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

e-ISSN : 3031-7355
JCBLT, Vol. 3, No. 2, February 2026
Page 41-58

Criminal Liability for Artificial Intelligence Crimes in Iraqi Legislation "A Prospective Analytical Study in Light of Digital Autonomy"

Maher Tariq Abbas
Independent Research, Iraq

DOI : https://doi.org/10.61796/ejcblt.v3i2.1724

Sections Info

Article history:
Submitted: November 10, 2025
Final Revised: December 22, 2025
Accepted: January 17, 2026
Published: February 28, 2026

Keywords:
Artificial Intelligence
Criminal Liability
Iraqi Law
Digital Autonomy
Smart Robots.

ABSTRACT

Objective: *The paper analyzes a modern judicial problem that new technologies have imposed on legal systems, ending to the conclusion that general rules of criminal liability in the Iraqi Legal System are insufficient to address crimes created by self-learning (AI) systems. Secondly, the study will examine the extent to which the provisions of Iraqi Penal Code No. 111 of 1969 have kept pace with contemporary developments i.e. Legislative Gap (Legislative lag).* ***Method:*** *Based on a comparative analytical methodology, this research relies on international frameworks and European Parliament resolutions.* ***Results:*** *The results suggest that the break between programmer and machine created by "deep learning" puts personal liability on more difficult footing. In conclusion, the study shows that it is necessary to develop a modern legislative framework in Iraq through adopting a digital liability regime.* ***Novelty:*** *This need for a model legal framework should act as a sufficient plea against the perception of users presumed liability and incrementally granting an electronic legal personality to autonomous systems, with necessary amendments in the Iraqi Cybercrime Draft Law.*

INTRODUCTION

AI (Artificial Intelligence) is one of the most important characteristics of contemporary life. It is no longer just an auxiliary technological tool, but also a thing that has attained a certain degree of "digital autonomy", enabling it to mimic human cognitive functions and sometimes even exceed them. This evolution promises human prosperity, yet it has simultaneously created generative legal difficulties. Arguably the most vital of these developments is the rise of a category of so-called smart crimes that pose unprecedented questions on conventional criminal liability.

The main challenge of this study appears in the effective "legislative gap" within Iraqi law. While the Iraqi Penal Code No. 111 of 1969 is based on "Anthropocentric" philosophy in which criminal capacity is limited to human beings, self-learning artificial intelligence systems (Machine Learning) are now able to make decisions independently that may lead to criminal consequences unintentionally created by programmer or user. This technological reality raises a serious question that we will discuss in this study, which is whether the general rules of Iraqi legislation allow those non-human entities to be included with him under the umbrella of penalization? Or are we looking at a situation of "impunity" because the causal chain is broken between the creator of the machine and its autonomous act?

In light of Iraqi legislative steps toward accessing an anti-cybercrime law, this study has gained exceptional importance at the present time. This research aims to propose a jurisprudential and legal basis which looks for harmony between the interest

of fostering innovation and the public interest. In order to cover such a polymorphous matter completely, a comparative analytical method has been use. It means to analyze the provisions of Iraqi law and its comparison with modern comparative legislation trends, as well as European Parliament recommendations. This is done with respect to the realm of the research, which is exclusive to the civil-criminal liability of autonomous systems, thus not extending to conventional deterministic software.

Thus, the direction of this study has been mapped out to begin with an exploration of what precisely artificial intelligence is, and how it differs from a traditional tool. It subsequently examines the jurisprudential debate about its legal character and concludes with a brief overview of the practical difficulties facing the Iraqi judiciary and legislature. Lastly, it offers a vision for the future underpinned by considerations of national specificity in the political and legislative landscape with that wider view of transformative change at the digital level.

Section One: Methodological Framework and Literature Review

Subsection One: The Methodological Framework of the Research

The methodology, which is the study plan itself, and the methodological framework maps fully developed and well-focus on methods this forms the basic structure of scientific research identifying legal and logical pathways that guide researchers in answering their questions. This has become especially important, as AI is still a relatively new implementation in the Iraqi legislative system.

