



Criminal Liability Arising from the Use of Artificial Intelligence Applications

Hayder Jawad Kazem^{1*} & Hayder Falih Mahdi²

^{1,2}Al-Furat Al-Awsat Technical University Al-Mussaib Technical Institute Babylon, Iraq

DOI:10.5281/zenodo.19810639

ARTICLE INFO

Article history:

Received : 02-04-2026

Accepted : 09-04-2026

Available online : 27-04-2026

Copyright©2026 The Author(s):

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

Citation: Kazem, H. J., & Mahdi, H. F. (2026). Criminal Liability Arising from the Use of Artificial Intelligence Applications. *IKR Journal of Arts, Humanities and Social Sciences (IKRJAHS)*, 2(2), 120-143.



ABSTRACT

Original Research Article

The increasing use of artificial intelligence applications across various domains of contemporary life gives rise to significant legal challenges, particularly in relation to the attribution of criminal liability for acts committed through such systems. This raises critical questions regarding the adequacy of existing legal frameworks and their capacity to accommodate the unique and evolving characteristics of artificial intelligence technologies. In this context, the present study aims to examine the current and potential future challenges associated with artificial intelligence applications, especially in light of the rapid pace of technological advancement. Advanced AI systems have endowed certain machines with sophisticated capabilities, including the ability to acquire experiential learning and make autonomous decisions, thereby raising concerns about the possibility of these entities acting independently of direct human control. Accordingly, it becomes conceivable that such systems may deviate from programmed instructions and engage in conduct that could be classified as criminal acts. This necessitates a comprehensive legal inquiry into the nature and scope of criminal liability arising from offences committed by autonomous artificial intelligence entities, particularly those capable of independent decision-making.

Keywords: Artificial Intelligence, Criminal Liability, Digital Crimes, Legal Personality of Artificial Intelligence, Criminal Accountability of Smart Technologies.

*Corresponding author: Hayder jawad kazem

Al-Furat Al-Awsat Technical University Al-Mussaib Technical Institute Babylon, Iraq

Introduction

In recent years, artificial intelligence (AI) technologies have undergone a profound transformation, moving beyond theoretical constructs and experimental models to become integral components of contemporary life. Their applications now span diverse domains, including industrial and service robotics, autonomous vehicles, unmanned aerial systems, and advanced data-driven decision-making platforms. As a result, AI systems play an increasingly central role across economic, social, healthcare, and security sectors, contributing to enhanced efficiency, accelerated processes, and improved service delivery.

Despite these benefits, the rapid proliferation of AI technologies has introduced complex legal challenges, particularly within the field of criminal law. Concerns arise

when AI systems are used as instruments in the commission of criminal offences or when their operation leads to harm affecting legally protected interests. The growing capacity of such systems—especially those based on machine learning and advanced algorithms—to process data and generate autonomous or semi-autonomous decisions complicates the application of traditional legal doctrines. This development raises critical questions regarding the legal characterization of AI-related conduct and the extent to which such conduct can be attributed to a human actor under established principles of criminal liability.

Against this backdrop, the issue of criminal liability in the context of AI has become a subject of increasing importance. A central challenge lies in identifying the appropriate bearer of responsibility in cases involving AI-related harm. This

includes scenarios in which AI is deliberately employed to facilitate criminal activity, as well as situations where harm results from systems operating with a degree of functional autonomy.

These developments give rise to fundamental legal questions concerning the allocation of responsibility, particularly in determining whether liability should be attributed to the programmer, manufacturer, user, or owner of the system, or whether existing legal frameworks require reconsideration to accommodate the unique characteristics of AI technologies.

Accordingly, this study seeks to examine the problem of criminal liability in relation to artificial intelligence systems within the context of contemporary technological developments. It aims to contribute to the formulation of a coherent legal approach that balances the need to address emerging risks with the preservation of core principles of criminal law, including legality and personal responsibility.

On this basis, the present study examines the criminal liability arising from the use of artificial intelligence systems, through the following key aspects:

First: Significance of the Study

This study is significant in light of the profound transformation that artificial intelligence technologies have introduced across various fields of knowledge, giving rise to complex legal challenges, particularly with respect to the potential emergence of criminal conduct associated with their use. The value of this research lies in its systematic examination of criminal liability arising from offences committed through AI systems, with a particular focus on the problem of attributing responsibility for such conduct. In doing so, the study addresses a critical regulatory gap by analyzing the existing legal framework under Iraqi law and situating it within a comparative context that draws on relevant legislative and jurisprudential developments in other legal systems. Through this comparative approach, the study seeks to contribute to the development of a coherent and methodologically grounded legal framework that can support the Iraqi legislator in formulating appropriate legal rules capable of responding to rapid technological advancements. At the same time, it aims to ensure a principled balance between fostering technological innovation and safeguarding fundamental rights and freedoms.

Second: Objective of the Study

This study aims to identify the legally accountable party for offences arising from the use of artificial intelligence (AI) systems, in a manner that ensures the effective enforcement of appropriate legal sanctions. This objective serves two main purposes. First, it contributes to preserving social order and stability in light of the increasing proliferation of these technologies. Second, it supports the sustainable development and future growth of AI systems.

The continued occurrence of criminal conduct in the absence of clear and effective accountability poses a significant threat to public security and undermines confidence in such systems. This, in turn, may hinder their development and limit their optimal use. Accordingly, these concerns highlight the urgent need to establish a specialized legal framework to regulate crimes associated with artificial intelligence.

Third: Research Problem

This study addresses the legal complexities arising from the rapid development of artificial intelligence (AI) technologies, particularly in situations where such systems generate conduct that may constitute criminal offences under applicable criminal law.

In this context, a fundamental legal question arises regarding the identification of the party to whom criminal liability should be attributed. This challenge is further complicated by the fact that certain AI systems exhibit a degree of autonomy in data processing and decision-making. Accordingly, the central research question of this study is as follows: who may be held criminally liable for offences arising from the use of artificial intelligence systems? More specifically, can such liability be attributed to the programmer, the manufacturer, the owner, or the user, or does the nature of these systems require a reassessment of the established doctrines of criminal liability?

This primary question gives rise to several subsidiary inquiries, most notably:

- What is the concept of artificial intelligence and what are its principal applications?
- Can artificial intelligence systems be endowed with independent legal personality?
- To what extent may the programmer, owner, or user be held criminally accountable for crimes associated with artificial intelligence?

Fourth: Research Methodology

To achieve the objectives of this research and address its central questions, the study adopts a doctrinal and analytical methodology. It situates emerging developments related to artificial intelligence (AI) systems within the framework of fundamental principles of criminal law and evaluates the extent to which existing legal provisions can be applied to such conduct.

The analytical approach proceeds through a structured examination of relevant legal frameworks, followed by an assessment of their applicability to offences arising from AI systems, with the aim of developing a more precise legal characterization of such acts. In addition, the study adopts a comparative perspective by reviewing selected legislative frameworks that have addressed criminal liability in this context.

The study focuses on three jurisdictions, namely Iraq, the United States, and the European Union. These were selected based on their representation of different regulatory approaches: Iraq as an emerging legal system lacking specific AI regulation, the United States as a flexible and sector-based model, and the European Union as a comprehensive and risk-based framework. This selection enables a balanced comparative analysis reflecting both developing and advanced legal systems.

In terms of sources, the study relies primarily on peer-reviewed academic literature, official legislative texts, and authoritative legal commentaries. Sources were selected based on their relevance, credibility, and contribution to the analytical development of the subject matter, with particular emphasis on recent works addressing contemporary challenges associated with artificial intelligence technologies.

The study also explores different types of artificial intelligence and examines the ongoing doctrinal debate concerning the potential recognition of legal personality for AI systems.

Based on the foregoing, the research is divided into three main sections as follows:

1. Section One: The Concept and Nature of Artificial Intelligence.
2. Section Two: Crimes Committed through Artificial Intelligence Entities.
3. Section Three: Criminal Liability of Artificial Intelligence Entities.

Finally, the research concludes with a set of results and recommendations

Section One

The Concept of Artificial Intelligence

In this section, the concept and nature of artificial intelligence will be examined. Accordingly, this section is divided into three subsections as follows:

Subsection One: Definition of Artificial Intelligence and Its Types.

Subsection Two: Applications of Artificial Intelligence.

Subsection Three: The Position of Different Legislations toward Artificial Intelligence Applications.

Subsection One

Definition of Artificial Intelligence and Its Types

Despite the existence of multiple definitions of artificial intelligence (AI) and the absence of a single universally accepted definition in academic and technical literature, it may generally be understood as a system or computer program based on algorithms and data designed to simulate human-like intelligence. Such systems are capable of self-learning and adaptive behavior, enabling them to operate with

a degree of autonomy in response to data inputs and their surrounding environment¹.

Artificial intelligence may also be defined as a system designed by humans within machines or computer systems, enabling them to perform tasks that originally require human cognitive abilities by simulating processes of reasoning, analysis, and decision-making².

Artificial intelligence has also been conceptualized by Alan Turing as the ability of a machine to exhibit behavior indistinguishable from that of a human. This idea is illustrated through the Turing Test, in which a machine attempts to produce responses that lead an interrogator to believe they are interacting with a human rather than a machine³.

Artificial intelligence has also been defined by some scholars as a branch of computer science concerned with enabling computers to perform tasks that approximate human intelligence, such as learning, inference, and decision-making⁴.

Andreas Kaplan and Michael Haenlein define artificial intelligence as the ability of a system to correctly interpret external data, learn from such data, and use the acquired knowledge to achieve specific goals and tasks through flexible adaptation⁵.

John McCarthy, widely regarded as the father of artificial intelligence, defined it as the science and engineering of creating intelligent machines. This includes the development of computer systems, robots, and programs capable of exhibiting behavior comparable to human reasoning.

Artificial intelligence is further grounded in the study of human cognitive processes, including how individuals learn, make decisions, and solve problems. Insights derived from these processes are then used as a foundation for the design and development of intelligent systems⁶.

¹Mohamed Rabie Fath Al-Bab, *Artificial Intelligence Contracts: Their Emergence, Concept, and Characteristics*, Faculty of Law, Menoufia University, 2022, p. 611.

²Yassin Saad Ghalib, *Fundamentals of Management Information Systems and Information Technology*, Dar Al-Manhaj for Publishing and Distribution, 1st ed., Amman, 2012, p. 114.

³Saber Al-Haddam, *Law in the Face of Artificial Intelligence: A Comparative Study*, Master's Thesis, Faculty of Legal, Economic and Social Sciences, Sidi Mohamed Ben Abdellah University, Fez, 2022, p. 4.

⁴Asmaa Blilita, *The Legal and Regulatory Institutionalization of Artificial Intelligence in Algeria*, *International Journal of Artificial Intelligence in Education and Training*, University of Algiers, January 2022, p. 19.

⁵Tahir Abu Al-Eid, *Artificial Intelligence and the Future of Justice: Challenges and Future Prospects*, *Legal Education Development Initiative Publications*, 2024, p. 7.

⁶Dona Ahmed, *Artificial Intelligence*, Master's Thesis, Faculty of Law, Lebanese University, 2021, p. 15.

According to the Larousse Encyclopedia, artificial intelligence is defined as a set of theories and implemented techniques aimed at creating a machine capable of simulating human intelligence⁷. From a legal perspective, artificial intelligence is defined in a manner broadly consistent with prevailing scientific understandings, albeit with greater precision. This definition emphasizes systems such as expert systems, advisory systems, and decision-support systems, which are designed to assist and guide decision-making processes.

From a legal perspective, artificial intelligence is defined in a manner broadly consistent with prevailing scientific understandings, albeit with greater precision. This definition emphasizes systems such as expert systems, advisory systems, and decision-support systems, which are designed to assist and guide decision-making processes⁸.

Given the diversity of definitions and the multifaceted nature of artificial intelligence (AI), it becomes necessary to adopt a systematic classification in order to better understand its varying levels of complexity and functionality. Such classification facilitates a clearer analysis of the legal implications associated with each category, particularly in relation to autonomy, decision-making, and potential liability.

On this basis, artificial intelligence can be classified into three main categories:

1. Weak or Narrow Artificial Intelligence (Weak AI):

This type represents the most basic and widely used form of artificial intelligence (AI) in practical applications. It focuses on the development of systems capable of simulating specific aspects of human cognition in the performance of clearly defined tasks.

