Criminal–Judicial Challenges and Limitations Concerning Emerging Crimes Committed by Robots or Artificial Intelligence

1. Hayder Kareem Abbood Al-Jizani: Ph.D. student in Public Law, Department of Public Law, Isf.C., Islamic Azad University, Isfahan, Iran
2. Masoud Heidari*: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran
3. Hayder Hussein Ali: Department of Law, Faculty of Law, University of Karbala, Karbala, Iraq
4. Yasin Saeedi: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran

*Correspondence: heidari5525@iau.ac.ir

Abstract

With the rapid advancement of technology and the integration of artificial intelligence (AI)–equipped robots into various aspects of human life, new legal challenges have emerged that previously did not exist—particularly those relating to the criminal liability of AI systems, especially in cases where such systems are implicated in the commission of crimes and accusations are directed toward AI-based entities. This is precisely the issue addressed in the present study, which seeks to provide a comprehensive and holistic perspective on the developments and legal deficiencies associated with the criminal responsibility of robots. Through the analysis of existing legal frameworks in this area, the study examines the overarching concept of robots and the related legal and technological transformations. It focuses on how robots may become involved in intentional or unintentional offenses and seeks to identify the potential legal responsibility of designers, developers, and users of these systems. The findings of this research indicate that current laws suffer from ambiguity and inadequacy in determining the exact nature of liabilities arising from the conduct of AI-driven robots, which in turn leads to confusion and weakens the administration of criminal justice. Challenges such as evidentiary difficulties in proving technology-based crimes, protecting the rights of victims of robotic offenses, distinguishing between human and machine intent, assigning responsibility in the absence of direct human control, determining the role of corporations in the design and operation of robots, resolving conflicts between legal principles and modern technologies, defining the liability of robot users or owners, and the absence of a clear legal definition of the "agent" in robotic crimes are discussed within this framework.

Keywords: criminal challenges, criminal liability, robots, cybercrime, artificial intelligence

Received: 17 May 2025
Revised: 01 September 2025
Accepted: 09 September 2025
Initial Publish: 22 October 2025
Final Publish: 01 January 2026

Citation: Al-Jizani, H. K. A., Heidari, M., Hussein Ali Ali, H., & Saeedi, Y. (2026). Criminal–Judicial Challenges and Limitations Concerning Emerging Crimes Committed by Robots or Artificial Intelligence. *Legal Studies in Digital Age,* 5(1), 1-11.

1. Introduction

Since the mid-twentieth century, the world has witnessed profound and wide-ranging transformations that have remarkably reshaped the face of human life. The information revolution has fundamentally reconstructed various aspects of existence, generating a qualitative leap in the structure of societies and in the ways humans interact with their surroundings. Within this process of continuous advancement, artificial intelligence (AI) has emerged as a prominent technological force, attaining a central position and permeating all dimensions of daily life while exerting an increasing influence across diverse domains and applications (Caliskan et al., 2021; Chen et al., 2020).

The impact of AI is not confined merely to economic or technical dimensions but extends to intricate legal issues, particularly the question of liability for crimes that may be committed by or through such technologies. Although the primary purpose of AI development is to enhance human life quality and increase efficiency, the growing autonomy of AI systems raises deep and critical questions regarding the possibility of assigning legal responsibility to intelligent systems for harmful acts or even for direct and indirect offenses—since these systems can learn autonomously and make independent decisions without continuous human intervention (Al-Sherbiny, 2021).

This reality renders the application of traditional concepts of criminal liability—rooted in the moral element of human awareness and volition—extremely difficult, as AI operates on complex algorithms that process vast quantities of data in real time. This circumstance gives rise to new challenges in determining who should bear responsibility for crimes committed by such systems. The central question thus arises: Is liability to be attributed to the AI system itself, or to the programmer, the manufacturer, or the user? (Amish, 2021).

These inquiries emerge in a context where the existing legal framework is incapable of responding to these novel demands, as traditional rules of criminal responsibility are inadequate to address such offenses—especially considering the internal complexity and rapid decision-making capacity of intelligent systems (Al-Sherbiny, 2021). These challenges necessitate a fundamental reconsideration of the legal system and a re-evaluation of the need to develop modern criminal rules consistent with the nature of these technologies and aligned with the pace of their evolution (Al-Falasi, 2023; Al-M'ebid, 2024).

The objective of this study is to provide a deep legal analysis of criminal liability arising from robot-related crimes through an examination of existing gaps in legal systems, an exploration of potential legislative solutions to address these deficiencies, an evaluation of relevant jurisprudential opinions, and a review of comparative legal positions to present a comprehensive and reliable framework. This is particularly important as robots equipped with AI systems have become an inseparable part of modern life, and their use in medical, industrial, and security fields has become an undeniable reality (Abu al-Eid, 2024; Al-Maghrabi, 2023).

