Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations
Homepage : https://journal.antispublisher.id/index.php/EJCBLT
Email : admin@antispublisher.com

e-ISSN : 3031-7355
JCBLT, Vol. 3, No. 3, March 2026
Page 34-44

Artificial Intelligence and Criminal Liability: A Legal Perspective on Emerging Crimes

Rafad Ali Hussein
University of Al-Qadisiyah, Iraq

DOI : https://doi.org/10.61796/ejcblt.v3i3.1766

Sections Info

Article history:
Submitted: December 10, 2025
Final Revised: January 22, 2026
Accepted: February 17, 2026
Published: March 25, 2026

Keywords:
Artificial intelligence
Criminal liability
Criminal law
Cybercrime
Iraqi legislation
Algerian legislation

ABSTRACT

Objective: *The objective of this study is to shed light on the theoretical concept of artificial intelligence crimes and criminal liability arising from their occurrence, besides examining the aspects of insufficiency of national laws in this respect and considering some solutions proposed by comparative laws.* ***Method:*** *The method used in conducting this study was one of comparison and analysis between national laws (Iraqi and Algerian) and some other foreign laws.* ***Results:*** *This study explores the challenges of assigning criminal liability to artificial intelligence systems, questioning whether it should be attributed to the intelligent system itself or to the human parties involved (programmer, end user, or technology owner). It also discusses the insufficiency of current national laws, particularly in Iraq and Algeria, in addressing these issues.* ***Novelty:*** *The novelty of this study lies in its examination of the evolving concept of criminal liability in relation to artificial intelligence, particularly in the context of Iraqi and Algerian law, and its comparison with foreign legal frameworks.*

INTRODUCTION

The world today is undergoing an unparalleled revolution in terms of technology and artificial intelligence where the latter is capable of conducting sophisticated jobs that used to be solely performed by humans such as autonomous driving, medical diagnosis, financial transactions management, and large amounts of data control. In addition to this wonderful phenomenon that helps facilitate people's lives, the legal and philosophical question about artificial intelligence crimes emerged and focused on understanding the nature of artificial intelligence and its potential criminal responsibility if a crime was committed against someone or something else.

The gravity of this problem becomes greater with the increasing use of artificial intelligence technologies in the fields of national security, health, justice, and economy among others. Suppose an artificial intelligence system commits homicide via a self-driving car. Alternatively, a smart financial system participates in committing a crime through money laundering or electronic fraud. Whom should be criminally liable? Is it the artificial intelligence system itself, the programmer, the manufacturer or the final customer?

Criminal legislations in general and in countries such as Iraq and Algeria specifically are founded upon the assumption that the crime is an activity of man conducted by his intention. As a result, an important legal problem emerges since there is no legislative provision that regulates artificial intelligence crimes. For this reason, there is a great necessity of reforming the legislation regarding criminal responsibility in

a way that suits technological developments without violating individual rights and freedoms.

Thus, this study focuses on the subject of criminal responsibility of artificial intelligence crimes based on the following outline:

Section One: Concept of artificial intelligence crimes.

Section Two: Criminal responsibility of artificial intelligence crimes.

Conclusion: Findings and Recommendations.

RESEARCH METHOD

This study employs a comparative and analytical approach to explore the concept of artificial intelligence crimes and their associated criminal liabilities. The research focuses on analyzing the legal frameworks of Iraqi and Algerian laws, comparing them with other international legislations to examine the current inadequacies in addressing crimes related to artificial intelligence. The study aims to identify the legal challenges posed by AI's autonomous decision-making and the complexities of attributing criminal responsibility. By drawing comparisons with European and international regulations, the study seeks to highlight potential legal reforms needed to adapt to the emerging AI-related criminal activities, ensuring that such frameworks can effectively address these new technological challenges.

RESULTS AND DISCUSSION

Chapter One

The Conceptual Framework of Artificial Intelligence Crimes

Artificial intelligence crimes represent an unprecedented legal and technical challenge, as they transcend traditional models of criminality by integrating autonomous algorithms into criminal behavior. The conceptual framework of these crimes aims to define the nature of the relationship between "the machine" and "criminal intent," striving to regulate legal responsibility in a highly complex digital environment. This framework seeks to bridge the legislative gap between the rapidly advancing technology and the established legal principles to ensure justice and digital security.