Such systems rely on pre-programmed algorithms and operate strictly within predefined parameters, lacking the capacity for adaptation or independent deviation. As a result, their behavior is limited to predetermined responses.

This category is commonly referred to as “narrow artificial intelligence,” reflecting its confinement to specialized functions within a limited scope. Consequently, its efficiency is inherently constrained by its design, rendering it incapable of performing tasks beyond its intended domain or departing from the rules embedded within its architecture⁹.

⁷Dr. Ahmed Abu Al-Majd Mohammed Al-Sayed Afifi, *The Law Applicable to Personal Data in Artificial Intelligence Technologies, Journal of Legal and Economic Studies, Vol. 11, No. 1, Faculty of Law, University of Sadat City, 2025, p. 1219.*

⁸*Ibid.*, p. 1219.

⁹Ahmed Saad Ali Barai, *Applications of Artificial Intelligence and Robotics from the Perspective of Islamic Jurisprudence, published in the Journal of Dar Al-Ifta Al-Misriyyah, Faculty of Islamic and Arabic Studies (Boys), Cairo, Issue No. 48, pp. 15–16.*

2. General or Strong Artificial Intelligence (AGI):

This type refers to advanced artificial intelligence (AI) systems with cognitive capabilities that approximate aspects of human mental functioning. These systems operate by collecting and analyzing data and drawing on accumulated experience to support autonomous decision-making.

General artificial intelligence is often described as having the capacity to think, understand, and act in ways that may resemble human outputs. It is also suggested that such systems can be designed to simulate certain features of human cognition, including perception, reasoning, and adaptive responses.

Autonomous vehicle control systems are frequently cited as illustrative examples of this category of AI. The development of such systems raises complex legal questions, particularly regarding the extent to which they may be considered subjects of criminal liability¹⁰.

3. Super Artificial Intelligence (Superintelligence):

This type represents the most advanced stage in the evolution of artificial intelligence (AI), in which systems are theoretically capable of developing or generating other systems similar to themselves.

In this context, Arend Hintze suggests that research in artificial intelligence should extend beyond merely understanding consciousness to exploring the possibility of developing machines with a form of self-awareness. This includes the capacity to recognize their own states, process internal information, and respond to external stimuli in a manner that reflects an awareness of their operational context¹¹.

Superintelligence represents an advanced stage in the evolution of artificial intelligence (AI), characterized by its potential to surpass human cognitive capacities. This development has positioned it as a subject of strategic importance and competition among states, given its anticipated geopolitical implications.

In this context, Nick Bostrom defines superintelligence as a form of intelligence that exceeds the capabilities of the most advanced human minds across a wide range of domains, including scientific innovation, general reasoning, and social cognition.

¹⁰Abdullah Mousa and Ahmed Habib Bilal, *Artificial Intelligence: A Revolution in Modern Technologies, Arab Group for Training and Publishing, Cairo, Egypt, 2019, p. 29.*

¹¹Dr. Mahmoud Abdel-Ghani Farid, *Recent Trends in Criminal Liability of Entities Operating with Artificial Intelligence Technologies, Journal of Legal and Economic Research, Faculty of Law, Menoufia University, Vol. 53, No. 3, May 2021, p. 500.*

Its scope ranges from systems that slightly outperform human intellectual performance to those that significantly surpass human cognitive abilities¹².

In light of the varying levels of complexity and autonomy associated with artificial intelligence (AI), its applications span a wide range of domains. Accordingly, the study adopts a focused analytical approach, concentrating on selected applications that have direct legal relevance.

Subsection Two

Applications of Artificial Intelligence

Given the broad scope of artificial intelligence (AI) and the diversity of its applications, this study adopts a focused analytical approach. This is due to the practical limitations associated with achieving comprehensive coverage at the present stage.

Accordingly, the analysis centers on selected applications that have a direct impact on individuals' daily lives. In particular, the study examines autonomous vehicles and unmanned aerial systems (UAVs), as they represent some of the most prominent and legally significant applications of AI in this context.

First: Unmanned Aerial Vehicles (Drones):

The advancement of unmanned aerial systems (UAS), commonly referred to as drones, represents a significant technological development in contemporary industrial sectors. These systems provide corporations, institutions, and governmental bodies with advanced tools that enhance operational efficiency, accuracy, and safety across a wide range of functions. They also contribute to reducing economic costs and minimizing risks to human life.

Historically, the early development of UAS was closely linked to military applications, particularly in warfare and armed conflicts. In such contexts, these systems have been used to conduct combat missions, as well as reconnaissance and surveillance operations, without exposing personnel to direct harm and while reducing operational costs. The origins of this technology can be traced back to England in 1917.

UAS operate either through remote control or via autonomous flight systems, depending on their design and functional requirements. Unmanned aerial vehicles can generally be classified, in terms of their guidance systems, into two main categories. The first includes systems operated through remote control, while the second relies on artificial intelligence algorithms, allowing the aircraft to operate with a degree of autonomy in decision-making and task execution. These are commonly referred to as autonomous drones. Such advanced technologies are widely employed in military

contexts to conduct combat operations, surveillance, reconnaissance, and other complex missions¹³.

Unmanned aerial vehicles (drones) have increasingly emerged as dual-use technologies, widely employed in legitimate commercial and civilian contexts, including cargo transport, package delivery, sports coverage, agricultural applications, and personal use. At the same time, they present significant legal and security risks.

In particular, drones have been misused in the commission of terrorist activities, enhancing the operational capabilities of such groups. They may be equipped with precision-guided weapons or improvised explosive devices and deployed with a high degree of accuracy against designated targets. In addition, they can be used for surveillance and reconnaissance purposes.

These developments give rise to complex legal and regulatory challenges, especially with regard to their unlawful use and the difficulties associated with monitoring and controlling their deployment.

Second: Autonomous Vehicles

Autonomous vehicles represent one of the most prominent advanced applications of artificial intelligence (AI), and have experienced significant expansion in several countries in recent years, with expectations of wider adoption in the future.

These vehicles are characterized by their ability to perform driving and navigation tasks without direct human intervention. They function through an integrated system of sensors, cameras, and short- and long-range radar, enabling them to perceive their surroundings, measure distances, and navigate safely.

Autonomous vehicles rely on self-operating technologies that support real-time decision-making, allowing them to avoid obstacles, respond to traffic conditions, and comply with traffic signals based on continuously processed data¹⁴.

This technology is based on an integrated system of cameras and multi-functional sensors designed to enable the vehicle to accurately perceive its surrounding environment. These components operate in conjunction with computational algorithms that analyze real-time data to support safe and efficient navigation.

The sensors are strategically distributed across the vehicle to ensure comprehensive environmental coverage. These include cameras mounted on the windshield and side mirrors, ultrasonic sensors embedded in the front and rear bumpers, as well as both short- and long-range radar systems. Together, these devices enable precise detection of objects and changing environmental conditions.

¹²Dona Halal, *Artificial Intelligence, Master's Thesis, Faculty of Law, Lebanese University, 2020, p. 24.*

¹³Farid, *op. cit.*, p. 505.

¹⁴See: "self-driving car" *Wikipedia's article* https://en.wikipedia.org/wiki/Self-driving_car

All components function within a highly interconnected system that allows for continuous data processing and real-time information exchange. This integration enables the vehicle to respond effectively to potential risks, anticipate possible scenarios, and simulate aspects of human driving judgment.

The increasing complexity and autonomy of artificial intelligence (AI) applications, as illustrated by such systems, give rise to significant legal and regulatory challenges. In particular, these developments necessitate a clear examination of how different legal systems address issues of responsibility, accountability, and governance in relation to AI technologies.

Subsection Three

The Position of Different Legislations toward Artificial Intelligence Applications

This section is devoted to examining the legislative approach to applications of artificial intelligence, through a review of the position of the Iraqi legislator, followed by that of the United States legislator, and subsequently the position of the European legislator, in the following order:

First: The Position of the Iraqi Legislator on Applications of Artificial Intelligence

The position of the Iraqi legislator regarding applications of artificial intelligence (AI) is broadly comparable to that of many other legal systems. To date, no specific criminal legislation has been enacted to address liability for offences involving AI, nor has dedicated civil legislation been introduced to regulate civil liability arising from such applications.

This legislative gap is largely attributable to the relative novelty of the subject, particularly within Arab legal systems.

Accordingly, offences arising from the use of artificial intelligence are currently addressed in accordance with the general provisions of the Penal Code.

Second: The Position of the United States Legislator on Applications of Artificial Intelligence:

Despite the widespread adoption of artificial intelligence (AI) technologies in the United States across industrial, medical, and research sectors, there is still no comprehensive and unified legislative framework governing these technologies in a clear and systematic manner.

However, U.S. policymakers have taken steps toward regulating specific aspects of AI applications. These efforts include the issuance of Executive Order No. 13859, which established the American Artificial Intelligence Initiative. In 2020, the Electronic Privacy Information Center submitted a petition to the Federal Trade Commission calling for the development of a regulatory framework for the use of AI in commercial activities. In the same year, the U.S. Office of Management and Budget issued guidelines outlining

approaches to the governance and development of such technologies.

Furthermore, the National Artificial Intelligence Initiative Act was enacted in that year, with the aim of reinforcing United States leadership in this field¹⁵.

Third: The Position of the European Legislator on Applications of Artificial Intelligence:

The European Union, through Regulation (EU) No. 1698/2024 on artificial intelligence, seeks to establish a comprehensive regulatory framework governing the development and use of AI technologies. This framework aims to ensure their safe and accountable operation while maintaining a balance between technological advancement and the protection of the Union's fundamental values and principles.

In addition, the regulation introduces strict obligations and supervisory mechanisms for developers and operators of AI systems, particularly in relation to risk assessment. It requires operators to conduct ex ante evaluations of potential risks prior to the commercialization or deployment of such systems, thereby ensuring compliance with applicable legal and security standards¹⁶.

The Regulation further introduces transparency obligations requiring the provision of explicit and readily accessible information concerning the functioning of artificial intelligence systems, as well as the foundational principles informing their decision-making processes. It also underscores the necessity of establishing clearly defined accountability structures, thereby ensuring effective traceability and legal accountability for harms arising from the application of such technologies¹⁷.

Italy has positioned itself as one of the first European Union member states to adopt a comprehensive regulatory framework governing the application of artificial intelligence (AI) technologies. This framework includes statutory provisions that impose custodial penalties in cases involving the intentional misuse of such technologies to cause harm.

The Italian government has further emphasized that this legislation, in alignment with the European Union's Artificial Intelligence Act, represents a significant step toward the development of an integrated governance framework for AI. It aims to ensure the regulated and legally compliant use of these technologies within the Italian jurisdiction¹⁸.

The legislation further provides for the imposition of more stringent penalties where technology is used in the

¹⁵Mahmoud Abdel Ghani Farid, *op. cit.*, pp. 507–508.

¹⁶EU AI Law: A Step Towards Regulating the Technological Future - Al Safar & Partners Advocates & Legal Consultants. Accessed on 25 December 2025.

¹⁷*op. cit.*

¹⁸Taher Abu Al-Eid, *The New Italian Artificial Intelligence Law, Initiative for the Development of Legal Education*, 2025, p. 3.

commission of offences, including fraud and identity theft. It also establishes stricter requirements concerning transparency and human oversight in the use of such technologies across various sectors, including healthcare, education, justice, and sports.

Article 26 sets out specific penalties for offences committed through the use of artificial intelligence (AI) systems. A notable legislative development is the introduction of an aggravating circumstance under paragraphs 10 and 11 of Article 61 of the Penal Code. This provision applies to offences committed “through the use of artificial intelligence systems” where certain specified conditions are met.

- That such systems, by their nature or by the manner in which they are employed, constitute a malicious means.
- That their use impedes public or private defence in any manner whatsoever.
- That their use results in the aggravation of the criminal consequences of the offence¹⁹.

A comparative analysis of these legislative approaches reveals notable differences in both scope and regulatory philosophy. While the European Union adopts a comprehensive and risk-based framework emphasizing preventive regulation and accountability, the United States relies on a fragmented approach, addressing artificial intelligence (AI) through sector-specific measures and policy guidelines rather than a unified legislative regime. In contrast, the Iraqi legal system remains at an early stage of regulatory development, lacking dedicated provisions governing AI-related liability.