This development calls for systematic legal regulation and analysis of the implications of such phenomena, as humanity has transitioned from an era in which crimes were committed exclusively by human agents to one where robots can play active roles in acts capable of causing serious harm to individuals or property. The fundamental question thus becomes whether these intelligent systems themselves can be held criminally responsible or whether liability should be directed toward their creators, developers, or controllers—particularly in sensitive fields such as medicine, where programming errors in surgical robots have caused substantial harm, or in autonomous vehicles that have resulted in fatal accidents (Al-Hasanat, 2024; Al-Zawwi, 2024).

These cases raise serious concerns, as traditional rules of criminal liability provide inadequate coverage for such situations, compelling a profound re-examination of the concept of the "actor" in the era of intelligent systems and their growing independence in decision-making. In the current context, reliance on conventional rules to address acts originating from non-human systems is no longer feasible—especially given their increasing predictive capabilities and their capacity for complex autonomous decision-making (Calo, 2015, 2016). The absence of legal frameworks will ultimately lead to legislative vacuums and, consequently, to legal disorder in the future. Therefore, the purpose of this study is to examine the criminal–judicial challenges and limitations associated with emerging crimes committed by robots.

2. Concepts and Theoretical Foundations

2.1. Robot

Etymologically, the term *robot* derives from the Czech word *robota*, meaning "forced labor," first introduced in Karel Čapek's 1921 play *R.U.R. (Rossum's Universal Robots)* to refer to beings that executed commands without perception or independent will (Čapek, 1921).

Terminologically, a robot is defined as an artificial entity designed to perform specific tasks according to preprogrammed instructions or semi-autonomous sensory responses, possessing a high degree of automation and capable of interacting with its environment without continuous human involvement (European Commission, 2020).

In legal contexts, however, the definition of robots has significantly expanded to include entities possessing advanced autonomy. The European Parliament, for instance, has characterized such robots as intelligent and self-directed entities capable of limited perception and environmental adaptation through learning algorithms—features that qualify them for inclusion within a novel legal framework referred to as "electronic personality" (European Parliament, 2016).

Considering the multiplicity of definitions proposed for the concept of the robot, a comprehensive definition in criminal law may describe it as "a technological and relatively autonomous system that interacts with its environment according to intrinsic programming or prior human instruction, endowed with an advanced capacity for decision-making that may exhibit automation and dynamic adaptability." These features create a legal gap between the act performed by the robot and the criminal responsibility attributable to it—a system possessing a hybrid nature that shares the ability to act with humans but lacks moral volition. This necessitates the adoption of modern and dynamic legal approaches capable of balancing the technological nature of such systems with the criminal implications of their conduct (Al-Hamrawi, 2021; Ibrahim, 2023).

2.2. Artificial Intelligence

Artificial intelligence refers to a programmed entity with varying degrees of decision-making autonomy and a limited ability to interact and adapt to its environment. It has been defined as a technology that enables computers to simulate human cognitive abilities such as learning, comprehension, problem-solving, decision-making, creativity, and independence (IBM, 2024). It is also described as an automated system capable of issuing recommendations or decisions—within human-defined objectives—that affect real or virtual environments (Jonker & Rogers, 2024). AI may also be understood as the simulation of human thinking processes by systems designed to act like humans, performing functions such as understanding, planning, and forecasting (PMC, 2019).

2.3. Cybercrime

Among the most pressing issues confronting the global community today is the cyber domain—a virtual world that has evolved into a parallel reality to the physical one (Al-Duwaik, 2019). Cybercrimes are defined as acts committed via the Internet, including the deletion or destruction of data within a computer or network system, or both (Al-Hawāmidah, 2017). They have also been described as deliberate acts of sabotage or interference targeting electronic systems, potentially resulting in death or harm to individuals or groups, significant damage to physical property, disruption of civil relations, or severe economic loss (Mourlam, 2016). Another definition characterizes them as any harmful or unlawful act intended to alter, delete, add, process, steal, distort, or manipulate data through a computer or other technological means for illegitimate purposes (Giles, 2018).

3. Challenges in Aligning Existing Laws with the Criminal Liability of Robots

Current legal frameworks face substantial challenges in adapting criminal liability to robots, owing to the advanced technical nature of robots and artificial intelligence—features that extend beyond the traditional criminal-law paradigm premised on the assumption of a "rational and aware human actor." The most salient challenges can be summarized as follows:

First: Absence of legal personality for robots. Traditional criminal statutes regard the actor as either a natural or a legal person, whereas robots lack independent legal personality—rendering the direct attribution of criminal liability to them difficult and complex (Abdullah & Zangana, 2023).

Second: Ambiguity in allocating responsibility among human parties. Where an offense is committed by a robot, the question arises: Who is responsible—the programmer, the manufacturer, the owner, or the user? In many legal systems, there is a legislative gap regarding the precise allocation of criminal liability among these parties, which results in a lack of legal clarity.