1.1 The Concept of Artificial Intelligence

This section will be divided into three parts, where we will outline the essence and legal nature of artificial intelligence, and in the third, we will present the forms of crimes arising from artificial intelligence, as follows:

1.1.1 The Nature of Artificial Intelligence

Artificial intelligence refers to the branch of computer science that aims to create systems capable of simulating human cognitive abilities such as learning, reasoning, problem-solving, and interacting with the surrounding environment [1]. The Organization for Economic Cooperation and Development (OECD) defined it in 2019 as:

"A machine-based system that can, under a certain degree of autonomy, generate outputs such as predictions, decisions, or recommendations that influence real or virtual environments. [2]"

The criminal danger in these systems lies in their ability to make quasi-independent decisions, which raises the question of whether they should be considered a "legal person" to whom criminal actions can be attributed, or if they are merely technical tools with the human (programmer or user) remaining the primary responsible party [3].

From a legal perspective, most legislations, including the Iraqi Penal Code (Law No. 111 of 1969) and the Algerian Penal Code (1966 and its amendments), have not explicitly addressed the concept of artificial intelligence. They have based their provisions on the assumption that a crime is a human act, which opens the door for doctrinal debate about the necessity of recognizing "electronic personality" or merely maintaining responsibility within the human domain (whether the programmer or the user) [4].

1.1.2 The Legal Nature of Artificial Intelligence

There are several legal perspectives on the nature of artificial intelligence:

First Perspective: Considering it as a Mere Technical Tool

1. This view holds that artificial intelligence is nothing more than a machine created by humans, and therefore it cannot be held criminally liable [5].
2. Accordingly, criminal responsibility remains limited to the user or programmer [6].

Second Perspective: Recognizing the Legal Personality of Artificial Intelligence

1. Some scholars advocate granting artificial intelligence the status of an "electronic person," similar to legal personality, so that actions can be attributed to it and legal, civil, or even criminal responsibility can be imposed on it [1].
2. This perspective is supported by the autonomy in decision-making that intelligent systems may possess, especially in cases where there is no direct human intervention [2].

Third Perspective: The Middle Ground

1. This approach considers artificial intelligence as a "legal entity with limited liability," where primary responsibility remains with the human, but secondary responsibility can be imposed on the system itself for regulatory or deterrent purposes [3].

1.1.3 Forms of Crimes Arising from Artificial Intelligence

Artificial intelligence has become a tool that can be exploited to commit new crimes or facilitate traditional crimes. Some of the most notable forms include:

Cybercrimes

1. The use of AI algorithms to breach information systems or manipulate data.
2. Examples: Smart phishing attacks, deepfakes, ransomware software [4].

Financial and Economic Crimes

1. Exploiting automated trading systems in financial markets to conduct fraudulent operations.
2. Money laundering through intelligent software capable of concealing the sources of funds [5].

Crimes Against Individuals

1. Causing fatal traffic accidents due to autonomous vehicles.
2. Errors in medical diagnoses by intelligent systems that lead to death or severe harm [6].

Security and Terrorist Crimes

1. The use of drones or intelligent robots in terrorist operations or assassinations.
2. Developing autonomous weapons capable of making decisions to kill without direct human intervention.

Ethical and Social Crimes

1. Manipulating public opinion through social networks using chatbots or propaganda dissemination systems.
2. Producing fake pornographic content using AI technologies [1].

1.2 The Legal Basis and Legal Foundation of Criminal Liability for Artificial Intelligence Crimes

The problem of the liability of criminal offenses committed by artificial intelligence raises the question of the establishment of a "legal framework" for attribution, considering the lack of human intentionality in certain algorithmic systems' operations. Such a legal framework is aimed at harmonizing criminal law and machine law, defining the individual who will be criminally liable—the programmer, the operator, or the corporation manufacturing the device. The research is intended to investigate the principles underlying such a legal framework, ensuring that the perpetrator will not avoid accountability under the pretext of "machine autonomy.