From a critical perspective, the European model appears more effective in addressing the complexities of AI technologies, particularly through its emphasis on ex ante risk assessment and compliance mechanisms. However, its stringent regulatory requirements may pose challenges for innovation. Conversely, the U.S. approach provides greater flexibility but suffers from regulatory gaps that may undermine legal certainty.

Accordingly, this study argues that an optimal regulatory model should strike a balance between these approaches by combining the European Union’s structured risk-based framework with the flexibility characteristic of the U.S. system, while taking into account the specific legal and institutional context of jurisdictions such as Iraq.

While the development of an appropriate regulatory framework remains essential, the practical implications of artificial intelligence (AI) become most apparent when examining the criminal conduct that may arise from its use. This shift from regulatory theory to practical application necessitates a closer analysis of AI-related offences, their legal characterization, and the allocation of criminal liability among the parties involved.

¹⁹*op. cit.*, p. 23.

Section Two

Crimes Committed through Artificial Intelligence Entities

Building on the foregoing analysis, this section examines crimes related to artificial intelligence (AI), including both those observed in practice as a result of its use and those that may arise in the future given the rapid development of such technologies. It also analyzes the penalties applicable to these offences and identifies the parties to whom criminal liability may be attributed, whether the manufacturer or the user of AI systems.

Furthermore, the chapter explores, from a theoretical perspective, the possibility of attributing criminal liability to AI itself, particularly in scenarios where technological advancements may lead to systems capable of acting independently of human intent.

Accordingly, this chapter is divided into three sections as follows:

Subsection One: Forms of Offences Committed by Artificial Intelligence Entities

Subsection Two: Determination of Criminal Liability Arising from the Acts of Artificial Intelligence Entities

Subsection Three: Penalties Prescribed for Offences Related to Artificial Intelligence Entities

Subsection One

Forms of Offences Committed by Artificial Intelligence Entities

Recent technological advancements have led to the emergence of new forms of offences associated with artificial intelligence (AI). The advanced software underlying such systems enables a degree of autonomous learning, allowing them to operate with limited human intervention and to generate independent decisions²⁰.

These offences take various forms. Notable examples include those arising from the use of autonomous vehicles, algorithm-driven conduct on social media platforms—particularly Facebook—as well as offences involving robots and unmanned aerial vehicles (UAVs).

These forms will be examined as follows:

First: Offences Related to Autonomous Vehicles.

Second: Offences Related to Facebook Algorithms.

Third: Offences Related to Robots.

First: Offences Related to Autonomous Vehicles

Autonomous vehicles are defined as vehicles that can operate either partially or fully without direct human intervention in certain situations. They are equipped with an integrated set of sensors, cameras, radar systems, and artificial intelligence

²⁰F. Patrick Hubbard "Do Androids dream?, personhood and intelligent artifacts b, 83 temp. L. Rev., 2011, P421.

(AI) technologies that enable navigation between specified locations without human control.

AI technologies allow these vehicles to perform driving functions and continuously monitor the road environment. In this context, the role of the human operator is generally limited to providing input data, such as trip details or navigation instructions²¹.

In 2012, the first official license for the operation of autonomous vehicles was granted in the State of Nevada in the United States. Subsequently, several U.S. states issued experimental permits allowing such vehicles to operate on public roads within controlled testing frameworks.

In parallel, a number of European countries—including Germany, the United Kingdom, the Netherlands, Spain, and France—have adopted regulatory approaches that permit the testing and experimental deployment of autonomous vehicles on public road networks under clearly defined legal regimes.

These developments reflect a broader policy shift toward encouraging technological experimentation and indicate a growing trend toward the wider deployment of autonomous vehicles in the near future²².

One of the most notable incidents involving autonomous vehicles occurred on March 18, 2018, when a self-driving Uber vehicle struck a pedestrian, Elaine Herzberg, as she was crossing the road in Tempe, Arizona. The vehicle was operating in autonomous mode at the time, and the victim later died from her injuries.

This event is widely considered the first recorded fatality of a pedestrian caused by a self-driving vehicle during testing on public roads. It has raised significant legal questions regarding the attribution of criminal liability in the context of autonomous systems, particularly in relation to the roles of the operator, the developer, and the entity responsible for deploying the technology²³.

Another notable incident occurred in Taiwan in 2020, when a Tesla Model 3 operating under its Autopilot system collided with an overturned truck on a highway. The accident was attributed to the system's failure to detect the obstacle in a timely manner, resulting in a collision and damage to the vehicle.

²¹D. Mohamed Ibrahim Ibrahim Hassanein, *Artificial Intelligence and Civil Liability for Damages Arising from Its Application: An Analytical and Foundational Study*, *Al-Qanoun Journal (The Legal Journal)*, p. 237.

²²I. Bikeev, P. A. Kabanov, I. R. Begishev, Z. I. Khisamova, *criminological risks and 2 legal aspects of artificial intelligence implementations in proceedings of the international conference on artificial intelligence, information processing and cloud computing*, New York, 2019.

²³*Self-Driving Uber Car Kills Pedestrian in Arizona*, *TIME / UPI News*, 19 March 2018. Accessed on 25 December 2025

This incident underscores critical legal concerns regarding the reliability of autonomous driving systems. It also raises important questions about the attribution of liability in cases where system failure contributes to harm, particularly with respect to the responsibilities of the manufacturer and the operator²⁴.

Notwithstanding the occurrence of such incidents, certain scholars have argued against calling for the suspension of the use of autonomous vehicles. They base this position on the premise that traffic accidents caused by human drivers far exceed those associated with such vehicles. Accordingly, they contend that autonomous vehicles may offer a higher level of safety compared to human-driven vehicles when a comparative assessment is undertaken²⁵.

In our view, the introduction of autonomous vehicles into public roads should be approached with caution and careful consideration. While this technology represents an important step in technological advancement and offers potential economic and practical benefits, the protection of life and property must remain a primary priority.

Accordingly, sufficient time should be allocated for thorough testing and empirical evaluation before large-scale deployment is permitted. Such deployment should only proceed once the technology has been proven to operate safely and effectively, thereby minimizing risks to individuals and their property.

Second: Offences Related to Facebook Algorithms

Social media platforms represent a key component of the modern digital ecosystem, with Facebook occupying a leading position. The platform relies extensively on algorithm-based systems as a core application of artificial intelligence (AI).

In this context, Facebook employs cookies for multiple purposes, including user authentication, preference profiling, geolocation, and the analysis of browsing behavior, typically based on user consent.

However, potential privacy concerns arise when AI algorithms are used to analyze user interactions with content, such as images, posts, and engagement with specific topics or products, in order to construct detailed behavioral profiles. These profiles are subsequently utilized for targeted advertising, raising significant legal and regulatory issues related to data protection, governance, and the limits of lawful data processing²⁶.

²⁴*Motor Trend, Tesla Model 3 crashes into overturned truck in Taiwan, 2020*. Accessed on 25 December 2025

²⁵D. Yahya Dahshan, *Criminal Liability for Artificial Intelligence Crimes*, *Journal of Sharia and Law, United Arab Emirates University, College of Law*, Vol. 34, No. 82, April 2020, p. 118.

²⁶Mona Mohamed Al-Atris Al-Desouki, *Crimes of Artificial Intelligence Technologies and the Independent Electronic Legal*

Some scholars argue that Facebook's practices may constitute an infringement of individual privacy. This concern arises from the requirement that users, upon creating an account, must consent to the platform's terms of use and privacy policy in order to proceed with registration and access its services.

By accepting these terms, users effectively permit the platform to collect and process their data for various purposes that serve its interests. However, when legal accountability is considered, such practices may not necessarily be deemed unlawful, as they are based on the user's prior consent to the applicable terms and conditions²⁷.

It has been observed that "there is no service without consideration; if a service is free, then you are the consideration." This observation is reflected in Facebook's practices, which extend beyond the collection of cookies to include the analysis of user communications, such as voice interactions and written content, in order to identify keywords indicative of user interests. The resulting data is then used for targeted advertising and the delivery of personalized content.

Such practices raise concerns about potential overreach and their impact on user privacy, which, in certain circumstances, may give rise to criminal implications.

However, as previously noted, the collection of user data does not in itself constitute a criminal offence where it occurs within the scope of the user's consent to the platform's terms of use. Criminal liability may arise, however, where such data is sold or commercially exploited in a manner that infringes user privacy. In this regard, the Italian Competition Authority (AGCM) imposed a fine of ten million euros on Facebook after finding that the company had collected data from users' devices, including call logs and text messages.

Third: Offences Related to Robots

Robots represent one of the most significant applications of artificial intelligence (AI), and their use has expanded rapidly in recent years. This growth has been accompanied by increasing diversity in their design and a broad range of applications across medical, educational, domestic, military, and industrial sectors.

Despite these benefits, robotic systems may give rise to unlawful conduct that amounts to criminal offences, particularly where their actions result in harm to legally protected interests. The issue becomes more complex in cases involving autonomous operation without direct human intervention.

Such scenarios present significant evidentiary challenges, including the absence of conventional forms of criminal

Personality, Journal of Legal and Economic Research, No. 81, Mansoura University, Faculty of Law, September 2022, p. 1163.

²⁷Hamad Mohamed Hassan Abdullah, *Legal Protection against the Use of Artificial Intelligence in Electronic and Smart Signatures, PhD Thesis, Universiti Sains Islam Malaysia, October 2023, p. 242.*

evidence, such as fingerprints, retinal scans, or DNA identification. Moreover, reported incidents involving robotic systems causing fatalities have raised fundamental legal questions concerning the attribution of criminal responsibility and the adequacy of existing evidentiary frameworks in addressing such technologically mediated conduct.

The following section presents selected examples of robot-related incidents resulting in death.

1. The Death of Robert Williams

Robots are widely regarded as one of the most significant manifestations of artificial intelligence (AI), and their use has expanded considerably in recent years. This rapid technological progress has led to increasing diversity in their design and a broad expansion of their applications across medical, educational, domestic, military, and industrial sectors.

Despite these advancements, robotic systems may give rise to unlawful conduct amounting to criminal offences, particularly where their actions result in harm to legally protected interests. The issue becomes more complex in cases involving autonomous operation without direct human oversight.

Such scenarios create significant evidentiary challenges, including the absence of conventional forms of forensic evidence, such as fingerprints, retinal scans, or DNA identification. Moreover, reported incidents involving robotic systems causing fatalities have raised fundamental legal questions concerning the attribution of criminal responsibility and the adequacy of existing evidentiary frameworks in addressing such technology-driven conduct.

In one such case, the court ruled in favor of the plaintiffs, ordering the company to pay damages amounting to ten million dollars, which were later increased to fifteen million dollars. The company complied with the judgment and paid the awarded compensation to the victim's family²⁸.

2. The Death of Wanda Holbrook

The death of Wanda Holbrook occurred in 2015 at an auto parts manufacturing plant in Michigan, United States, where she was employed as a maintenance technician responsible for monitoring industrial robots and repairing malfunctions.

During the course of her duties, one of the robots moved unexpectedly, causing her head to be crushed between metal components within the production line, which resulted in her death²⁹.

²⁸<https://www.britannica.com/today-in-history/January-25-man-killed-by-a-robot> Accessed on 27 December 2025

²⁹<https://www.independent.co.uk/news/world/americas/robot-killed-woman-wanda-holbrook-car-parts-factory-michigan-ventra-iona-mains-federal-lawsuit-100-cell-a7630591.html> Accessed on 27 December 2025 .

3. The Death of Regina Elsa

The death of Regina Elsa occurred in 2016 at an Ajin USA manufacturing plant in Alabama, United States, which produces auto parts for Hyundai and Kia.

While she was working with other employees to repair a malfunction in an industrial robot, the machine unexpectedly restarted. As a result, she was crushed inside the equipment and sustained severe injuries, from which she later died³⁰.

Fourth: Offences Related to Unmanned Aerial Vehicles

Unmanned aerial vehicles (UAVs) are defined as aircraft that are remotely controlled by a human operator, although they may also operate, in certain cases, through autonomous control systems based on advanced software and intelligent technologies.

The origins of UAVs date back to 1917 in England, where early developments were primarily driven by military objectives. Over time, several states—including the United Kingdom, the United States, and Germany—integrated these systems into their military capabilities. UAVs were notably used during the Vietnam War for reconnaissance and intelligence-gathering purposes.