Third: Lack of explicit provisions addressing crimes arising from robots. Many laws do not contain express rules criminalizing the design or modification of robots for the purpose of committing offenses (Al-Zawwi, 2024). Moreover, specific penalties are often not prescribed in this area, which limits the judiciary's ability to address such crimes effectively.

Fourth: Technical challenges in proving robotic fault. Robots typically operate on complex algorithms; accordingly, determining whether fault or negligence exists is highly challenging. This is especially true where a robot's behavior stems from its autonomous decision-making, which further complicates the proof of criminal liability (Bin Awda, 2022).

Fifth: Confronting crimes involving medical robots. This field raises numerous ethical and legal challenges in determining criminal liability for errors committed by medical robots, particularly when such errors cause severe injury or even the death of patients (Al-Maghrabi, 2023). This necessitates enacting legal rules that are novel, clear, flexible, and precise—rules that respond to technological developments while avoiding misguided ijtihād (Abu al-Eid, 2024).

Sixth: Legislative vacuums in some countries. Certain jurisdictions still lack specialized legislation governing the criminal liability of robots (Ibrahim, 2023). This places courts in a difficult position when confronting emerging offenses. Under such conditions, allocating responsibility between developers and users requires a redefinition of traditional concepts of legal liability. Consequently, new legal frameworks must be designed to account for advances in AI and machine learning. Judicial systems should offer innovative solutions that protect individual and societal rights without stifling innovation in robotic technologies.

3.1. Non-Alignment of Existing Criminal Laws with Robot Crimes

The misalignment of criminal statutes with robot-related offenses produces serious legal gaps that significantly affect the protection of individual rights and public security. Traditional criminal laws—drafted on the premise of a human actor endowed with reason and will—are ill-suited to address newly emergent offenses involving robots, because these technological entities lack will and awareness and cannot readily be fitted into classical criteria of criminal responsibility. The principal challenges arising from this non-alignment may be explained as follows:

First: Lack of independent legal personality for robots. Under the classical structure of criminal liability, only natural or legal persons can bear liability; robots, as entities without cognition or criminal intent, cannot have criminal responsibility attributed to them. They operate solely on algorithms that are either preprogrammed or learned autonomously, lacking intent or awareness (Amish, 2021).

Second: Complexity in proving fault and mens rea. Within criminal law, liability is realized when a clear relationship is established between the criminal act and the perpetrator's intent. Given the data-driven complexity of robotic operation, determining whether criminal fault or intent existed is exceedingly difficult; moreover, robotic decisions may result from machine-learning processes or environmental responses, further complicating the attribution of responsibility.

Third: Multiplicity of human actors in the liability chain. In many instances, it is not straightforward to identify which human actor—programmer, manufacturer, owner, or user—should be held responsible. The absence of explicit legal provisions differentiating these responsibilities creates legislative gaps and complicates the identification of the principal actor (Al-Rubai'i, 2024).

Fourth: Absence of explicit and comprehensive criminal provisions concerning robot-related offenses. In most criminal law systems, statutes specifically addressing robot-related crimes have yet to be enacted. Even cybercrime laws often fail to provide sufficient coverage for offenses arising from robotic performance, thereby limiting the judiciary's capacity to adjudicate these cases effectively.

Fifth: The "black box" problem in AI decision-making. AI systems—particularly those operating through deep learning—are often treated as "black boxes," meaning that even developers may lack precise understanding of their decision-making pathways. This renders the identification of technical errors or the attribution of criminal liability exceedingly difficult (Burrell, 2016).

Sixth: Lack of jurisprudence and practical experience. The paucity of judgments and case law concerning robot-related crimes is a serious obstacle to the development of a reliable judicial understanding. As a result, judges facing novel cases may lack interpretive tools to align existing rules with new facts, which in turn hinders the gradual evolution of the criminal justice system in this area.

3.2. Absence of a Clear Definition of the "Actor" in Robotic Crimes

This concept refers to the lack of a clear legal definition of the legal or institutional personality that may be deemed the actor in offenses committed by robots or intelligent systems. The absence of such a definition generates a major difficulty within the structure of criminal law because it renders the attribution of criminal responsibility for harmful acts committed by robots highly problematic. This situation encompasses a set of challenges that can be categorized as follows:

First: Complexity in identifying the actor among human participants. In crimes involving robots, the primary difficulty lies in determining the true actor. Is it the programmer who designed the robot, the user who deployed it, or the manufacturer who produced it? The multiplicity of stakeholders—and the absence of explicit statutory provisions—makes the attribution of criminal responsibility highly complex (Al-Falasi, 2023).