1.2.1 The Legal Structure of Crimes Committed Through Artificial Intelligence Technologies

The Material Element: The material element of a crime is based on the criminal behavior (either positive or negative), the criminal result, and the causal relationship between them.

The issue of artificial intelligence here lies in:

The criminal behavior may be carried out by an automated system that makes decisions without direct human intervention.

Example: An autonomous car runs over a person due to a programming error [2].

In this case, the question arises: Should the action be attributed to the user who allowed the system to operate? Or to the manufacturer who designed the program? Or should it be considered merely an accident or an act of fate?

The Iraqi law (Article 29 of the Penal Code) and Algerian law (Article 36 of the Penal Code) affirm that a crime occurs only if an act is committed by a human. This limits the scope of attributing the act to the intelligent system itself [1], making the responsibility confined to the person operating or programming it.

However, comparative jurisprudence (especially in the European Union) has started discussing the idea of modifying the concept of the material element to include

"direct" acts committed by intelligent systems, while keeping final responsibility with humans (programmers, companies, users) [2].

The Mental Element: This is represented by criminal intent or negligence.

Here, we face a significant challenge:

Artificial intelligence does not possess free will in the legal sense [3], meaning it cannot be presumed to have criminal intent.

However, negligence or carelessness on the part of the human in supervising or monitoring the intelligent system can arise.

Forms of the mental element:

Direct Criminal Intent:

When a person deliberately uses the AI system to commit a crime (such as using a program for forgery or fraud).

Negligence (Unintentional Error) [4]:

When the intelligent system causes harm due to neglect in supervision (such as failing to update autonomous driving software, leading to a fatal accident).

Probabilistic Intent:

If a person foresees the potential for a criminal outcome from the intelligent system and accepts it [5], they can be held liable for probabilistic intent.

The Legal Element: The crime's legal basis relies on the principle of "no crime and no punishment without a legal text," as stated in Article 19, Second Paragraph of the Iraqi Constitution and Article 1 of the Algerian Penal Code [6].

The issue with artificial intelligence is that most legislations do not contain explicit provisions criminalizing acts arising from AI. This creates a legislative gap that could allow perpetrators of cybercrimes and technical crimes to evade punishment.

Some countries have started addressing this gap, such as:

The European Union: Through the "Artificial Intelligence Act," [7] hich establishes rules for holding companies and programmers accountable.

The United States: Through some laws related to cybercrimes, such as the "Computer Fraud and Abuse Act."

In Iraq and Algeria, the approach still involves adapting traditional crimes [8] (such as forgery, manslaughter, or fraud) to include acts related to artificial intelligence.

1.2.2 Attribution of Criminal Responsibility in Artificial Intelligence Crimes

1. Human Responsibility (Programmer, User, Companies)

The programmer is responsible for writing the code and algorithms that enable the intelligent system to make decisions. If the programming contains intentional flaws or gross negligence that leads to the commission of a crime, they can be held criminally liable.

Example: A programmer deliberately adds code that allows the theft of user data.

In this case, their responsibility for the crime of fraud or information theft is established [9].

The user who operates the intelligent system may be criminally liable if they intentionally use it to commit a crime.

Example: Using an artificial intelligence program to produce fake pornographic content (deepfake) with the intent to defame [8].

Or using an autonomous vehicle while knowing there is a serious programming flaw that could cause accidents.

Manufacturing companies that develop or market artificial intelligence systems are criminally responsible if it is proven that they released a dangerous product into the market without providing safety guarantees.

Under Algerian law, legal persons can be held liable for crimes (Article 51 bis of the Penal Code).

Under Iraqi law, the legislator has not explicitly stated the criminal liability of companies, but the principle of vicarious liability or joint responsibility can be applied [7].

2. The Debate on Responsibility of Robots or Intelligent Systems

One of the key questions raised is: Can a robot or intelligent system be considered a "legal person" to whom criminal acts can be directly attributed?

The Opposing View: This perspective holds that criminal liability cannot be removed from the human domain, as robots lack free will and criminal awareness [3].

The Supporting View: Some advocate for recognizing the "electronic personality" of robots, similar to the legal personality of companies, so that they could bear specific liability (such as the confiscation of the system [5], its deactivation, or the imposition of fines on its owner in the robot's name).