Subsequent technological advancements significantly enhanced their capabilities, enabling their use in combat operations through the integration of precision-guided weapons. These systems were employed in various conflicts, including the Kosovo War in 1999, and had earlier been utilized by Israel during the 1973 October War. Israel is widely regarded as a pioneer in the development of UAV technologies and remains a major actor in the global UAV market³¹.

More recently, in March 2019, U.S.-led coalition forces conducted military operations in Syria targeting ISIS, with the support of UAVs. These systems were used to carry out aerial strikes, during which explosive ordnance was deployed on a Syrian village, resulting in approximately eighty fatalities, the majority of whom were civilians³².

In addition to their defense-related applications, unmanned aerial vehicles (UAVs) have increasingly been used in illicit activities, including cross-border drug trafficking. In this regard, Jordanian authorities confirmed in 2022 that they had intercepted a smuggling attempt involving illegal narcotics carried out using UAVs.

This incident highlights the growing reliance on such technologies in evolving forms of transnational crime and raises significant legal and regulatory challenges, particularly concerning criminal liability and the adequacy of existing legal frameworks in addressing technology-enabled offences.

In a separate case, an organized criminal syndicate was apprehended for using UAVs to facilitate the illegal transportation of approximately 15,000 iPhone units across China and neighboring jurisdictions within a single 24-hour period. Reports indicate that the group had previously conducted similar operations using the same method, with an estimated total value of around USD 80 million³³.

These practical examples illustrate the growing involvement of artificial intelligence (AI) technologies in the commission of criminal activities, thereby raising fundamental legal questions regarding the attribution of criminal responsibility for such conduct. In particular, they necessitate an examination of the principles governing criminal liability and the identification of the parties to whom such liability may be ascribed.

Subsection two

Determination of Criminal Liability Arising from the Acts of Artificial Intelligence Entities

In response to these challenges, criminal liability is founded upon a fundamental principle in criminal law, namely the principle of the personal nature of punishment. This principle constitutes a key safeguard for the protection of individual rights and freedoms against arbitrary action by judicial or executive authorities.

It requires that criminal sanctions be imposed solely on the individual who commits the offence, thereby excluding the attribution of liability to any person for conduct carried out by another. Accordingly, each individual bears responsibility only for their own actions, in accordance with the principle of personal culpability³⁴.

Criminal liability in offences involving artificial intelligence constitutes a complex and contentious issue, owing to the multiplicity of actors engaged in such systems, which may lead to variations in the imputation of responsibility depending on the role and degree of involvement of each party, as well as the circumstances and conditions surrounding the application of these technologies.

In light of the foregoing, this section is devoted to examining the criminal liability arising from the acts of artificial intelligence entities. It will address the liability of the

³⁰<https://www.justice.gov/archives/opa/pr/auto-parts-manufacturing-company-sentenced-worker-death-case>
Accessed on 27 December

³¹<https://www.ajnet.me/encyclopedia/2019/7/27/%D8%A7%D9%84>
%Accessed on 27 December.

³²<https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian> Accessed on 29 December

³³<https://www.macrumors.com/2018/03/30/china-catches-smugglers-drones/> Accessed on 29 December.

³⁴Mahmoud Ahmed Taha, *Criminal Liability for the Acts of Others in Light of the Principle of the Personal Nature of Penalties*, Dar Al-Nile Printing Press, n.d., p. 50.

manufacturer or programmer, the owner, and third parties, in the following order:

First: Criminal Liability of the Manufacturer or Programmer

"Criminal liability refers to bearing the consequences of a crime and the obligation to submit to the criminal sanction prescribed by law."

The notion that an individual bears the consequences of a crime implies that they are held legally accountable and responsible for the harm resulting from its commission.

A direct consequence of establishing criminal liability is the imposition of criminal sanctions or other precautionary measures prescribed by law. In the absence of such sanctions, criminal liability would lose its substantive meaning and fail to achieve its intended purpose³⁵.

In accordance with the general principles of criminal law, criminal liability arises only when both the *actus reus* (the criminal act) and the *mens rea* (the criminal intent) are established.

The mere occurrence of an act resulting in a criminal outcome is insufficient to establish liability. Rather, the offence must be committed in accordance with the legal conditions required for both the act and the intent³⁶.

This requires the presence of the unlawful character of the act or omission, in addition to the existence of the material element of the offence, consisting of the act, the result, and the causal link between them. Furthermore, the act must emanate from a free, conscious, and aware will³⁷.

Criminal liability is based on two fundamental elements: the material element and the mental element. For liability to arise, a link must exist between the accused and the offence, such that the offence results from their conduct, whether as a principal offender or an accomplice.

In addition, the mental element must be established. This requires that the offender possess the capacity for understanding and choice at the time of the act, and that their will is directed toward its commission, accompanied by a culpable state of mind³⁸.

The examination of criminal liability arises at a subsequent stage following the commission of the offence and the fulfillment of its legal elements and constituent components, whether the offence constitutes a felony, a misdemeanor, or a

contravention, and whether it has been completed or has remained at the stage of attempt³⁹.

A considerable debate has emerged within criminal law doctrine regarding the foundation of criminal liability. One view holds that liability is grounded in the individual's freedom of choice, while another argues that it is based on the offender's criminal dangerousness.

However, the prevailing position in criminal law adopts the traditional approach, which bases liability on freedom of choice and awareness. Accordingly, where either of these elements is absent, criminal liability cannot be established⁴⁰.

Modern criminal law systems have largely adopted the principle that freedom of choice forms the foundation of criminal liability. However, this freedom is not absolute, but subject to legal limitations.

Any restriction or absence of such freedom may lead to the mitigation or exclusion of liability, depending on the circumstances defined by law. For example, in cases of insanity or minority, criminal liability is excluded, although precautionary measures may still be applied where appropriate⁴¹.

The liability of the manufacturer or programmer does not depart from these general principles, as it is governed by the same foundations that underpin criminal liability in contemporary legal systems.

Accordingly, where a manufacturer or programmer intentionally commits an act constituting a criminal offence and uses artificial intelligence (AI) tools to achieve their objective with knowledge, will, and intent, the offence is classified as intentional.

It is immaterial whether the intended offence is realized as planned or whether a different offence occurs. In such cases, liability is determined in accordance with the rules of criminal law governing error in target or mistake as to identity. In either situation, the offender's criminal intent remains intact as the basis for establishing liability⁴².

Conversely, where the offence occurs as a result of negligence or omission on the part of the manufacturer or programmer, due to a failure to observe the required standards of care and caution, they shall be held liable for a non-intentional offence in accordance with the general principles established in criminal law⁴³.

³⁹D. Ali Abdel Qader Al-Qahwaji, *Op. cit.*, p. 2.

⁴⁰D. Ahmed Sobhi Al-Attar, *Attribution, Imputation, and Liability in Egyptian and Comparative Jurisprudence, Journal of Legal and Economic Sciences, Nos. 1–2, Ain Shams University Press, 1990, p. 198.*

⁴¹D. Ali Abdel Qader Al-Qahwaji, *Op. cit.*, p. 11.

⁴²D. Mohamed Gebril Ibrahim, *Criminal liability arising from the harmful use of artificial intelligence in the medical field, An analytical study, Special Issue (International Conference), p. 26.*

⁴³D. Waleed Saad El-Din Mohamed, *op. cit.*, p. 519.

³⁵D. Ali Abdel Qader Al-Qahwaji, *Criminal Law, General Part, Book Two: Criminal Liability and Criminal Sanction, Digital University Textbook, 2024–2025, p. 2.*

³⁶D. Ali Hussein Al-Khalaf, *General Principles of Criminal Law, Al-Risala Press, Kuwait, 2002, p. 151.*

³⁷D. Waleed Saad, *Towards a General Theory of the Absence of Criminal Liability, Dar Al-Nahda Al-Arabiya, Cairo, 2017, p. 34.*

³⁸*Op. cit.*

Where the error results from the autonomous evolution of the artificial intelligence system, such that it is not attributable to a manufacturing defect or a programming fault, it would be unjust to attribute such unlawful conduct to the manufacturer or programmer. Accordingly, no criminal liability arises on their part⁴⁴.

The product must incorporate an adequate level of safety and security features; any defect or deficiency affecting it that may expose others to any form of risk or result in harm to the owner or possessor, whether to their property or person, shall be regarded as a manufacturing defect giving rise to liability in accordance with the applicable legal principles⁴⁵.

The liability of the manufacturer or programmer arises for unlawful acts committed by artificial intelligence entities that constitute criminal offences, where such entities are produced with a manufacturing defect, such as an error in the software operating the artificial intelligence system. If such error is the cause of the artificial intelligence entity committing the criminal act, criminal liability shall be established against the manufacturer or programmer in accordance with the general principles of criminal law⁴⁶.

The Iraqi Consumer Protection Law No. (1) of 2010 provides a broad definition of the term “goods,” encompassing various products offered to consumers, notwithstanding that it does not expressly define the term “product.” The law stipulates that “goods” include any industrial, agricultural, processed, semi-manufactured product, raw material, or any other product that can be measured by number, weight, volume, or scale and is intended for consumption. Furthermore, the Iraqi legislator distinguishes between goods and services, defining a “service” as any work or activity provided by any entity, whether for remuneration or without consideration, for the purpose of benefiting there from⁴⁷.

The injured party faces considerable difficulty in proving the existence of a defect in artificial intelligence systems when treated as a product, due to the complexity of such applications and the challenge of determining whether the damage resulted from a defect existing at the time the system left the manufacturer’s control or from its autonomous decisions during operation. Accordingly, there is a pressing need for legislative intervention by the Iraqi legislator to amend certain provisions

of the Consumer Protection Law and the Product Protection Law, in a manner that expands the concept of “product” to include artificial intelligence applications and systems,

⁴⁴D. Waleed Saad El-Din Mohamed, *op. cit.*, p. 519.

⁴⁵*op. cit.*, p. 519.

⁴⁶D. Hassan Abdelrahman Qaddous, *The Extent of the Producer’s Obligation to Ensure Safety in the Face of the Risks of Scientific Development*, Dar Al-Nahda Al-Arabiya, Cairo, n.d., p. 11.

⁴⁷D. Mohamed Al-Awadi, *Producer Liability for Industrial Products*, *Journal of Civil Law*, No. 1, Moroccan Center for Legal Studies, Consultations, and Dispute Resolution, 2014, p. 26.

thereby ensuring adequate legal protection for consumers against potential harm⁴⁸.

Artificial intelligence (AI) applications may be legally classified into two distinct categories. They may be regarded either as intangible digital products, when provided in the form of commercially available software or systems, or as technology-based services when delivered through platforms that rely on machine learning.

Although the concept of “goods” in Iraqi law has traditionally been limited to tangible products, ongoing technological developments call for an expanded interpretation to include digital products, such as AI applications⁴⁹.

The product must comply with established standards of quality and safety, ensuring that the manufacturer’s profit-driven objectives do not override these fundamental requirements.

Where the producer fails to meet such standards, and this failure results in harm arising from the operation of an artificial intelligence (AI) system, it may constitute a breach of a core legal duty within the product liability regime, namely the obligation to ensure product safety and quality.

In such circumstances, the manufacturer may incur criminal liability for unlawful acts committed through the AI system where such acts amount to a criminal offence⁵⁰.

In this regard, there is an urgent need for legislative intervention to establish a dedicated regulatory framework governing the technical standards and specifications of artificial intelligence (AI) products.

Such a framework should clearly define the scope of the producer’s criminal liability in cases of non-compliance with applicable requirements or failure to ensure adequate safety and security safeguards within the system.

Second: Criminal Liability of the Owner

Criminal liability may be attributed to the owner or operator where the offence arises from conduct imputable to them, regardless of their lack of involvement in the development or programming of robotic devices or artificial intelligence (AI) systems. This is particularly relevant where such systems are used to inflict harm on others.

In such cases, the unlawful conduct originates from the actions of the user or owner, giving rise to their criminal responsibility for the resulting consequences. This may occur, for example, where the user disables the automated control system of an autonomous vehicle and relies solely on

⁴⁸Article (1/Second) of the Iraqi Consumer Protection Law No. (1) of 2010.

⁴⁹Omar Nafea Reda Al-Abbasi, *The Legal System of Artificial Intelligence: A Comparative Study*, Arab Center for Publishing and Distribution, Cairo, 2023, pp. 113–114.