Second: Treating the robot as a tool or intermediary, not an independent actor. Some scholars contend that a robot is not an autonomous actor but merely a tool in human hands; consequently, legal and criminal liability should be assigned to the human controller. However, given the capacity for autonomous learning in some robots, behaviors may emerge that are unpredictable and independent—thereby challenging the notion of the robot as a mere instrument.

Third: Difficulty proving the mental element of criminal intent. In criminal law, establishing the mental element (mens rea) is fundamental to liability; robots, however, possess neither intent nor cognition and act only according to algorithms or input data. As a result, proving criminal intent in such cases is difficult or impossible, producing a legislative gap when attempting to align traditional criminal rules with these circumstances.

Fourth: Technical and legal challenges in collecting criminal evidence. The lack of a precise definition of the actor in robot-related crimes complicates the processes of evidence gathering and analysis. Issues such as how to conduct a technical inspection of a robot, analyze its software, or extract digital data to understand its complex behaviors introduce significant ambiguity into investigation and adjudication (Amish, 2021).

3.3. Ambiguity in Allocating Fault Between the Human and the Intelligent System

Ambiguity in allocating responsibility between the human individual and the intelligent system—particularly with respect to offenses or harms arising from the operation of such systems—constitutes a serious and complex challenge due to their distinctive nature, which combines human programming with autonomous decision-making. This ambiguity can be analyzed as follows:

First: Multiplicity of human parties and the distribution of responsibility. When harm arises from an intelligent system, disputes frequently concern whether responsibility lies with developers (programmers), where the error may stem from algorithmic flaws or bias in training data; with operators (companies or entities responsible for oversight and safety); or with end users when misuse occurs or when unpredictable behaviors arise. The clearest example is smart-vehicle incidents, in which fault may be distributed among algorithm designers, manufacturers, and drivers—yet traditional law does not clearly delineate how such responsibility should be allocated (Lagioia & Sartor, 2019).

Second: Lack of legal personality for intelligent systems. In criminal law, liability is built upon two elements—mens rea and the criminal act—both of which presuppose human will and awareness. Intelligent systems lack such will and awareness and cannot, as entities possessing independent legal capacity, be prosecuted or punished. This legal gap is particularly evident where harmful acts occur without direct human intervention, such as in the operation of self-learning medical robots.

Third: Conflicts among national and international approaches. States have adopted divergent approaches to AI-related liability. Within the European Union, there is emphasis on strict liability for manufacturers when intelligent systems fail, whereas in the United States, tort-based rules predominate and the burden of proving fault generally rests with the injured party. In many Arab countries, however, explicit legislation is still lacking; ambiguity in allocating responsibility between human actors and intelligent systems has opened a gap between technological growth and legal response—necessitating flexible legislative frameworks that recognize AI's distinctive features while strengthening international cooperation to harmonize global legal standards (Ablhad, 2023).

3.4. The Position of the Robot User or Owner's Liability

When addressing the criminal liability of a robot's user or owner, it must be recognized that we are dealing with a complex legal issue whose importance grows daily with the advancement of intelligent and robotic technologies. The criminal liability of a robot's user or owner represents one of the fundamental and central topics in assessing legal responsibility related to artificial intelligence and robotic technologies, as law faces serious difficulties in determining who must answer for damages or crimes arising from such systems.

A clear distinction should be made between the owner of the robot and its practical user, since in some cases, another person may use the robot on a daily basis—such as a factory worker or an individual operating a medical robot. In such situations, liability may not be clear, particularly when the user lacks the necessary technical knowledge or adequate understanding of how the robot operates. Therefore, it is essential that users be aware of the robot's operational limits and how to respond to emergency conditions or technical malfunctions, since if an accident occurs due to carelessness or misuse on their part, the responsibility will rest directly upon them.

Accordingly, the establishment of clear legal frameworks prescribing penalties for negligence or misuse by users or owners has become an unavoidable necessity (Al-M'ebid, 2024).

3.5. The Conflict Between Legal Principles and Modern Technologies

This conflict is not limited to the tension between traditional legal rules and new technologies but extends to a deeper clash between fundamentally different conceptual systems regarding the notions of agency and legal accountability. The "black-box" problem exemplifies this tension, as it threatens transparency and justice: AI algorithms are often opaque and, at times, even unknown to their own programmers. This situation clearly contradicts legal principles that require clarity of motive, criminal intent, and the victim's right to know the cause and circumstances of harm. Consequently, the current legal order faces a profound challenge in realizing justice—especially when robotic actions are not interpretable or when owners and users cannot explain the robot's behavior (Burrell, 2016).