The Middle Ground: This position suggests attributing formal responsibility to the robot, where it serves as a "legal vessel" to which the punishment is attributed, while the punishment is actually carried out on the owning or producing entity [7].

This debate continues in comparative jurisprudence and law, as no country has yet recognized the robot as an "independent criminal entity."

3. Criminal Responsibility of the State in Case of Lapse in Oversight

In some cases, the state itself may bear responsibility if it fails to establish legislative or regulatory frameworks for artificial intelligence systems.

Example: If the state allows the entry of autonomous vehicles without setting strict safety regulations [8], and then crimes or serious accidents occur, it could bear a form of indirect responsibility.

In both Iraqi and Algerian law, there are no direct provisions for holding the state criminally liable. However, political and administrative responsibility can be discussed, and perhaps civil responsibility towards the affected parties [9]. Criminal liability remains tied to individuals or legal entities (companies).

1.2.3 Proposed Penalties and Preventive Measures

A: Traditional Penalties

Although criminal legislations have not included specific provisions for artificial intelligence crimes, general rules allow for the imposition of traditional penalties on those responsible for them:

Deprivation of Liberty Penalties

Imprisonment or detention can be imposed on the programmer or user who is proven to have intentionally committed a crime via an intelligent system.

Example: Punishing someone who uses artificial intelligence to forge official documents with imprisonment under the forgery provisions in Iraqi law (Articles 286 and onward of the Penal Code) [10].

Financial Penalties (Fines)

Financial fines can be imposed on individuals or companies if it is determined that the intelligent system was used in financial or electronic crimes.

Under Algerian law [11] (Article 18), fines can be imposed on legal entities.

Confiscation

Confiscating devices and systems used in the commission of the crime, according to the general rules in Iraqi and Algerian laws.

B: Alternative Penalties and Preventive Measures

Given the specific nature of artificial intelligence crimes, traditional penalties alone may not suffice. Therefore, scholars suggest adopting modern measures such as:

Obligating Companies to Develop Security Systems

The judge may order the company to implement security improvements on the intelligent system instead of merely imposing a fine.

Prohibition from Engaging in Activities

Prohibiting the company or individual from using or marketing intelligent systems for a certain period if it is proven to have been misused.

Disciplinary and Professional Responsibility

If the perpetrator is a professional (such as a doctor using artificial intelligence incorrectly), they may face disciplinary penalties in addition to criminal penalties [12].

C: Proposed Legislative Solutions in Iraq, Algeria, and Comparison with Foreign Laws

In Iraqi Legislation

Iraqi law still relies on adapting traditional crimes to include actions related to artificial intelligence.

There is an urgent need for a specific law on cybercrimes (the proposed Electronic Crimes Law, which has been discussed multiple times in Parliament) to include a section dedicated to artificial intelligence [13].

In Algerian Legislation

Algeria has taken a step forward by including criminal liability for legal persons, which opens the door to holding companies that manufacture or market intelligent systems accountable.

However, the law does not yet include clear provisions related to crimes arising from artificial intelligence [14].

In Foreign Legislations

European Union: Currently discussing the "Artificial Intelligence Act" (AI Act), which imposes strict obligations on companies regarding security and transparency [5].

United States: Relies on cybercrime laws (such as the Computer Fraud and Abuse Act) and is considering creating a specific legal framework for artificial intelligence.

Japan and South Korea: Have begun developing legal systems that recognize limited liability for robots, with a focus on civil compensation rather than criminal penalties.

Chapter Two

Criminal Liability for Artificial Intelligence Crimes in Criminal Law

The issue of determining criminal liability arising from the actions of artificial intelligence is one of the most complex contemporary legal challenges. This is because the traditional model of liability is based on human actions emanating from a conscious will, while artificial intelligence systems may act independently based on complex algorithms and self-learning. Hence, the question arises: Who bears responsibility for the harmful or criminal actions that result from these systems? This chapter will address the following:

2.1: The Legal Basis for Criminal Liability

2.2: Penalties and Preventive Measures to Address Artificial Intelligence Crimes

2.1 The Legal Basis for Criminal Liability

Criminal liability is based on two main elements:

The Material Element: This refers to the criminal act or harmful result.