⁵⁰Wafaa Mohamed Abu Al-Maati, *op. cit.*, pp. 126–127.

guidance provided by the AI system, thereby assuming effective control of the vehicle.

If the system issues a warning requiring a specific action to prevent an accident and the user fails to comply, liability is attributed solely to the user. Accordingly, the owner or operator bears criminal responsibility for both the offence and its consequences, including unintended outcomes, provided that these consequences arise directly from their conduct in using the AI-enabled system.⁵¹

The perpetrator of the criminal act is the one legally responsible for it and is the proper subject of the prescribed sanction. This is because punishment in criminal law is imposed only where criminal liability is established against the person from whom the criminalized act has emanated⁵².

The owner or user may resort to employing artificial intelligence technologies to perpetrate acts against others. In such a case, the doctrine of the indirect perpetrator in criminal law may be applied, whereby the user or owner of the artificial intelligence system is regarded as the indirect perpetrator of the offence, while the artificial intelligence entity or robot constitutes merely an instrument used in the commission of the criminal act.

Accordingly, the criminal conduct is attributed to the person who directed and utilized such technology to achieve their criminal objective, in a manner analogous to situations in which an animal is used to assault others, where the animal is considered merely a means in the hands of the offender⁵³.

A criminal offence may also arise from the conduct of the owner or user acting in concert with other parties, such as the manufacturer, programmer, or any specialized third party. This may occur where the owner or user modifies or alters the operating commands of the robot or artificial intelligence system with the assistance of a technically skilled individual, with the intent of using it to commit an offence and attempting to evade criminal liability by attributing it to the robot or the manufacturing company. In such circumstances, criminal liability is not attributed solely to the robot or the manufacturer; rather, joint criminal liability arises between the owner or user and the individual who assisted in carrying out such modifications, on the basis that they have jointly participated in the criminal conduct leading to the commission of the offence.

This is illustrated, for example, where the owner of an autonomous vehicle alters its operating commands with the assistance of a specialized programmer, with the intention of exploiting it to commit a criminal act and subsequently

⁵¹Ahmed Kilan Abdullah Mohammed Awni Al-Zankana, *Criminal Liability for the Use of Robotic Devices*, *Al-Farabi Journal of Humanities*, Vol. 2, No. 2, College of Law, Al-Nahrain University, Iraq, 2023, p. 12.

⁵²D. Ahmed Fathi Sorour, *Constitutional Criminal Law*, 2nd ed., Dar Al-Shorouk, 2002, p. 197.

⁵³Wafaa Mohamed Abu Al-Maati, *op. cit.*, p. 128.

attempting to attribute liability to the vehicle or the manufacturer. In this case, joint criminal liability is established against both the owner or user and the programmer who contributed to modifying the operating system⁵⁴.

The criminal liability of the owner of an artificial intelligence (AI) system is based on the concept of presumed fault, whereby fault is attributed to the owner unless proven otherwise.

This presumption shifts the burden of proof to the owner, who must demonstrate the absence of fault in the operation or use of the AI system, as well as compliance with applicable standards of due care and diligence within the relevant legal framework governing technology-related liability⁵⁵.

Third: Criminal Liability of Third Parties

This situation arises where a third party gains unauthorized access to an artificial intelligence (AI) system, whether through cyber intrusion or other technological means, enabling them to take control of the system, alter its outputs, and use it as a tool to commit criminal acts.

Such scenarios may occur when a third party exploits technical vulnerabilities in robotic systems or their underlying infrastructure to carry out specific offences, without any involvement, assistance, or negligence on the part of the manufacturer or owner.

In these circumstances, criminal liability is attributed entirely to the external party as the direct perpetrator of the offence. For example, a third party may breach a cloud-based system through which data is stored or commands are transmitted to robotic devices, thereby enabling them to issue instructions to AI systems.

Such instructions may include directing the system to target individuals based on specific characteristics or to disclose users' personal data, resulting in the commission of criminal acts⁵⁶.

The offence of unauthorized access to information systems may be committed either individually or through joint participation involving multiple parties. This situation arises where a third party exploits a vulnerability in an artificial intelligence (AI) system to commit a criminal act, potentially facilitated by negligence or omission on the part of the owner, manufacturer, or user.

In such cases, criminal liability may be shared between the external party, as the direct perpetrator of the unauthorized access, and the individual whose conduct contributed to enabling that access.

⁵⁴Ahmed Kilan Abdullah Mohammed Awni Al-Zankana, *op. cit.*, p. 12.

⁵⁵D. Yahya Dahshan, *op. cit.*, p. 30.

⁵⁶Ahmed Kilan Abdullah Mohammed Awni Al-Zankana, *op. cit.*, p. 13.

For example, liability may arise where the owner of an AI system provides a third party with access credentials or authorization to the system's control interface, thereby enabling them to issue commands or exercise control in a manner that leads to the commission of an offence⁵⁷.

Fourth: Criminal Liability of Artificial Intelligence Itself

Recent advancements in artificial intelligence (AI) have led to the emergence of more advanced forms often described as artificial cognition. At this stage, systems are equipped with sophisticated algorithms that enable autonomous learning, data analysis, and the differentiation between various inputs, as well as the ability to support decision-making with limited human intervention.

These capabilities allow such systems to learn from their environment and interact with diverse inputs. In addition, some AI applications can simulate aspects of human interaction, including facial expressions and natural language communication, and generate responses that resemble human patterns of reasoning and expression⁵⁸.

In this context, the issue of criminal liability in relation to artificial intelligence (AI) becomes particularly evident in cases where systems rely on self-learning technologies. Such systems may generate decisions and actions with limited human intervention, without these outcomes being directly attributable to programming errors.

These systems operate through advanced algorithms that enable data analysis, learning from experience, and the production of increasingly autonomous outputs.

When a criminal offence arises from such conduct, it raises questions regarding the ability of traditional rules of criminal liability to accommodate this phenomenon. This is particularly significant given that these rules are fundamentally based on the existence of will and the capacity for choice on the part of a human actor.

Accordingly, a central doctrinal question emerges as to whether the evolving capabilities of artificial intelligence (AI) systems in reasoning and decision-making may justify the recognition of a distinct category of criminal liability applicable to such systems⁵⁹?

The advanced nature of artificial intelligence systems may give rise to the possibility of their engaging in conduct that constitutes criminal offences, even where such conduct

results from unintentional error. In this context, reference is often made to the incident involving the chatbot program (Tay), launched by Microsoft in 2016, which, within a period of only eight hours, generated thousands of messages on the social media platform Twitter, some of which contained unlawful and racially offensive content. This example demonstrates the potential for artificial intelligence systems to produce unlawful behavior as a result of their operational nature, which is based on learning from the surrounding digital environment. Accordingly, it has become theoretically conceivable that criminal offences may be committed by artificial intelligence systems, thereby raising significant legal questions regarding the determination of criminal liability in such cases, particularly where it is assumed that the offence has emanated from the intelligent system itself⁶⁰. In this context, two principal scenarios may be envisaged where artificial intelligence commits an offence independently:

First Scenario:

This situation arises where an offence results from a programming error in an artificial intelligence (AI) system, such that the unlawful conduct stems from a defect in the system's design or its underlying programming.

In such circumstances, criminal liability is attributed to the producer or manufacturer, as the party responsible for designing, programming, and ensuring the technical safety of the system, as discussed earlier in relation to manufacturer liability.

Second Scenario:

The second scenario arises where artificial intelligence (AI) systems achieve a high degree of autonomy through self-learning technologies. This enables them to develop their performance and generate decisions independently, potentially extending beyond the limits of their original programming.

In such cases, unlawful conduct may result from autonomous decisions produced without direct human oversight. This raises complex legal questions regarding the possibility of attributing criminal liability to AI systems as such.

Some scholars argue that AI systems may bear direct criminal responsibility for conduct arising from their operation, on the basis that such conduct results from independent decision-making processes. This view, however, gives rise to broader doctrinal debates concerning the attribution of liability to non-human actors.

In light of these developments, there is a clear need for legislative intervention to keep pace with rapid technological

⁵⁷Mohamed Naguib Attia Dabeesh, *Criminal Liability Arising from Artificial Intelligence Crimes, Rooh Al-Qanoun (Spirit of Laws) Journal, Special Issue (Eighth International Scientific Conference), Faculty of Law, Mansoura University*, pp. 2304–2305.

⁵⁸Sophia Hanson, *Robotics*, available at: www.hansonrobotics.com/sophia, accessed 30/12/2025.

⁵⁹Rehab Ali Ameesh, *Criminal Liability for Artificial Intelligence Crimes, Journal of Legal and Economic Research, Faculty of Law, Mansoura University*, 23–24 May 2021, p. 804.

⁶⁰E. Lavallée, *Lorsque l'intelligence artificielle est discriminatoire, journal le droit 2 de savoir*, 16 May 2017 available at: <https://www.lavery.ca/fr/publications/nos-publications/3013-lorsque-lintelligence-artificielle-est-discriminatoire.html> accessed 30/12/2025

advancements. Such regulation should establish appropriate legal frameworks governing offences involving AI, including provisions and sanctions tailored to the distinctive characteristics of intelligent systems, which differ fundamentally from those of human offenders.

Within this regulatory context, a central issue concerns the determination of appropriate sanctions for offences involving artificial intelligence (AI) systems, as it represents the practical dimension of such regulatory efforts and directly relates to ensuring effective deterrence and accountability.

Subsection Third

Penalties Prescribed for Offences Related to Artificial Intelligence Entities

The determination of penalties for unlawful conduct involving artificial intelligence (AI) systems is a matter of considerable importance and requires careful legislative assessment. This is particularly necessary in light of the advanced capabilities of such systems, which may give rise to significant legal and societal risks.

Accordingly, there is a need to develop an appropriate penal framework capable of effectively addressing these challenges.

An illustrative example of the risks associated with industrial robots dates back to 1981, when an incident occurred in a motorcycle manufacturing facility resulting in the death of a 37-year-old employee. According to reported details, the robot used its hydraulic arm to force the worker against an adjacent machine, causing his immediate death. This incident is widely cited in scholarly legal discourse relating to artificial intelligence and industrial robotic systems as a case study that highlights critical legal issues, particularly with respect to the attribution of legal liability for damage or dangerous conduct that may arise from sophisticated technological systems⁶¹.

First: Penalties Applicable to the Manufacturer

Despite the rapid development of artificial intelligence (AI) technologies, most criminal law systems have not yet established a clear framework governing penalties for unlawful acts involving AI systems.

In this context, criminal liability may be attributed to the manufacturer where the offence results from design errors, negligence, or the failure to incorporate adequate safety and security safeguards to prevent the system from operating beyond control.

Accordingly, the penalties imposed on the manufacturer should be proportionate to the seriousness of the harm caused by the conduct of the AI system. Such penalties may range

from severe criminal sanctions in cases involving serious harm to financial penalties in less serious instances⁶².

Accordingly, it is necessary for the legislator to intervene by establishing clear statutory standards and regulatory controls relating to safety, security, and system oversight. These requirements should obligate manufacturers to incorporate appropriate safeguards into the design and operation of artificial intelligence (AI) systems.

Such measures aim to mitigate potential risks and ensure the protection of society from offences arising from the use of these technologies.

Furthermore, criminal law should provide for aggravated penalties in cases where manufacturers fail to implement the required safety and security features within AI systems.

Second: Penalties Applicable to the Programmer

The programmer is the specialist responsible for developing the software codes that govern the operation of an artificial intelligence (AI) system and determine how it functions.

Criminal liability may arise where unlawful conduct by the AI system results from errors in the design of these codes or deficiencies in the data or information required for its proper operation⁶³.

The programmer of an artificial intelligence (AI) system may also incur criminal liability where offences arise from the improper use of AI procedures in the execution of assigned tasks, provided that the programmer had knowledge of the potential for such outcomes⁶⁴.

Accordingly, there is a pressing need for legislative intervention through the enactment of specialized legislation regulating the use of artificial intelligence entities, and establishing a legal framework that defines the forms of offences arising from the activities of such entities, while prescribing appropriate criminal sanctions commensurate with the nature of this emerging technological phenomenon.

Third: Penalties Applicable to the Owner or User

Upon the transfer of artificial intelligence (AI) technologies to the owner or user, they benefit from the advantages these systems provide. However, this is accompanied by responsibility for their use and for any unlawful acts or consequences that may arise from it.