First: Research Problem and Questions: The research problem crystallizes in the significant legislative gap between "traditional liability rules" based on human fault, and the "advanced technological reality" of AI having decision making autonomy. The research questions are focused on the following:

1. How effective are the provisions in (Draft Iraqi Anti-Cybercrime Law) to criminalize those crimes that operate autonomously from artificial intelligence?
2. Do the general rules of the Iraqi Penal Code attribute criminal intent (mens rea) to a non-human entity (a smart robot)?
3. Who is held criminally liable once the chain of causation is broken between the programmer and the crime produced by self-teaching from a machine?

Second: Research Significance

1. Scientific Significance: Updating the Iraqi legal library with a contemporary perspective using academic developments that separates law and technology.
2. Practical Significance: Serving as a critical eye for the Iraqi legislature on the draft of the cybercrime law, to correct its short-comings before it becomes final.

Third: Research Objectives

1. What is the legal nature of AI Tool or the perpetrator?
2. The mental element of the crime in circumstances of algorithmic autonomy
3. Issue legal recommendations for intimate amendments to the Iraqi penal provisions as commensurate with the Fourth Industrial Revolution.

Fourth: Research Methodology and Scope

Adopted Methodology:

This study is fundamentally based on a comparative analytical approach to dealing with the intersection between technological concepts and legal rules, advancing through the following tracks:

1. Critical Supplemental Path: Unpacking the pertinent Iraqi legal predicates in accordance with Penal Code No. 111 of 1969, and discerning their correspondence to notions of "technological autonomy" and "self-learning." To show what they call the “legislative gap” that exists when it comes to describing crimes that are committed by AI without human volition.
2. Reconciling Modern Legal Trajectories: Analyzing the Iraqi Legislative Position and its Compatibility with Contemporary Jurisprudential Movements. Notably, this includes the European approach that has come to be known as "electronic personality," along with substantial work in Libyan and Egyptian academic circles, from which we have also had intriguingly developed opinions regarding problems like the severance of the causal link and the black box. This will mean that EU law is directly relevant when understood and worked out at court level.

Scope of the Research:

1. Subject-Matter Coverage: We are solely interested in the criminal legal assessment of liability for conduct performed by an artificial intelligence (AI) system ("robotic entity"), concentrating on the idea of indirect perpetration (perpetrator-by-means) and virtual perpetration.
2. Spatial Scope: The research is primarily centered on the Iraqi legal system, with a comparison to innovative systems.
3. Temporal Scope: The study observes the present day where there is an explosion of "Generative AI" and anticipates an upcoming "Artificial General Intelligence" (AGI) along with the new laws it will require.

Subsection Two: Literature Review and the Knowledge Gap

This new research is based on studying a set of rigorous studies that treat the issue of artificial intelligence from different angles. Prominent among these are:

1. Research paper Amna Ali Al-Hashik : This paper explored the often-debated autonomy of smart robots and showcased existing hurdles when questioning their legal personhood. It found traditional legal frameworks insufficient for the future idea of “machine consciousness [1].”
2. Research of Al-Mahdi Abdullah Al-Shafei : This study examined the liability provisions, where it has been taken into account to transverse between arguments for rejection and others in favor. This focused on the ethical and legal issues involved in distributing liability among the relevant human agents (the manufacturer, programmer and user) [2].
3. Research by Ibrahim Al-Sayed Hassanein Zayed: The research examined the "robotic entity" and attempted to establish a liability regime that recognizes

both corporate liability and the distinct independent being of the robotic entity itself with specific emphasis on criminal protection required for it.

4. Study by Nihal Kamal Zarad: This study looked at criminal liability for the actions of artificial intelligence from a future perspective It examined the ability of AI applications to commit crimes through their own volition, completely against the owner's intent [3].
5. Research by Mohammed Abdul Rahman Abdul Mohsen : This study used the "medical robot" as an applied paradigm to discuss the criminal fault that occurs from using smart surgical technologies and whether or not this is also attributed to the medical actions of a human surgeon [4].
6. One study, conducted by Taha Othman Al-Maghrabi, focused on "criminal protection" with respect to the mistakes of surgical robots from the angle of both technical and operational fault in smart medical systems [5].