Artificial intelligence represents a hybrid of human and machine agency. Modern robots are no longer passive tools but hybrid entities blending human programming with autonomous learning and environmental adaptability. This contradicts the civil-law principle of the *instrument*, which holds that a tool bears no liability and that responsibility lies solely with the human user. Yet, in the case of robots, harmful behavior may result from independent decision-making. Law therefore confronts a fundamental dilemma: Should a robot be regarded as a mere instrument, as an independent actor, or as an entity with partial liability? This complexity demands a re-evaluation of traditional classifications of legal responsibility (Caliskan et al., 2021).

In adapting legal norms to the accelerating pace of technological change, the inherent stability and generality of legal principles often contrast sharply with the astonishing speed of technological innovation. This temporal gap between legislation and application produces legal vacuums that can be exploited or used to evade accountability. Such tension necessitates the creation of more flexible legislative mechanisms—such as updateable or dynamic laws—that evolve alongside technological transformation (Calo, 2015).

3.6. The Principle of the Personal Nature of Criminal Responsibility

The principle of the personal nature of criminal responsibility is one of the fundamental tenets of criminal law. It holds that criminal liability applies only to individuals whose intent or will to commit an offense can be proven. This means that a person

may be prosecuted only for acts personally performed or in which they effectively participated, and—except in legally specified exceptional cases—not for the acts of others. The principle is based on the idea that punishment must be imposed solely upon one who, by their own free will and awareness, committed or contributed to the offense, without extending liability to innocents or relatives.

However, with the advent of AI-related crimes and the technological revolution, an essential question arises: Can this principle of personal responsibility be applied to harms caused by autonomous systems such as self-driving vehicles, where determining the true actor is exceedingly difficult? Although the principle of personal criminal responsibility remains the cornerstone of criminal justice, it now faces technical and conceptual challenges due to collective or technologically mediated offenses (Darwish, 2025).

3.7. Challenges in Proving Technology-Based Crimes

In a world where AI and robots have become integral to modern life, proving crimes committed by robotic systems poses a fundamental challenge for judicial institutions. This difficulty is intertwined with traditional concepts such as criminal intent (*mens rea*) and causality—concepts that are difficult to identify or establish within the context of machine intelligence. In some instances, errors in algorithmic self-learning may result in harmful acts without direct human involvement or prior intent, thereby eroding the traditional notion of intent and creating a novel situation that requires new evidentiary tools (Smejkal & Kodl, 2021).

To bridge this evidentiary gap, the establishment of a comprehensive *digital audit trail* system is proposed, allowing the traceability of AI system decisions. The use of *digital-twin* technology to reconstruct technical events is also recommended, since the nonlinear nature of machine learning complicates the causal link between act and harm. These considerations suggest that the burden of proof should shift away from the victim and toward the manufacturer, developer, or operator—focusing on system accountability rather than individual intent or negligence (Hamon et al., 2022).

In analyzing criminal-law concepts, it is also necessary to acknowledge the complex structure of the digital age, including AI and robotic systems. This necessitates a rethinking of the concept of intent, as the classical understanding of *mens rea* as a reflection of human awareness can no longer explain robotic behavior—particularly in cases of self-learning error. In such conditions, not only does intent vanish, but its legal meaning collapses, producing an epistemic and legislative vacuum.

3.8. The Role of Courts in Interpreting New Laws

The judiciary bears a vital responsibility in filling the legislative gaps arising from the emergence of robots and AI technologies. Traditional statutes were drafted within a framework understandable only through human acts, whereas behaviors stemming from technological entities rely on algorithms that demand novel interpretation to bridge existing legal voids.

In this context, the Supreme Court of Canada issued a landmark judgment discussing how the "effective-cause" principle could be applied to damages arising from a self-driving vehicle, even in the presence of direct human intervention. In that ruling, the Vehicle Safety Protection Act was interpreted to encompass two scenarios: defective system design and unpredictable environmental reactions—illustrating the courts' capacity to fill legislative gaps (Chen et al., 2020). Similarly, European Union courts have integrated ethical and technical principles into their legal interpretations, with many judgments of the Court of Justice of the European Union reflecting a broader technological perspective in addressing AI-related laws.

Thus, judicial interpretation is no longer confined to the letter of the law but extends to its spirit—whose ultimate aim is to realize justice in an era of technological transformation. Nonetheless, courts still face major challenges: they must move beyond traditional interpretive styles to deliver rulings capable of addressing unprecedented technological realities. Hence, the judiciary can be viewed as an effective instrument for aligning criminal law with modern phenomena such as robotic behavior, which resists classical definitions of criminal liability (Al-Hasanat, 2024).

Despite this, the judicial apparatus encounters real obstacles, including insufficient technological expertise and a lack of relevant case law—factors that make interpretation difficult, ambiguous, and sometimes contradictory. There is therefore an urgent and fundamental need to enhance judges' technical knowledge or to integrate specialized experts into the judicial

structure through a coherent program, since courts' interpretive roles extend beyond explaining existing statutes to formulating new understandings of liability in the digital context—balancing legal stability with the acceptance of technological innovation.