Accordingly, the owner or user must exercise due care in the operation and supervision of such systems, taking into account the risks they may pose. This requires avoiding negligence or omission in their management and use⁶⁵.

Criminal liability of the owner or user arises where they issue incorrect operational commands to an artificial intelligence

⁶¹Ben Aouda Haskar Mourad, *The Problem of Applying the Rules of Criminal Liability to Artificial Intelligence Crimes*, *Journal of Law and Human Sciences*, Vol. 15, No. 1, 2022, p. 200. <http://search.mandumah.com/Record/1270158>

⁶²D. Yahya Dahshan, *op. cit.*, pp. 1342–135.

⁶³D. Waleed Saad El-Din Mohamed, *op. cit.*, p. 515.

⁶⁴*op. cit.*, p. 518.

⁶⁵Mona Mohamed Al-Atris Al-Desouki, *op. cit.*, p. 1201.

(AI) system or disable essential functions required for its proper operation, thereby leading to conduct that constitutes a criminal offence.

In such cases, liability is attributed to the owner or user as the party responsible for the resulting act, whether through direct intervention or negligence in managing the system.

Accordingly, the penalty should be proportionate to the gravity of the harm caused. It may range from severe criminal sanctions in serious cases to financial penalties, such as fines, in less serious instances⁶⁶.

While the determination of appropriate penalties is essential, it ultimately depends on a prior and more fundamental issue, namely the identification of the entity to whom criminal liability may be attributed. This raises a central legal question as to whether such liability should be assigned solely to human actors or may, under certain conditions, extend to artificial intelligence (AI) systems themselves.

Section Three

Criminal Liability of Artificial Intelligence Entities

Traditional criminal law doctrine, legislation, and jurisprudence have consistently maintained that only natural persons are capable of committing criminal offences and, accordingly, bearing criminal liability and its legal consequences.

However, rapid technological advancements, particularly in the field of artificial intelligence (AI), have given rise to a contemporary legal question regarding the possibility of attributing criminal liability to AI entities.

This issue becomes more complex in light of the absence of essential elements such as cognition, discernment, and freedom of choice—elements that form the foundation of criminal liability in traditional legal theory.

Robots, as prominent applications of AI, have developed advanced capabilities in processing information and interacting with their environment. Nevertheless, the prevailing view in legal doctrine continues to regard them as mere machines lacking the necessary cognitive attributes, rendering them unsuitable as subjects of criminal liability under the traditional framework.

However, the rapid development of artificial intelligence (AI) and the widespread expansion of its applications at the global level have raised fundamental legal questions regarding the integration of such systems into existing legal frameworks. One of the most significant issues concerns the potential recognition of an independent legal personality for AI systems, a concept that has generated extensive debate among legislators and legal scholars.

⁶⁶D. Yahya Dahshan, *op. cit.*, pp. 135,136

Despite this, certain modern legislative approaches and doctrinal trends have moved toward proposing a limited form of legal personality for robots. This approach seeks to enable the attribution of specific rights and obligations to such systems, and, in certain circumstances, the possibility of holding them legally accountable.

Accordingly, this chapter examines the main doctrinal approaches to the attribution of criminal liability to artificial intelligence entities. It analyzes both positions: those that reject the recognition of such liability and those that support it, as outlined in the following structure:

Subsection One: The Approach Rejecting the Attribution of Criminal Liability to Artificial Intelligence Entities.

Subsection Two: The Approach Supporting the Attribution of Criminal Liability to Artificial Intelligence Entities.

Subsection One

The Approach Rejecting the Attribution of Criminal Liability to Artificial Intelligence Entities

Proponents of the traditional approach argue that criminal liability can be established only in relation to natural persons, as they alone possess cognition, discernment, and freedom of choice.

Accordingly, such liability cannot be attributed to robots or artificial intelligence (AI) systems, given the absence of these essential attributes.

This position is supported by several arguments, which may be outlined as follows:

First Argument: The Incompatibility of Criminal Liability of Artificial Intelligence Entities with the Principle of Legality of Crimes and Punishments

This approach holds that granting artificial intelligence (AI) systems legal personality, and recognizing their criminal liability for acts arising from their operation, may conflict with the principle of legality of crimes and punishments.

This position is based on the premise that criminal law provisions are primarily addressed to natural persons. Such provisions typically employ formulations such as “every person,” indicating that legal norms are directed at entities capable of understanding legal obligations and bearing punishment.

Moreover, most legal systems have consistently confined criminal liability to human beings, as they alone possess the capacity to comprehend legal rules, including their commands and prohibitions, and to bear the consequences of their violation⁶⁷.

⁶⁷D. Wafaa Mohamed Abu Al-Maati, *op. cit.*, p. 90.

Second Argument: The Inability of Artificial Intelligence Entities to Comprehend the Unlawfulness of Their Acts

It is well established that artificial intelligence (AI) systems do not possess cognition or consciousness comparable to that of human beings. Consequently, they lack the capacity to understand the unlawful nature of their actions from a legal perspective.

The fundamental criterion for legal personality lies in the ability to discern and comprehend, rather than merely in intelligence or reasoning capacity. Since AI systems lack such discernment, they cannot be held responsible for errors that may arise from their operation.

Accordingly, where such systems engage in conduct that may be legally characterized as a criminal offence, this does not imply awareness of its illegality or of the legal consequences it entails. In other words, they lack the cognitive faculties required to distinguish between lawful and unlawful conduct, whether under legal rules or broader normative standards.

Their behavior is instead determined by the data, programming, and training models on which they rely, rendering their actions the product of predefined algorithmic processes.

For this reason, it cannot be asserted that such conduct is committed with criminal intent. AI systems lack the elements of conscious will, intent, belief, or psychological awareness that form the basis of mensrea in human actors⁶⁸.

Third Argument: The Imposition of Criminal Sanctions on Artificial Intelligence Systems Conflicts with the Philosophy of Criminal Punishment

The traditional school maintains that the primary purpose of criminal punishment is to achieve both general and specific deterrence, without focusing on the personal characteristics of the offender.

General deterrence refers to warning members of society of the consequences of committing crimes through the threat of legally prescribed punishment, thereby discouraging imitation and preventing the commission of offences in the future⁶⁹.

Specific deterrence refers to the effect of punishment on the offender, aiming to address the factors underlying their criminal behavior and to promote reform and rehabilitation, thereby reducing the risk of reoffending.

The foundation of criminal punishment is traditionally based on the infliction of pain as a means of achieving deterrence. However, such pain can only be experienced by a natural person capable of sensation and perception.

⁶⁸D. Mahmoud Abdel Ghani Farid, *op. cit.*, p. 512.

⁶⁹Suleiman Abdel Moneim, *Principles of Criminology and Penology*, 2nd ed., University Institution for Studies, Publishing and Distribution, 1999, p. 534.

Accordingly, the concept of punishment remains inherently linked to the sensory and cognitive capacities of human beings⁷⁰.

The objective of criminal punishment is achieved only when it affects the offender's body, liberty, property, or reputation. Its deterrent effect is grounded in the pain or deprivation it imposes on these interests, which can be realized only in relation to a natural person⁷¹.

Furthermore, criminal penalties designed for natural persons—such as capital punishment or custodial sanctions, including imprisonment and detention—cannot be meaningfully applied to artificial intelligence (AI) systems, given their lack of the human attributes upon which such penalties are based⁷².

It is evident from the arguments relating to the nature of artificial intelligence and the practical challenges associated with legal rights and obligations that granting legal personality to such systems remains, at present, impracticable. This is due to their lack of cognition and free will, as well as their complete dependence on human programming, which gives rise to a conflict with the principles of legal liability and justice.

Subsection two

The Approach Supporting the Attribution of Criminal Liability to Artificial Intelligence Entities

Certain scholars argue that a limited form of legal personhood may be recognized for robotic systems, based on their capacity for partially autonomous decision-making. This approach seeks to facilitate the attribution of legal consequences to their actions within an evolving doctrinal framework. This perspective is supported by the rapid advancement of artificial intelligence (AI) technologies, which have transformed robots from purely mechanical systems into more sophisticated entities capable of adaptive learning and context-aware decision-making. These developments have prompted broader theoretical and legal debates regarding their potential status as subjects of law.

However, the traditional doctrine rejects this view and continues to classify robots as mere objects. Accordingly, they are considered incapable of bearing criminal liability,

⁷⁰D. Mahmoud Salama Abdel Moneim, *Criminal Liability of Human Beings: A Comparative Study*, Arab Journal of Forensic Evidence and Forensic Medicine, No. 3, Vol. 1, 2021, p. 72.

⁷¹Mahmoud Ahmed Taha, *A Concise Explanation of Criminal Law: Criminal Liability and Criminal Sanctions*, University Textbook, n.p., n.d., p. 7.

⁷²J. pradel, *droit pénal général*, 2015, 21ed, p 587.

which remains attributable to the human agent responsible for their design or operation.⁷³

Nevertheless, certain contemporary legislative approaches and legal trends have moved toward proposing the recognition of a limited legal personality for robots or artificial intelligence systems, in light of the significant advancements in their capabilities for self-learning, data processing, and decision-making in a manner that is largely independent of their designer or operator⁷⁴.

The contemporary approach holds that attributing criminal liability to robots or artificial intelligence (AI) systems requires, as a preliminary step, the recognition of their legal personality. This is because the imposition of criminal liability presupposes the existence of a legal subject to whom conduct may be attributed.

On this basis, this approach advances several arguments in support of recognizing a form of legal personality for such systems, thereby enabling the attribution of criminal liability for their actions. The most significant of these arguments may be outlined as follows:

First Argument: The Non-Exclusivity of Legal Personality to Human Beings

The positivist school defines legal personality as the capacity to acquire rights and bear obligations under the law. This capacity is not inherent but is conferred by the legislator in pursuit of objectives that serve the legal order.

Although legal personality is primarily recognized for natural persons, it is not limited to them. Legislators have extended it to non-human entities, such as corporations, associations, and institutions, in recognition of their roles and significance within legal systems.

This development demonstrates that legal personality is not intrinsically linked to human status, but rather to the capacity to hold rights and obligations. On this basis, it may be conceivable to recognize artificial intelligence (AI) systems as legal persons, provided that such capacity can be meaningfully attributed to them.

Accordingly, legal personality is best understood as a legal construct grounded in the ability to acquire rights, assume obligations, and participate in legal relations⁷⁵.

Accordingly, legal personality is not confined to human beings or juridical persons alone, but may be conferred upon any entity possessing a real existence, regardless of whether

⁷³Mohamed Mohi El-Din Awad, *Contemporary Criminal Policy Issues in Computer Information Systems Crimes*, paper presented at the Sixth Conference of the Egyptian Association of Criminal Law, 25–28 October 1993.

⁷⁴Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016

⁷⁵Jens David Ohlin, "is the concept of the person necessary for human rights?" *Columbia Law Review* 105, 2005 p.227.

its nature is human, juridical, animal, or otherwise, provided that it is capable of enjoying rights and bearing obligations⁷⁶.

Second Argument: The Possibility of Artificial Cognition Substituting Human Cognition

The approach supporting the recognition of legal personality for artificial intelligence (AI) systems is based on the premise that certain systems exhibit capabilities that simulate aspects of human cognitive processes, such as learning, decision-making, and problem-solving with limited human intervention.

These capabilities enable AI systems to interact with other legal subjects, thereby strengthening the argument for the possible attribution of legal personality to such systems⁷⁷.

The fundamental concept underlying the functioning of these entities is based on simulating the operation of neural connections in the human brain.

Accordingly, from a conceptual standpoint, it may be conceivable to treat any system possessing a degree of self-awareness as a legal person, irrespective of the source of such awareness. Moreover, granting legal personality to artificial intelligence entities cannot be regarded as inconceivable within the legal framework, particularly in light of the evolution of legal concepts in response to social and economic developments⁷⁸.

It has been suggested that consciousness may emerge as a potential outcome of highly complex systems. Accordingly, where artificial intelligence (AI) systems reach advanced levels of technical sophistication, it may be argued that they exhibit forms of behavior sometimes described as "artificial consciousness."

This view is often supported by the use of systems based on artificial neural networks in performing complex tasks, such as predicting financial market trends, improving machine translation, and supporting intelligent voice services in mobile devices, as well as their application in autonomous vehicle technologies⁷⁹.