First: The Knowledge Gap (Identifying the Lacunae in Previous Studies)

Despite the academic depth of these scholarly works, there remain some fundamental gaps that have not been diligently addressed, such as:

1. The Iraqi Legislative Shortcoming: However, most of the previous literature found in this vein was either general and theoretical or particularistic with reference to a jurisdiction (Egyptian, Libyan or European legislation). Thus, legal jurisprudence doesn't have an in-depth critical analysis that takes this theoretical frameworks and lay them on the debate of (Draft Iraqi Anti-Cybercrime Law).
2. The "Black Box" Dilemma: The existing literatures have not taken deep account of the "rules of criminal evidence," in plausible situations where the judge cannot ever understand how the mechanistic process was leveraged by which algorithm to reach the criminal decision.
3. The Contrast Between General and Special Rules: There is a wide gap between the fundamental principle of the Iraqi Penal Code No. 111 of 1969 (which is basically based on human perpetrator in crime) with modern, technology-leveled laws.

Second: The Contribution of Our Research in Bridging the Gap

This research will help fill in some of these gaps by doing the following:

1. Establishing the Iraqi Legislative Specificity: Through identifying and interpreting the provisions of the draft Iraqi cybercrime law and providing appropriate formulations of a provision that criminalizes the "autonomous algorithmic act."
2. The Apportioned Liability Model: The research will suggest a framework for determining the "apportionment of liability" commensurate with the Iraqi judicial environment. This guarantees that the killer (human or technological) cannot be granted impunity in the guise of "machine autonomy."
3. Bridging Technology and Sanction: Utilizing the idea of "self-learning" (as indicated by Al-Hashik's research) and convert them into concrete legal

indicators. The these indicators can be used by the Iraqi criminal judge to identify "conditional intent" (dolus eventualis) of programmer or user

RESEARCH METHOD

This study employs a comparative analytical legal research method to examine the adequacy of Iraqi criminal law in addressing crimes committed by autonomous artificial intelligence systems. The approach integrates doctrinal legal analysis with comparative perspectives to explore the gap between traditional liability principles and emerging technological realities. Primary legal sources include the Iraqi Penal Code No. 111 of 1969, the Draft Iraqi Cybercrime Law, and relevant civil liability provisions, while secondary sources consist of scholarly articles, legal doctrines, and international frameworks, particularly the European Parliament Resolution on robotics.

The analytical process is conducted through two main stages. First, a critical doctrinal analysis is applied to identify inconsistencies between anthropocentric legal principles and the concept of technological autonomy, focusing on issues such as mens rea, causation, and liability attribution. Second, a comparative analysis is carried out by examining modern legal developments in international and regional contexts to identify alternative regulatory models, including electronic legal personality and strict liability frameworks.

The scope of the research is limited to criminal liability arising from autonomous AI systems, excluding deterministic software lacking independent decision-making capabilities. Spatially, the study focuses on the Iraqi legal system while incorporating comparative insights from global legal trends. Temporally, the research addresses contemporary developments in artificial intelligence, particularly self-learning and generative systems, to anticipate future regulatory needs.

Through this methodological framework, the study aims to provide a structured legal interpretation and propose a forward-looking model for addressing the challenges of AI-related criminal liability within the Iraqi legislative context.

RESULTS AND DISCUSSION

Section Two: The Theoretical Framework and the Legal and Technological Nature of Artificial Intelligence Systems

Understanding the legal character of AI serves as a basis for setting up the rules of criminal liability. In the absence of a precise, legal definition for this body, the criminal judge must become reconciled with "personal culpability" (Personality of Punishment) and the "principle of legality" (Nullum crimen, nulla poena sine lege). We will address this in two subsections:

Subsection One: The Problematic Legal Personhood of Artificial Intelligence

First: The Essence of Artificial Intelligence and its Legal Nature

This is because, to engage in the controversy surrounding the troubling legal personhood of artificial intelligence, we must first identify its nature one of the most accurate dilemmas currently facing criminal jurisprudence. The interpretation of this

intelligence is defined by the Academy of the Arabic Language in Cairo, through Glossary of Informatics Terms [6], as "the simulation by machines and software for human cognitive capacities and their modes of operation." Indeed, the idea of essence considered in broad terms by AlShafei, goes beyond technical description, transmuting into some computational entity with a self-moving power to deduce things and generate predictions transforming its role from a tool operated externally for human purposes to that of an "effector agent" or today's "algorithmic perpetrator" acting in real life without explicit human intent [7].