3.9. The Challenge of Protecting Victims of Robotic Crimes

Protecting victims of crimes involving robots presents unprecedented legal difficulties, especially given the challenge of determining liability. Studies indicate that 60% of victims face serious barriers to obtaining justice—obstacles stemming from legislative gaps and the multiplicity of actors involved, including manufacturers, programmers, and operators, which together render the attribution of criminal liability particularly complex (Janahi, 2024).

To ensure the protection of victims of offenses committed by robots—especially in contexts involving autonomous AI algorithms—human oversight must be seriously considered. In this era of technological transformation, reliance on traditional justice models grounded in the conscious and rational human actor is no longer sufficient. Thus, an urgent need arises to redefine both evidentiary tools and liability standards (Al-Hasanat, 2024).

Furthermore, the evolving nature of the human-technology relationship requires law to embrace a broader and more flexible conception of victim protection—one that encompasses not only unjust automated decisions but also establishes robust criteria for both direct and indirect liability, particularly in response to the growing number of technology-driven criminal cases.

3.10. The Effect of Automated Decision-Making on Proof of Crime

Automated, algorithm-driven decisions pose a fundamental challenge to traditional systems of criminal proof. Within this framework, the concept of "digital evidence" becomes one of the essential pillars of evidentiary practice—especially in the absence of conventional indicia such as observable behavior or a clearly identifiable human perpetrator. In this respect, digital logs may be regarded as a mirror reflecting the decision-making process and may be used to reconstruct the circumstances of the act's commission. Nevertheless, this effort faces significant technical difficulties, notably because these systems' internal logic is frequently obscured by the "black box," which hides the rationale of algorithmic decision-making from view (Burrell, 2016). Consequently, research and the development of analytical tools capable of correctly interpreting the logic of algorithms are required—steps that would strengthen the credibility of proof. It is no longer sufficient to rely solely on traditional indicia; rather, a deep understanding of "machine will," verification histories, and the interactive contexts in which decisions are made must be brought to bear. This can only be achieved through full convergence and harmonization between criminal investigative methodologies and modern technologies—an alignment that supports accurate and impartial judicial rulings and prevents the conflation of human volition with machine volition (Hamon et al., 2022; International Organization of Supreme Audit Institutions, 2023).

3.11. The Challenge of Distinguishing Human Will from Machine Will

Discerning human will from machine will is foundational to understanding the human–machine relationship within the framework of criminal responsibility. This challenge began with the advent of algorithms capable of adopting autonomous decisions without direct human intervention—thereby creating uncertainty in pinpointing the precise source of will and action: Is the behavior the product of human awareness, or is it the natural result of an independently configured program exhibiting a level of learning complexity? Such behavior raises serious questions about the limits of responsibility and the possibility of attributing outcomes to a robot that operates beyond direct human oversight. This ambiguity is especially acute in environments reliant on generative AI, where systems are configured to produce outputs over which humans may lack prior control or direct awareness. This development confronts legislators with a conceptual and legal impasse, insofar as the presumption of "machine will" conflicts with the traditional criminal-law concepts of intent, awareness, and deliberation. Although there may appear to be a functional resemblance between human intent and the "intent" of an intelligent system, a decisive difference lies in the absence of moral purpose in the latter—an absence that deprives the act of the uniquely human evaluative dimension (Lubab, 2023).

3.12. Responsibility in the Absence of Direct Human Control

In light of the growing autonomy of intelligent robots, the traditional legal system faces a serious challenge: assigning criminal responsibility where direct human oversight is absent. When the human element is removed from the decision-making loop in certain automated systems, a complex legal situation arises in which it is difficult to link the criminal behavior to a prosecutable actor under classical criminal-law frameworks—a situation that may be described as a "causal vacuum." Emerging legal tendencies propose redefining the human–machine relationship under a "legal guardian" model, whereby responsibility is assigned to the developer or operator of the robot, even in the absence of direct oversight or classical criminal intent. This evolution requires rethinking traditional principles of criminal responsibility and developing more flexible legal models (European Commission, 2020; Ibrahim, 2023). On this basis, some comparative systems have turned to forms of objective liability to fill the gap, placing the burden of proof upon the technical parties involved, such that an algorithmic defect or inadequate security updates is treated as a sufficient basis for liability—an approach designed to strengthen victim protection and to balance criminal justice with technological progress (Al-Zubaidi & Shahin, 2024; Lagioia & Sartor, 2019).

Undoubtedly, this orientation is a sound and necessary step, particularly at this sensitive juncture preceding the consolidation of comprehensive and robust legislation in this field.