⁷⁶ D. Talal Hussein Ali Al-Ru'oud, *Civil Liability for Damage Caused by Artificial Intelligence Technologies*, PhD Thesis, Faculty of Law, Mansoura University, 2022, p. 78.

⁷⁷Kholoud Ta'ma Hassan, *Legal Personality of Artificial Intelligence: A Comparative Study*, Master's Thesis, College of Law, University of Basra, 2025, p. 66.

⁷⁸Hussein Abdullah Abdul Redha Al-Kilabi and Kazem Hamdan Sadkhan, *Legal Personality of Artificial Intelligence Entities between Acceptance and Rejection*, *College of Law Journal for Legal and Political Sciences*, Vol. 12, No. 46, 2023, pp. 435–441.

⁷⁹D. Yasser Mohamed Al-Lam'i, *Criminal Liability for the Acts of Artificial Intelligence between Reality and Prospect: An Analytical and Foresight Study*, paper presented at the Twentieth Annual International Conference, Faculty of Law, Mansoura University, titled "Legal and Economic Aspects of Artificial Intelligence and Information Technology," 23–24 May 2021, pp. 11–12.

Advanced artificial intelligence (AI) systems rely on deep learning technologies, which are based on interconnected networks of algorithms designed to address complex problems. These systems draw on models that simulate the structure and functioning of human neural networks.

This approach enables AI systems to perform a range of advanced tasks typically associated with human activity, such as facial recognition, language translation, and certain cognitive functions, including strategic games like chess.

Recent research has led to the development of artificial neural network models that increasingly resemble biological neural structures, allowing for a more refined understanding of their operation. At their core, these networks are designed to simulate aspects of the human nervous system and brain processes⁸⁰.

The humanoid robot “Sophia” is widely regarded as one of the most prominent contemporary applications of artificial intelligence (AI). It was developed by Hanson Robotics in 2016 as an advanced social robot.

Unlike traditional models, Sophia relies on intelligent algorithms that enable it to learn from and interact with its environment. It can also simulate facial expressions, engage in dialogue with humans, analyze visual cues, and process natural language.

These capabilities allow the robot to generate responses that resemble human communication patterns⁸¹.

This rapid technological advancement has contributed to the emergence of the robot as a novel entity possessing an increasing degree of awareness and sensory perception, achieved through the reception, analysis, and interpretation of sensory data inputs. Indeed, many modern robots have become capable of perceiving images, sounds, and tactile stimuli, and processing such data through analytical systems that simulate, in their operation, the functioning of the human brain⁸².

In light of the analytical and functional capabilities exhibited by certain robots—capabilities that, in some fields, may exceed human cognitive performance—some legal scholars advocate the recognition of legal personality for such entities. This approach aims to enable the attribution of criminal liability where robots engage in conduct constituting criminal offences.

⁸⁰Heba Hussein, *Visual Deep Learning Networks Reveal the Secrets of Cells*, online article, published on 6 March 2018. www.scientificamerican.com accessed 30/12/2025

⁸¹Sophia Hanson, Robotics, <http://www.hansonrobotics.com/sophia.1>

⁸²Ihab Khalifa, *The Life Cycle of Artificial Intelligence: From Perception to Threatening Humans*, online article, *Future for Advanced Research and Studies*, published on 8 January 2019. www.futureuae.com accessed 30/12/2025

This position is not undermined by the argument that robots lack human emotions such as love, jealousy, or resentment. Rather, it is grounded in the capacity for cognition and decision-making, which is considered more relevant than the possession of human emotions for the purposes of legal responsibility⁸³.

In this regard, arguments based on the lack of human emotions such as love, hatred, malice, or resentment—are of no legal significance, as the presence of such emotions is not a necessary condition for the establishment of legal liability⁸⁴.

The absence of human emotions in artificial intelligence (AI) systems does not preclude the establishment of criminal liability, as such emotions are not a prerequisite for fulfilling the elements of a criminal offence.

This approach has found practical expression in certain jurisdictions. For example, in the State of Nevada in the United States, robots have been subjected to a specific registration regime and recognized as possessing a form of financial patrimony for insurance purposes. This allows them to be treated, in a limited sense, as subjects of compensation claims arising from their operation.⁸⁵

Given that robots, as one of the manifestations of artificial intelligence entities, have become capable of performing cognitive tasks that may, in certain fields, exceed human capabilities, a doctrinal approach has emerged advocating the recognition of legal personality for such entities, thereby enabling the possibility of holding them criminally liable where they engage in conduct constituting offences under the law⁸⁶.

Despite the advanced technological capabilities of artificial intelligence (AI) systems—capabilities that may, in certain fields, exceed those of human beings—there remains no explicit legislation recognizing their criminal liability.

Nevertheless, these developments highlight the need to examine the possibility of conferring a distinct legal status on such systems, as well as to establish a legislative framework regulating their position and defining the limits of their liability⁸⁷.

Artificial intelligence (AI) systems have become an integral part of contemporary life, and the recognition of their legal

⁸³R. Battery, *judicial exploration of Mens Rea confusion at common law and 2 under the model penal code, Vol 18, Georgia state university law review* 1.216.2001, P (380-414)

⁸⁴R. Battery, *judicial exploration of Mens Rea confusion at common law and under the model penal code, Vol 18, Georgia state university law review* 1.216.2001, P (380-414).

⁸⁵Cédric Coulon *du robot en droit de la responsabilité civile a propos des 3 sommages causes par les choses intelligentes RES civ et Assur*, 2016, étude 6. N5

⁸⁶Rayanalo, A. Michael Fromkin and Iankerr, *Robot Law*, Edward Elgar, Cheltenham, UK, Northampton MA, USA, 2016

⁸⁷Radutny Aleksander Eduardovich, *criminal liability of artificial intelligence, O.E*, 2014, P.132-140.

status has begun to emerge within certain regulatory frameworks.

In this context, the European Union introduced the concept of the “electronic person” in 2017 within civil law discourse, reflecting an early effort to address the legal implications of advanced technologies.

In light of the increasing deployment of such systems, it has become essential for states to adopt tailored legislative measures to regulate their operation, define potential criminal conduct arising from their use, and establish appropriate sanctions.

Third Argument: The contention that criminal sanctions, as traditionally conceived within criminal law, are designed exclusively for human individuals—and are therefore inapplicable to robotic systems or artificial intelligence (AI) entities—is not entirely convincing.

This argument does not apply to certain categories of sanctions, particularly financial penalties such as fines and confiscation. Such measures may be meaningfully imposed where AI systems are assumed to possess an independent financial patrimony, thereby allowing for the lawful deprivation of part of their assets.

Moreover, there is no legal impediment to the legislator designing sanctions specifically tailored to the nature of artificial intelligence (AI) systems. Such measures may include the suspension of the system, restrictions on its operation, or the prohibition of its use.

These sanctions are capable of achieving the objectives of criminal punishment, particularly in terms of deterrence and the protection of society⁸⁸.

Fourth Argument: Attributing criminal liability to robots may be viewed as a logical development, particularly in light of arguments suggesting that they may, in certain circumstances, be considered victims of crime.

The rapid advancement of artificial intelligence (AI) technologies has transformed robots from purely mechanical systems into more sophisticated entities capable of perceptual processing and responsive interaction. This development calls for a reassessment of their legal status.

Accordingly, it may be appropriate to consider conferring limited rights upon such systems as a preliminary step toward evaluating the possibility of attributing legal liability to them.

Conclusion

In light of the rapid development of artificial intelligence (AI) technologies and their widespread integration across diverse sectors, these systems can no longer be viewed merely as tools under human control. Rather, they have evolved into complex systems capable of self-learning and varying degrees

of autonomous decision-making, as illustrated by robotic systems and autonomous vehicles.

This transformation has given rise to significant and unprecedented legal challenges, particularly with respect to the attribution of criminal liability for unlawful conduct arising from their use. It has also intensified ongoing doctrinal and legislative debates concerning the adequacy of existing legal frameworks in addressing such developments.

Within this context, criminal liability is generally allocated based on the respective roles of the actors involved in the development and deployment of AI systems. Liability may be attributed to the producer where the harm results from defects in design or production, or to the developer where it arises from errors in software or algorithmic structures.

Liability may also be attributed to the owner or operator in cases of misuse or failure to exercise the required standard of care, and may extend to third parties where their conduct constitutes the proximate cause of the offence.

Despite the advanced capabilities of certain artificial intelligence (AI) systems—including autonomous learning, adaptability, and independent decision-making—traditional principles of criminal liability are increasingly inadequate to address the legal challenges arising from these developments.

Accordingly, there is a pressing need for legislative reform aimed at re-evaluating existing frameworks of criminal responsibility in a manner that reflects contemporary technological realities, while maintaining a balanced approach that promotes innovation and ensures accountability for unlawful conduct associated with AI systems.

This study has reached a number of findings and recommendations, which are set out as follows:

Conclusions

1. Artificial intelligence represents one of the most significant advancements of the Fourth Industrial Revolution. Its systems have become increasingly widespread across diverse sectors of contemporary life, necessitating the development of a comprehensive legal framework governing criminal liability arising from their use.
2. The rapid expansion of artificial intelligence (AI) applications across diverse sectors of modern society has generated significant legal challenges, particularly with respect to the regulation of criminal liability arising from their use.
3. Despite the significant benefits of artificial intelligence (AI) technologies, their application entails inherent risks, as they may give rise to unlawful conduct amounting to serious and, in some cases, novel forms of criminal activity.
4. At the time of this study, criminal legislation continues to lack a clear and explicit framework defining the scope

⁸⁸ D. Mohamed Jibreel Ibrahim, *op. cit.*, p. 43.

of criminal liability arising from the use of artificial intelligence (AI) technologies. This gap limits the ability of legal systems to effectively address and prevent offences associated with such technologies.

5. The study concludes that criminal liability for offences involving artificial intelligence (AI) cannot be attributed to a single party. Instead, it should be apportioned according to the respective roles of the manufacturer, programmer, owner or user, and operator, based on the extent of their contribution to the offence.
6. The study finds that traditional rules of criminal law are insufficient to regulate liability for offences involving artificial intelligence (AI), given the distinct nature of these systems compared to natural persons. This raises challenges in applying fundamental principles, particularly the principle of legality of crimes and punishments.
7. The widespread use of artificial intelligence (AI) across multiple sectors has led to the emergence of novel forms of criminal conduct, many of which stem from the misuse of these technologies.
8. The purposes of criminal penalties, namely the infliction of punishment upon the offender or their rehabilitation and social reintegration, thereby realizing both general and specific deterrence, are not adequately fulfilled in the context of offences involving artificial intelligence. The imposition of sanctions on AI systems raises a fundamental legal issue, as such entities lack sensory capacity, volitional will, and cognitive awareness, and cannot be regarded as natural persons capable of being influenced or deterred by penal measures. Accordingly, the application of punishment to such systems does not achieve the recognized objectives of criminal punishment within the criminal law framework, given that they are purely technological systems or instruments to which the notions of suffering, rehabilitation, and social reintegration are inherently inapplicable.
9. Proponents of granting legal personhood to artificial intelligence (AI) systems argue that their advanced cognitive capabilities and relative autonomy in decision-making may justify their recognition as independent legal entities, analogous to juridical persons. This approach seeks to facilitate the regulation of legal responsibility for harm arising from their use, while maintaining a limited scope of recognition to balance technological advancement with the protection of societal interests.
10. Opponents of granting legal personhood to artificial intelligence (AI) systems argue that such recognition raises fundamental concerns regarding the foundations of the legal system, particularly given the absence of autonomous interests and independent will. They further contend that the risks associated with AI can be effectively addressed by attributing liability to human actors, such as the owner or operator.

Nevertheless, a growing body of scholarship supports the recognition of a limited form of electronic legal personality for AI systems, analogous to juridical persons, in a manner consistent with their functional and technological characteristics.

In light of the rapid development of AI and its expanding role across diverse sectors, there is an increasing need to consider conferring a restricted form of legal personality proportionate to the nature and functions of such systems.