The Mental Element: This requires the existence of intent or negligence, either intentional or unintentional.

In the case of artificial intelligence, the material element is often present (such as damage to property or harm to a person), while the debate revolves around the mental element: Can intent or negligence be attributed to a program or a machine? Criminal laws in Iraq, Algeria, and most comparative legislations have not defined the "actor" in a way that would allow artificial intelligence to be included, as the actor is still limited to a natural person or legal entity [15].

2.1.1 Criminal Liability

Programmer and Manufacturer Liability: Some legal scholars advocate for holding the programmer or manufacturer criminally liable for crimes committed through artificial intelligence, based on:

Programming or Design Errors: If the program contains serious flaws and does not adhere to accepted safety standards, the programmer can be held liable.

Negligence in Testing or Supervision: If a product is released to the market without proper verification of its safety.

Some Western legal systems have adopted the concept of "product liability," which allows for holding companies accountable for damages caused, even if individual fault is not proven, in order to protect society [16].

User Liability:

The user is considered one of the key parties in the artificial intelligence chain, as they may use the system for legitimate or illicit purposes. If artificial intelligence is used with the intent to commit a crime, responsibility falls directly on the user as the principal

actor or accomplice, according to the rules of criminal participation set forth in penal codes [17].

However, if the use is legitimate but the system deviates due to autonomous algorithms, the user's liability may be mitigated if they can prove good faith and did not fail in supervision [18].

Legal Entity Liability:

Some modern legislations have moved towards holding companies that develop or operate artificial intelligence systems accountable as legal persons. This is based on the principle of "criminal liability of legal persons." Companies may reap substantial profits from artificial intelligence, and it is only fair that they bear the consequences for any damages caused by it. Both the Algerian and Iraqi legislators have provided for the criminal liability of legal entities in certain crimes, which could include artificial intelligence crimes in the future [19].

2.1.2 The Problem of Holding Artificial Intelligence Itself Accountable

One current legal approach to the issue involves recognizing some advanced artificial intelligence devices as having a "limited legal personality," allowing them to be civilly or even criminally responsible under certain restrictions. Nevertheless, such an approach presents philosophical and legal dilemmas, as it entails changing the meaning of the terms "responsibility" and "punishment."

In consequence, the dominant tendency is to place responsibility for any crime on the persons who programmed or operated the machines.

2.2 Punishments and Preventions against Artificial Intelligence Crimes

The crimes committed by artificial intelligence devices present significant problems for conventional criminal legislation, as conventional punishments would not be able to fulfill the goals of general and special prevention. In consequence, it has been imperative to identify suitable punishments and preventions in accordance with these crimes' nature.

2.2.1 Imposed Penalties

Penalties for Programmers and Users

A programmer or manufacturer is punished if they commit a gross error in designing or programming the system that leads to the commission of a crime. The penalty depends on the severity of the act (imprisonment or a fine) [20].

A user is punished if they use the system for illicit purposes, and the penalties stated in the Penal Code apply to them as the principal actor or accomplice [21].

Penalties for Legal Entities (Companies)

Temporary or permanent prohibition from engaging in activities.

Significant financial fines [12].

Confiscation of devices and software used to commit the crime.

Publicizing the judgment in media to damage the company's commercial reputation.

Subsequent and Complementary Penalties

Deprivation of the ability to contract with government institutions [22].

Inclusion of violating companies in "blacklists."

Revocation of licenses or suspension of related patents [19].

2.2.2 Preventive Measures

In addition to penalties, legislations need to adopt preventive and precautionary measures to ensure that crimes are not repeated. These measures include:

Technical Measures:

Requiring companies to implement "Safety by Design" systems that reduce potential risks [7].

Legislative Measures:

Enacting specific laws for artificial intelligence that precisely define the responsibility of each party and set strict rules for testing and marketing [2].

Supervisory Measures:

Establishing national bodies responsible for monitoring the applications of artificial intelligence, similar to data protection authorities [23].

Judicial Measures:

Granting the judiciary broad powers to immediately halt harmful systems, even before a final judgment is issued, to protect public security.