The core of Artificial Intelligence, from a legal perspective is established upon the following foundations:

1. **Autonomy and Liberation from Programming:** The essence of this lie within the system's capacity to take independent action in changing environments [8]. This can break the chain of events between the designer's intent and the actual physical act itself, creating a void for assigning traditional criminal liability. The real nature of artificial intelligence as a kind of machine with what Zayed calls "self-learning" capabilities beyond human supervision giving it independent volition similar to humans. Gabriel Hallevy on which Al-Shafei based his most of the ideas about criminal AI takes this further to note that as per the nature of these systems "virtual mens rea" created by algorithms may be conceived, requiring a legal characterization suitable for their non-human character.

Questions have arisen in jurisprudence over how much legal personality can be conferred upon artificial intelligence systems (particularly autonomous robots) such that they may be held criminally culpable in their own right, separate from the agency of the creator.

Second: Jurisprudential Trends in Determining the Legal Nature of Artificial Intelligence: Between Denial and Recognition of Virtual Personhood

The Trend Denying Legal Personhood:

And so, jurisprudence a segment of which (which is the prevailing opinion in traditional approaches) holds that artificial intelligence, in however developed form, is still just a "tool" or "property" owned by a human. This argument depends on the premise that legal personhood correlates with a sense of humanity and the machine lacks the moral and societal worth in punishment[9].

This trend is the mainstream in traditional criminal jurisprudence and followed by most of Arab legislation (including Iraqi legislation). Advocates of this movement go on from a legal platitude that advanced artificial-intelligence systems, however far along in technical sophistication or "algorithmic autonomy," lack the necessary ingredients to merit being granted legal personhood and should be treated as an "object" of right rather than a "subject" of it. This proposition rests on several legal and philosophical arguments, which we summarize below:

Absence of the Mental Element (Perception and Volition):

Another Jurisprudential theory lays down two elements, material and mental where material (act) is called as actus reus by the jurisprudence and mental (intent) is

mens rea. The mental element involves guilty intent and awareness of the consequences of you act. In this regard, jurisprudence contends that robots – even those displaying intelligent behavior – do not possess "human consciousness" and moral sentiments so as to be able to grasp the nature of what they are doing or their capacity for guilt. This means that the actual machine itself lack "free will" in the legal sense and simply performs complex mathematical functions based on data inputs, which makes it incapable of committing a crime [10].

The Mechanistic Nature of Artificial Intelligence (Principle of Subordination):

This so-called "Functional Argument" claims the legal recognition of a robot as an autonomous person is inherently at odds with its functional aspect as a "tool" used by humans for their benefit. Even as the robot may seem to "learn" deeply, it does not transcend a designation of "thing" (Chose) under civil and criminal law, remaining subordinate under control of its programmer or operator. As a result, any act of harm that comes out from it is regarded in law as the "crime committed through machine", and hence attaching thereon, the liability for the benevolent and non-benevolent of these objects are ruled by common principles applicable to all living beings and objects [11].

The Inadequacy of Penal Philosophy (Lack of Deterrence):

The guiding principles of modern legislated penal policy are the concepts of "general deterrence" and "specific deterrence." Jurists consider that applying traditional criminal penalties (imprisonment or fine) to a digital entity is an exercise in legal absurdity; the robot does not suffer the loss of liberty nor is affected in his financial capacity. Not even new forms of punishment (say, in the form of digital execution or erasure) work to provide the necessary psychological deterrent, because the machine fears nothing and has no will to survive. Thus, punishing an artificial intelligence would strip the sanction of its social-moral content [12].

Fear of the Loss of Human Liability (Impunity):

Supporters of this trend warn that if they grant legal personhood to artificial intelligence, it will be used by big corporations and programmers as a "legal shield" against criminal and civil liability by pointing the finger at the "autonomous entity." The result is as a segment of jurisprudence insists on "anthropocentric law," and thus, the human must remain the only subject of rights and obligations so that there is no loss in the full realization of everything regardless of its nature, namely, to renew victims' right to compensation and punishment [13].