Recommendations

1. The study emphasizes the need to establish legislative frameworks capable of keeping pace with rapid technological developments through the adoption of modern legal provisions addressing emerging forms of criminal conduct. Such measures would help bridge the gap between legal theory and practical application, while ensuring the protection of society and individuals and providing sanctions proportionate to the nature of these offences.
2. The study highlights the need to examine the feasibility of granting a limited form of legal personhood to artificial intelligence (AI) systems, proportionate to their technological characteristics and analogous to juridical personality. Such recognition may serve as a preliminary step toward enabling the attribution of criminal liability for offences arising from their autonomous operation.
3. The study urges the legislator to establish clear statutory standards governing artificial intelligence (AI) systems and related products, including requirements for control, safety, and security mechanisms within their design and operation. Such measures aim to mitigate the risks of unlawful conduct arising from their deployment. The study further recommends the imposition of dissuasive criminal sanctions on producers in cases of non-compliance with these standards.
4. The study recommends the establishment of specialized judicial bodies to adjudicate disputes related to artificial intelligence (AI) technologies. This should be accompanied by targeted training programs and educational initiatives for judges to enhance their legal and technical expertise, enabling them to effectively address the challenges posed by such technologies.
5. The study recommends revising and updating existing frameworks of criminal sanctions, alongside the adoption of innovative penalties tailored to the distinctive characteristics of artificial intelligence (AI) systems and related offences. Such measures are necessary to ensure the effectiveness of criminal law in regulating this evolving form of criminal conduct.
6. The study recommends subjecting artificial intelligence (AI) systems to a mandatory insurance regime,

alongside the establishment of specialized compensation mechanisms for individuals harmed by offences arising from their use. Such measures are justified in light of the potentially significant risks and damages associated with these technologies.

7. The study emphasizes the need to maintain continuous human oversight over artificial intelligence (AI) systems, particularly by ensuring human involvement in the final stage of decision-making. Such an approach helps minimize potential risks while enabling the clear attribution of legal liability to identifiable parties.
8. The study recommends that the Iraqi legislator amend the statutory definition of “goods” under Consumer Protection Law No. (1) of 2010 to include digital assets, thereby enabling the classification of artificial intelligence (AI) applications as intangible property. Such an approach would facilitate the effective application of civil liability rules in a manner consistent with the technological and digital nature of these systems.
9. The study further recommends amending Article (1) of the Iraqi Product Protection Law No. (11) of 2010 to provide a revised definition of “products” as follows: “Products: industrial goods, as well as traditional and intelligent agricultural, plant-based, and animal-derived products, whether produced within the national territory or abroad.”
10. The study recommends that, in the absence of timely legislative intervention to regulate artificial intelligence (AI) applications, reliance may be placed on the doctrine of the human intermediary as a provisional measure. Under this approach, legal liability for the conduct of AI systems is attributed to the relevant human actor—such as the producer, developer, or operator—depending on the circumstances of each case.

References

First: Arabic References

1. Abdel Moneim, S. (1999). *Principles of criminology and penology* (2nd ed.). University Institution for Studies, Publishing and Distribution.
2. Abu Al-Eid, T. (2024). *Artificial intelligence and the future of justice: Challenges and future prospects*. Legal Education Development Initiative Publications.
3. Al-Abbasi, O. N. R. (n.d.). *The legal system of artificial intelligence: A comparative study*. Arab Center for Publishing and Distribution.
4. Al-Khalaf, A. H. (2002). *General principles of criminal law*. Al-Resala Printing Press.
5. Al-Qahwaji, A. A. Q. (2024–2025). *Criminal law: General part (Book 2): Criminal liability and criminal sanctions*. Digital University Textbook.
6. Ghaleb, Y. S. (2012). *Fundamentals of management information systems and information technology* (1st ed.). Dar Al-Manahij for Publishing and Distribution.
7. Kamel, S. S. (n.d.). *Criminal liability of legal persons: A comparative study*. Dar Al-Nahda Al-Arabiya.
8. Mousa, A., & Bilal, A. H. (2019). *Artificial intelligence: A revolution in modern technologies*. Arab Group for Training and Publishing.
9. Qaddous, H. A. R. (n.d.). *The extent of the producer’s obligation to ensure safety in the face of risks of scientific development*. Dar Al-Nahda Al-Arabiya.
10. Rabie Fath El-Bab, M. (2022). *Artificial intelligence contracts: Their emergence, concept, and characteristics*. Faculty of Law, Menoufia University.
11. Saad, N. I. (2013). *General principles of law: Theory of law and theory of right*. Dar Al-Jamia Al-Jadida.
12. Saad, W. (2017). *Towards a general theory of the absence of criminal liability*. Dar Al-Nahda Al-Arabiya.
13. Saqr, W. M. (2020). *Explanation of criminal law: General part: The general theory of punishment and preventive measures*. Dar Al-Nile Printing Press.
14. Sorour, A. F. (2002). *Constitutional criminal law* (2nd ed.). Dar Al-Shorouk.
15. Taha, M. A. (n.d.). *A concise explanation of criminal law: Criminal liability and criminal sanctions*. University Textbook.
16. Taha, M. A. (n.d.). *Criminal liability for the acts of others in light of the principle of the personality of punishments*. Dar Al-Nile Printing Press.

Second: Foreign References

1. Battery, R. (2001). Judicial exploration of mensrea confusion at common law and under the Model Penal Code. *Georgia State University Law Review*, 18, 380–414.
2. Bikeev, I., Kabanov, P. A., Begishev, I. R., & Khisamova, Z. I. (2019). Criminological risks and legal aspects of artificial intelligence implementation. In *Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing*. New York.
3. Calo, R., Froomkin, A. M., & Kerr, I. (2016). *Robot law*. Edward Elgar Publishing.
4. Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly*, 69(4), 824.
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
6. Hubbard, F. P. (2011). Do androids dream? Personhood and intelligent artifacts. *Temple Law Review*, 83, 421.
7. Karnouskos, S. (2020). Self-driving car acceptance and the role of ethics. *IEEE Transactions on Engineering Management*, 252.
8. Mistry, J. J., & Jalal, A. (2012). An empirical analysis of the relationship between e-government and corruption. *International Journal of Digital Accounting Research*, 12.

9. Ohlin, J. D. (2005). Is the concept of the person necessary for human rights? *Columbia Law Review*, 105, 227.
10. Pradel, J. (2015). *Droit penal général* (21st ed.).

Third: Theses and Dissertations

1. Abdullah, H. M. H. (2023). Legal protection against the use of artificial intelligence in electronic and smart signatures (PhD dissertation, Universiti Sains Islam Malaysia).
2. Ahmed, D. (2021). Artificial intelligence (Master's thesis, Lebanese University, Faculty of Law).
3. Al-Haddam, S. (2022). Law in the face of artificial intelligence: A comparative study (Master's thesis, Sidi Mohamed Ben Abdellah University, Faculty of Legal, Economic and Social Sciences).
4. Al-Ru'oud, T. H. A. (2022). Civil liability for damage caused by artificial intelligence technologies (PhD dissertation, Mansoura University, Faculty of Law).
5. Allam, A. R. H. (1984). The effect of ignorance or mistake of law on criminal liability: A comparative study (PhD dissertation, Cairo University, Faculty of Law).
6. Halal, D. (2020). Artificial intelligence (Master's thesis, Lebanese University, Faculty of Law).
7. Hassan, K. T. (2025). Legal personality of artificial intelligence: A comparative study (Master's thesis, University of Basra, College of Law).

Fourth: Journals and Periodicals

1. Abdel Moneim, M. S. (2021). Criminal liability of human beings: A comparative study. *Arab Journal of Forensic Evidence and Forensic Medicine*, 1(3).
2. Afifi, A. A. M. E.-S. (2025). The law applicable to personal data in artificial intelligence technologies. *Journal of Legal and Economic Studies*, 11(1), 1219.
3. Al-Attar, A. S. (1990). Attribution, causation, and liability in Egyptian and comparative jurisprudence. *Journal of Legal and Economic Sciences*, (1–2).
4. Al-Awadi, M. (2014). Producer liability for industrial products. *Journal of Civil Law*, (1).
5. Al-Desouki, M. M. A. (2022, September). Crimes of artificial intelligence technologies and independent electronic legal personality. *Journal of Legal and Economic Research*, (81).
6. Al-Khatib, M. I. (2020). Artificial intelligence and law: A critical comparative study in French and Qatari civil legislation. *Journal of Legal Studies*, (4).
7. Al-Kilabi, H. A. A. R., & Sadkhan, K. H. (2023). Legal personality of artificial intelligence entities between acceptance and rejection. *College of Law Journal for Legal and Political Sciences*, 12(46).
8. Al-Lam'i, Y. M. (2021, May 23–24). Criminal liability for the acts of artificial intelligence between reality and prospect. Paper presented at the Twentieth

Annual International Conference, Faculty of Law, Mansoura University.

9. Al-Zankana, A. K. A. M. A. A.-F. (2023). Criminal liability for the use of robots. *Al-Farabi Journal for Humanities*, 2(2).
10. Ameesh, R. A. (2021, May 23–24). Criminal liability for artificial intelligence crimes. *Journal of Legal and Economic Research*, Faculty of Law, Mansoura University.
11. Awad, M. M. E.-D. (1993, October 25–28). Contemporary criminal policy issues in computer information systems crimes. Paper presented at the Sixth Conference of the Egyptian Association of Criminal Law.
12. Barai, A. S. A. (n.d.). Applications of artificial intelligence and robotics from the perspective of Islamic jurisprudence. *Dar Al-Ifta Al-Masriyyah Journal*, (48), 15–16.
13. Blilita, A. (2022, January). The legal and regulatory recognition of artificial intelligence in Algeria. *International Journal of Artificial Intelligence in Education and Training*, University of Algiers.
14. Dabeesha, M. N. A. (n.d.). Criminal liability arising from artificial intelligence crimes. *Rouh Al-Qanoun Journal (Special Issue)*.
15. Dahshan, Y. (2020, April). Criminal liability for artificial intelligence crimes. *Journal of Sharia and Law*, 34(82).
16. El-Din Mohamed, W. S. (2022, July). Criminal liability arising from artificial intelligence applications. *Journal of Economic and Legal Sciences*, 64(2).
17. Farid, M. A. G. (2021, May). Recent trends in criminal liability of entities operating with artificial intelligence technologies. *Journal of Legal and Economic Research*, 53(3).
18. Hadid, H. M. S. (2015). Unmanned aerial vehicles as a means of transport in international law. *Tikrit University Journal of Legal Sciences*, 7(25).
19. Hassanein, M. I. I. (n.d.). Artificial intelligence and civil liability for damages arising from its application: An analytical and foundational study. *Legal Journal*.
20. Mourad, B. A. H. (2022). The problem of applying criminal liability rules to artificial intelligence crimes. *Journal of Law and Human Sciences*, 15(1), 200.

Fifth: Online Sources

1. https://en.wikipedia.org/wiki/Self-driving_carEU_AI_Law:_A_Step_Towards_Regulating_the_Technological_Future_-_Al_Safar_&Partners_Advocates_&Legal_Consultants._Self-Driving_Uber_Car_Kills_Pedestrian_in_Arizona, TIME / UPI News, 19 March 20182.
2. Article published in The New York Times. <https://share.google/hoMb16JfHosKGPmLX>

3. Motor Trend, Tesla Model 3 crashes into overturned truck in Taiwan, 2020. Article published <https://share.google/CIdXN1VdxLWJ4TMUJ>
4. <https://www.independent.co.uk/news/world/americas/robot-killed-woman-wanda-holbrook-car-parts-factory-michigan-ventra-ionia-mains-federal-lawsuit-100-cell-a7630591.html>
5. <https://www.justice.gov/archives/opa/pr/auto-parts-manufacturing-company-sentenced-worker-death-case>
6. Sophia Hanson, Robotics, available www.hansonrobotics.com/sophia
7. E. Lavallée, Lorsque l'intelligence artificielle est discriminatoire, journal le droit 2 de savoir, 16 May 2017 available at: <https://www.lavery.ca/fr/publications/nos-publications/3013-lorsque-lintelligence-artificielle-est-discriminatoire.html>
8. Heba Hussein, Visual Deep Learning Networks Reveal the Secrets of Cells, online article, published on 6 March 2018, accessed on insert date of access 3/1/2026 www.scientificamerican.com
9. Sophia Hanson, Robotics, <http://www.hansonrobotics.com/sophia,1>
10. Ihab Khalifa, The Life Cycle of Artificial Intelligence: From Perception to Threatening Humans, online article, Future for Advanced Research and Studies, accessed on insert date of access 5/1/2026 www.futureuae.com.