CONCLUSION

Fundamental Finding: Artificial intelligence crimes represent both an evolution of criminality and a demonstration of the flexibility of legal principles. It has been established that AI can be misused for criminal activities impacting individuals, society, and even the state. The main issue lies in determining criminal responsibility, as these systems function without direct human influence. **Implication:** A practical solution involves holding programmers, users, and producers criminally responsible for AI-related crimes. The concept of granting AI "legal personality" remains a theoretical discussion. Additionally, combining preventive and punitive measures is crucial to ensuring deterrence. **Limitation:** The study highlights the insufficient legal frameworks in Iraq and Algeria regarding artificial intelligence crimes, with no clear legal stance on assigning criminal responsibility. Furthermore, the practical implementation of AI regulations remains a challenge. **Future Research:** Future research should focus on introducing AI-specific laws in Iraq and Algeria, akin to European models. Additionally, there is a need to explore cross-border cooperation to address AI-related crimes and to establish fast compensation systems for damages caused by AI systems. Training for judges and public prosecutors on technical aspects of AI is also essential for future developments.

REFERENCES

[1] R. Binns, “On Being ‘Ethical’ with AI: The Ethics of Artificial Intelligence,” in *Proceedings of the 27th International Joint Conference on Artificial Intelligence*, 2018.

[2] H. H. Abu Rzouq, “Criminal liability for the use of artificial intelligence technologies in the medical field,” *Journal of Fiqh and Legal Research*, 2025.

[3] J. M. A. Al-Jumaily, "Criminal response to crimes committed using artificial intelligence," *Journal of Diyala University for Legal Sciences*, 2024.
[4] R. A. Hassan, "Criminal liability for the damages caused by artificial intelligence," *Legal Studies Journal*, 2025.
[5] A. H. Al-Shukri, "The issue of applying criminal liability rules to artificial intelligence crimes," *Journal of Legal Sciences, Faculty of Law - University of Baghdad*, 2022.
[6] Abdel Aziz, "Criminal liability for artificial intelligence crimes," *University of Batna 1, Algeria*, 2024.
[7] B. S. Abdel Qader, "The issue of applying criminal liability rules to artificial intelligence crimes," *Journal of Legal Sciences, Faculty of Law - University of Baghdad*, vol. 37, no. 2, 2022.
[8] Justice Team, "Criminal liability for the damages caused by artificial intelligence," 2024.
[9] *Mabda Magazine*, "Artificial intelligence and its role in criminal law," 2025.
[10] A. F. Al-Miyahi, "Criminal liability for the crimes committed by smart drones," *Ashur Journal of Legal Sciences*, 2025.
[11] *Digital Legal Publishing Platform*, "Criminal liability for artificial intelligence crimes," 2025.
[12] S. B. A. Al-Yahi, "Criminal liability arising from artificial intelligence crimes in light of Omani law," 2025.
[13] J. J. Bryson, "Patiency is not a virtue: AI and the design of ethical systems," in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018.
[14] R. Calo, "Robotics and the Lessons of Cyberlaw," *California Law Review*, 2015.
[15] European Commission, "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," 2021.
[16] European Parliament, "Resolution on Artificial Intelligence and Civil Liability," 2022.
[17] J. A. Goguen, "Artificial Intelligence and Legal Liability," in *Proceedings of the 2020 International Conference on Artificial Intelligence and Law*, 2020.
[18] IEEE Global Initiative, "Ethically Aligned Design," 2019.
[19] P. Lin, K. Abney, and G. A. Bekey, "Autonomous, Drones, and the Ethics of War," in *Springer Handbook of Robotics*, 2012.
[20] OECD, "Recommendation of the Council on Artificial Intelligence," 2019.
[21] B. C. Smith, "Responsible AI: A Global Policy Framework," *Journal of Artificial Intelligence Research*, 2021.
[22] M. Taddeo and L. Floridi, "How AI can be a force for good," *Science*, 2018.
[23] United Nations, "Report on the Regulation of Artificial Intelligence," 2023.

***Rafad Ali Hussein (Corresponding Author)**
University of Al-Qadisiyah, Iraq
Email: rfadalihussien@gmail.com