3.13. The Challenge of the Corporate Role in Designing and Operating Robots

Corporate intervention in the design and operation of robots is a central axis within the broader framework of legal responsibility. Such entities—including developers, programmers, and hardware manufacturers—occupy a pivotal position in the technical and operational ecosystem of robotic production. Companies are viewed not merely as producers of new technologies but as legal actors from whom criminal or civil consequences may flow if robotic products cause direct or indirect harm in the course of their functions. Negligence in algorithmic design or the absence of preventive assessment standards can give rise to legal liability for these companies, particularly where mechanisms for risk assessment in public or sensitive environments have been disregarded (Janahi, 2024).

In addition, a lack of transparency in a robot's internal programming weakens traceability and thereby generates profound legal difficulties for courts attempting to attribute responsibility precisely. Much contemporary legal scholarship emphasizes that allocating responsibility among actors (companies, users, programmers) requires a fundamental re-examination of traditional attribution rules. Corporate responsibility for any failure to provide adequate safety measures for robots—or for ignoring foreseeable misuse or uncontrolled autonomous evolution—must be scrutinized (Al-Hamrawi, 2021; European Commission, 2020).

The burden of proof in this domain becomes heavier where design lacks clear ethical or legal boundaries; in such cases, companies may be found responsible for gross negligence or weak technical control. Assigning responsibility in a multi-actor environment requires the development of new legal foundations. Contractual provisions between manufacturer and user are not, by themselves, sufficient to guarantee justice in distributing losses; rather, binding regulations should require technical disclosures and regular assessments of intelligent technologies. Corporate legal accountability should not be confined to the production stage, but must also encompass ongoing oversight of software updates and of their interaction with the surrounding environment (Hamon et al., 2022; IBM, 2025).

4. Conclusion

This study aimed to examine the criminal and judicial challenges and limitations related to emerging crimes committed by robots or artificial intelligence. It can be concluded that the current and traditional model of crime—based on the material and moral elements—is incapable of comprehending the unique and distinct nature of robots that possess independent decision-making ability. This reality necessitates a complete reconstruction of criminological theory rather than a mere revision of existing statutory texts.

Furthermore, the absence of clear boundaries between criminal fault, technical error, and industrial malfunction in robot-related crimes calls for the development of new models of liability that integrate both criminal and technical responsibility.

Traditional punishments such as imprisonment and fines are ineffective for non-sentient entities incapable of experiencing pain or deprivation; therefore, technological penalties compatible with the electronic nature of AI robots must be designed.

Additionally, preventive oversight remains weak at the programming and design stages, as most existing systems focus primarily on end-use control while neglecting preventive measures within the production chain—an omission that increases the likelihood of technological crimes.

Existing laws fail to provide adequate legal solutions for situations in which robots act beyond human control, resulting in a phenomenon known as the "causal vacuum," where it becomes difficult to link an act to a specific legal actor. In this regard, an act should hypothetically be attributed to the closest human agent who could have foreseen the outcome, utilizing innovative concepts such as "reversed causality presumption."

There is an urgent need for new methods of criminal proof—such as tracing algorithmic decision-making histories, employing *digital twin* reconstruction techniques, and conducting scientifically rigorous algorithmic analyses—because traditional evidentiary tools cannot grasp the technical complexity of AI robots. Such evidence must be examined by qualified technical–legal experts and safeguarded against software manipulation.

The current legal system must establish new models of responsibility that combine absolute and personal liability for producers, programmers, and users, particularly in high-risk domains such as healthcare and financial transactions.

Finally, there is a pressing necessity for the creation of a continuous and effective operational oversight mechanism that monitors intelligent robots throughout their lifecycle—not merely during design and development phases—to ensure sustained control over the behaviors of intelligent systems.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abdullah, A. K., & Zangana, M. A. (2023). Criminal Liability for the Use of Robotic Devices: A Comparative Study. *Al-Farabi Journal for Human Sciences*, *2*(2).

Ablhad, F. (2023). *Artificial Intelligence from Concept to Legal Challenges*.

Abu al-Eid, T. A. (2024). *Legal Aspects of Medical Robots*. International Academy for Mediation and Arbitration.

Al-Duwaik, A. U. (2019). *Cyber Crises and Wars: Threats Beyond the Electronic Judiciary System*. Saqr Center for Studies, Iraq.

Al-Falasi, A. A. M. (2023). *Criminal Liability Arising from Artificial Intelligence Errors*.

Al-Hamrawi, H. M. O. (2021). The Foundations of Robots' Civil Liability Between Traditional Rules and the New Approach. *Journal of the Faculty of Sharia and Law, Tanta University*, *23*(8), 3059-3102.

Al-Hasanat, H. K. H. (2024). Criminal Liability Arising from Artificial Intelligence Errors. *Al-Zaytoonah University of Jordan Journal for Legal Studies*, *43*(4), 1849-1952.

Al-Hawāmidah, L. S. (2017). *Information Crimes, Pillars, and Methods of Confronting Them*.

