade, M. C. et al. (ed.) Estudos em homenagem ao Prof. Doutor Jorge de Figueiredo Dias, vol. II. Coimbra: Coimbra Editora.

Frisch, W. (2004) Comportamiento típico e imputación del resultado. Madrid: Marcial Pons.

Gleß, S., Weigend, T. (2014) Intelligente Agenten und das Strafrecht, Zeitschrift für die gesamte Strafrechtswissenschaft, 126(3), 2014, v. 126, n. 3, pp. 561-591.

Gómez-Jara Díez, C. (2015) Responsabilidade penal da pessoa jurídica: a teoria do crime para as pessoas jurídicas. São Paulo: Atlas.

Gómez Rivero, M. C. (2003) La responsabilidad penal del médico. Valencia: Tirant lo Blanch.

Gouveia, S. S. (2019) O problema da lacuna de responsabilidade na Inteligência artificial. In: Curado, M. et al. (ed) Vanguardas da responsabilidade: direito, neurociências e inteligência artificial. Coimbra: Petrony.

Grandi, C. (2023) Positive Obligations (Garantestellung) Grounding Criminal Responsibility for Not Having Avoided an Il-Legal Result Connected to the AI Functioning. RIDP, 94(1), pp. 67-76.

Hallevy, G. (2010) The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control, Akron Intellectual Property Journal, 4(2), pp. 171-201.

Heberling, R. T. (2021) Right to Life – Right to Death?, Yearbook Human Rights Protection: Right to Life, (4), pp. 585-602.

Hilgendorf, E. (2019) Introdução ao direito penal da medicina. São Paulo: Marcial Pons.

Iagnemma, C. (2020) I ‘robot medici’: profili problematici in tema di alleanza terapêutica e di responsabilità penale, Corti Supreme e Salute, (2), pp. 441-458.

Januário, T. F. X. (2016) Da teoria do delito para as pessoas jurídicas: análise a partir da teoria construtivista de "autorresponsabilidade" dos entes coletivos, REJ UNESP, 20(32), pp. 161-191.

Januário, T. F. X. (2018) Criminal liability for legal entities: a comparative study between Spain, Portugal and Brazil, Polar – Portuguese Law Review, 2(2), pp. 191-224.

Januário, T. F. X. (2018) Dos limites do risco permitido para as pessoas jurídicas: uma análise do defeito de organização como um problema de imputação objetiva, Conpedi Law Review, 4(1), pp. 1-23.

Januário, T. F. X. (2019) Criminal compliance e corrupção desportiva: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal. Rio de Janeiro: Lumen Juris.

Januário, T. F. X. (2020) Inteligência artificial e responsabilidade penal no setor da medicina, Lex Medicinae, 17(34), pp. 37-63.

Januário, T. F. X. (2021) Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (high-frequency trading – HFT) à luz do ordenamento jurídico brasileiro. RBCCRIM, 29(186), pp. 127-173.

Januário, T. F. X. (2023) The Role of Compliance Programs in Preventing Age Discrimination: an Analysis in the Light of Brazilian Law 10.741/03. In: Pavlovic, Z. et al. (ed.) Elderly People and Discrimination: Prevention and Reaction. Belgrade, Novi Sad: Institute of Criminological and Sociological Research, Vojvodina Bar Association, pp. 375-388.

Januário, 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: Pavlovic, Z. et al. (ed.) The right to life and body integrity. Belgrade, Novi Sad: Institute of Criminological and Sociological Research, Bar Association of Vojvodina, pp. 425-429.

Januário, 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, (1), pp. 365-404.

Januário, T. X. (2022) Inteligência artificial e direito penal da medicina, in: Rodrigues, A. M. (coord.), A inteligência artificial no direito penal, vol. II. Coimbra: Almedina. pp. 125-174.

Kaplan, A., Haenlein, M. (2019) Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, Business Horizons, 62(1), pp. 15-25.

Jesus, T. C. (2019) Inteligência artificial: a responsabilidade civil do robô. In: Lima, A. P. C. et al. (ed.) Direito digital: debates contemporâneos. São Paulo: Thomson Reuters Brasil, pp. 43-54.

Lacaze, M., Walther, J. (2023) French Report on Traditional Criminal Law Categories and AI, RIDP, 94(1), 153-194.