Al-M'ebid, O. I. (2024). Criminal Liability Arising from the Use of Artificial Intelligence Technologies in the Saudi Arabian Legal System: An Analytical-Comparative Study. *Arab Journal of Security Studies*, *40*(2), 143-157.

Al-Maghrabi, T. (2023). Criminal Protection Against Artificial Intelligence Technology Errors (Example: Surgical Robot). *Journal of Jurisprudential and Legal Research*, *35*(43), 575-676. https://doi.org/10.21608/jlr.2023.238537.1290

Al-Rubai'i, N. M. (2024). Cybercrime and Its Counter Mechanisms (A Comparative Study). *Al-Farabi Journal for Human Sciences*, *3*(1), 73-90.

Al-Sherbiny, A. I. M. (2021). The Impact of Artificial Intelligence Technology Advancement on Police Activities in Confronting Psychological Warfare. *Journal of Legal and Economic Research (Mansoura)*, *11*(1), 975-1035.

Al-Zawwi, M. O. (2024). Criminal Confrontation with Crimes Committed by Machine Robots in Libyan and Emirati Law. *Journal of Police and Legal Sciences*, *15*(2), Article 3. https://doi.org/10.69672/3007-3529.1029

Al-Zubaidi, M. A., & Shahin, N. Q. (2024). The Criminal Text Crisis in Confronting Artificial Intelligence Crimes: An Analytical Study. *Zaytoonah University of Jordan Journal for Legal Studies*(Special Issue, 5th Year), 19-38.

Amish, R. A. (2021). Criminal Liability for Artificial Intelligence Crimes. *Journal of Legal and Economic Research (Mansoura)*, *11*(1), 763-820.

Bin Awda, H. M. (2022). Challenges of Enforcing Criminal Liability Rulings on Artificial Intelligence Crimes. *Journal of Law and Human Sciences*, *9*(1), 187-205.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Caliskan, A., Bryson, J. J., & Narayanan, A. (2021). Semantics derived automatically from language corpora contain human-like biases. *Science*, *356*(6334), 183-186. https://doi.org/10.1126/science.aal4230

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, *103*(3), 513-564.

Calo, R. (2016). *Robots in American law*.

Čapek, K. (1921). *R.U.R. (Rossumovi Univerzální Roboti)*.

Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. *IEEE Access*, *8*, 75264-75278. https://doi.org/10.1109/ACCESS.2020.2988510

Darwish, I. M. (2025). Criminal Liability in the Penal Code. *Al-Qarar Journal for Peer-Reviewed Scientific Research*, *5*(15), 414-442. https://doi.org/10.70758/elqarar/5.15.17

European Commission. (2020). *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics*.

European Parliament. (2016). *Civil Law Rules on Robotics: Legislative Resolution*.

Giles, A. P. (2018). Transnational cyber offenses: Overcoming jurisdictional challenges. *Yale Journal of International Law*, *43*(1), 195-219.

Hamon, R., Junklewitz, H., Sanchez, M. J. I., Fernandez, L. D., Gomez, G. E., Herrera, A. A., & Kriston, A. (2022). *Artificial Intelligence in Automated Driving: an analysis of safety and cybersecurity challenges*.

IBM. (2024). Exploring privacy issues in the age of AI.

IBM. (2025). *AI Agents in 2025: Expectations vs. Reality*.

Ibrahim, M. J. (2023). The Legal Framework for Granting Legal Personality to the Robot as an Artificial Intelligence Technology: An Analytical and Future-Oriented Study. *Rūḥ al-Qawānīn Journal, Faculty of Law, Tanta University, 8th International Scientific Conference Special Issue: Technology and Law*.

International Organization of Supreme Audit Institutions. (2023). Developing an audit framework for algorithms. *INTOSAI Journal*.

Janahi, W. Y. (2024). The Legal Status of Smart Robots and the Liability of Their Operator: An Analytical Study in Comparative Bahraini Law. *Al-Huqūq Journal, Kuwait University*, *48*(3).

Jonker, A., & Rogers, J. (2024). *What is algorithmic bias?*

Lagioia, F., & Sartor, G. (2019). Artificial intelligence, liability and responsibility: A legal perspective. *Philosophy & Technology*, *32*, 317-334. https://doi.org/10.1007/s13347-019-00354-7

Lubab, A.-J. (2023). *The Political Philosophy of Artificial Intelligence*.

Mourlam, A. C. (2016). Unarmed Attacks: Cyber Combatants & The Right to Defend. *California International Law Journal*, *26*(1), 19-21.

PMC. (2019). Artificial intelligence crime: An interdisciplinary analysis.

Smejkal, V., & Kodl, J. (2021). Comparative Study of Cryptographic and Biometric Signatures. 2021 International Carnahan Conference on Security Technology (ICCST), https://doi.org/10.1109/ICCST49569.2021.9717373