Lascuraín, J. A. (2013) Compliance, debido control y unos refrescos. In: Arroyo Zapatero, L. et al. (ed.) El derecho penal económico en la era compliance. Valencia: Tirant lo Blanch.

Magro, M. B. (2020) Decisione umana e decisione robotica: un'ipotesi di responsabilità da procreazione robotica, Giustizia penale e nuove tecnologie, 8.5.2020, https://www.lalegislazionepenale.eu/wp-content/uploads/2020/05/Magro-Giustizia-penale-e-nuove-tecnologie.pdf, accessed on 13.9.2025.

Marks, M. (2019) Artificial Intelligence-Based Suicide Prediction, Yale Journal of Law and Technology, 21, pp. 98-121.

McCarthy, J. et al. (2006) A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine, 27(4), pp. 12-14.

McCarthy, J. (2007) What is Artificial Intelligence?. Stanford: Stanford University. https://www-formal.stanford.edu/jmc/whatisai.pdf, accessed on 12.9.2025.

Mulholland, C., Frajhof, I. Z. (2019) Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: Frazão, A. (ed.) Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil.

Navas Mondaca, I. (2013) Los códigos de conducta y el derecho penal económico. In: Silva Sánchez, J. M. et al. (ed.) Criminalidad de empresa y compliance: prevención y reacciones corporativas, Barcelona: Atelier.

Pavlović, Z. (2022) Protecting the Rights of the Unborn Child, Yearbook Human Rights Protection: from childhood to the right to a dignified old age: human rights and institutions, (5), pp. 257-273.

Pereira, A. G. D. (2019) O médico-robô e os desafios para o direito da saúde: entre o algoritmo e a empatia. Gazeta de Matemática, LXXX (189), pp. 30-34.

Pereira, A. G. D. (2021) Inteligência artificial, saúde e direito: considerações jurídicas em torno da medicina de conforto e da medicina transparente. Julgar, (45), pp. 235-261.

Pereira, A. L. D. (2018) Big-data, e-health e "autodeterminação informativa": a Lei 67/98, a jurisprudência e o regulamento 2016/679 (GDPR). Lex Medicinae, 15(29).

Piccotti, L. (2023) Resolution on traditional criminal law categories and AI, RIDP, 94(1), pp. 53-59.

Price II, W. N. (2017) Artificial Intelligence in Health Care: applications and legal issues. U of Michigan Public Law Research Paper No. 599.

Rodrigues, A. M. (2021) The Last Cocktail – Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence. In: Antunes, M. J. (ed.). Artificial Intelligence in the Economic Sector: Prevention and Responsibility. Coimbra: Instituto Jurídico, pp. 119-133.

Rodrigues, A. M., Sousa, S. A. (2021) Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal, Julgar, (45), pp. 193-214.

Roxin, C. (2008) Derecho Penal: parte general: tomo I: fundamentos. La estructura de la teoria del delito. Madrid: Civitas.

Siqueira, F. (2019) Autonomia, consentimento e direito penal da medicina. São Paulo: Marcial Pons.

Siqueira, F. (2020) O paradigma de respeito à autonomia do paciente e suas implicações no direito penal da medicina: em especial sobre a ilegitimidade das intervenções médicas arbitrárias. In: Estellita, H. et al. (ed.) Direito Penal da Medicina. São Paulo: Marcial Pons, pp. 19-54.

Sousa, S. A. (2020) "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial. Rodrigues, A. M. (ed.) A inteligência artificial no direito penal, vol I. Coimbra: Almedina.

Souza, C., Oliveira, J. (2019) Sobre os ombros de robôs? A inteligência artificial entre fascínios e desilusões. In: Frazão, A. (ed.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil.

Steibel, F. et al. (2019) Possibilidades e potenciais da utilização da inteligência artificial. In: Frazão, A. et al. (ed.) Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil.

Stone, P. et al. (2016) Artificial Intelligence and life in 2030: one hundred year study on Artificial Intelligence. Report of the 2015-2016 Study Panel. Stanford: Stanford University.

Terrizzi, L. (2023) Medical devices e diritto penale: profili di responsabilità del produttore e dell'utilizzatore. Milano: Giuffrè.

Wimmer, M. (2019) Inteligência artificial, algoritmos e o direito um panorama dos principais desafios. In: Lima, A. P. C. et al. (ed.) Direito digital: debates contemporâneos, São Paulo, Thomson Reuters Brasil.