The Trend Supporting Virtual Personhood:

The current jurisprudence aproaches this needs for the "smart robot" obtaining a legal personality similar to the one we attribute as "legal person" (i.e. corporate entity). The purpose here is not to equate a machine with that of a human but rather create a set of legal containers whereby the intentional acts that evolved out of the system via an independent decision making process (Machine Learning) that occurs without any direct involvement from the programmer. Their stance is a result of the following reasoning [14]:

Analogy to the Corporate Personality System:

This perspective derives from the claim that legal personhood is simply a legal fiction, not a biological phenomenon. But just as the law has already given legal personhood to companies and institutions, cases without soul or body, it can also give an "electronic personhood" to smart robots. The object here is to give us an independent legal container, a vessel for the specific litigation of the system and, potentially, the imposition of specific sanctions against it [15].

Addressing the "Machine Learning" Dilemma:

Advocates of this trend claim that the creation of artificial intelligence has reached a new level, wherein it is not just a question of computer acting as some passive tool, but that AI also independently makes decisions which programmer will ever be able to foresee. In examples of 'deep learning,' the apparatus may make a criminal decision that was not included in the programming blueprints, breaking the causal connection between the programmer's act and the criminal result. In this sense, the legal personality of the robot is required, in order to blame it for its "crime", based on its role as a "criminal" [16].

Accommodating Criminal and Civil Liability:

The goal of awarding virtual personhood is not to create equivalence in rights between machine and human, it is so we can find the legal means to hold the system accountable. Such a personality allows the robot (or its generally own insurance fund) to go to civil reparations, and commensurate criminal penalties can be also set: "temporary suspension, forced reprogramming or confiscation as well as digital obliteration" [17].

Bridging the Legislative Vacuum (The Prospective Vision):

Recognizing electronic personhood, researchers argue, allows us to avert the diffusion of liability across the programmer, manufacturer and user when none are at personal fault and autonomous decision-making causes damage. The push for this approach is undergirded by global legislative trajectories, exemplified most recently in the recommendations of the European Parliament delivered as early as 2017 when it called for a legal framework meant to govern robots as 'electronic persons' [18].

Third: The Stance of the Iraqi Legislator on the Criminal Liability of Artificial Intelligence

Standard Iraqi penal legislation illustrates that the legislator has yet to set down grounds for autonomous digital entities. Instead, we still depend on the age-old notion of assigning blame. This position can be summarized by the following points:

Confinement of Legal Personhood within General Rules:

According to the Iraqi Penal Code No. 111 of 1969, the area of criminal responsibility is limited to two categories exclusively: the natural (human) person as a legal and intellectual subject, and the legal (corporate) person except for official classes under Article(80), which states:" Legal persons are responsible for crimes committed on behalf of or in their name by their representatives or manages." As AI systems do not fall under either of these characterizations, they do not possess criminal capacity within the Iraqi legislative framework [19].

Characterizing Artificial Intelligence as a "Tool" or "Object":

When there are no specified statutory provisions, the Iraqi judiciary considers AI systems as "objects" (choses) or "tools," employed by a human actor. Hence the rules of liability of "the act of a thing" or the custodianship of machines apply to them. This characterization adds complexity to prosecution of crimes in the scenarios where a decision is being made (Machine Learning) autonomously by the system that goes beyond what a programmer intended. When the turn of the judge arrives, he or she stumbles on a very big challenge: proving "chain of causation" between what a human did and the result obtained by an independently functioning AI [20], [21].

Legislative Shortcoming in Combating Smart Crimes:

The use of texts formulated in the 1960s is a clear shortcoming versus modern cybercrimes. It does not, however, satisfactorily address the penal valences of algorithmic autonomy in light of Electronic Signature and Electronic Transactions Law No. 78 of 2012. Because the Iraqi legislator does not acknowledge the virtual personhood of robots, it is therefore impossible to impose technical sanctions (for instance, deletion or reprogramming). This allows to indefinitely limit liability to the "user", who can operate in good faith and thus violates the principle of personal culpability (personality of punishment) [22].

The Imperative for Legislative Amendment:

According to the researcher, the smart Iraqi legislator is invited at present to take a prospective vision through amending the Penal Code or issuing a law antivirus for crimes that arise from artificial intelligence. This law should create a type of "presumed" or "vicarious liability" for the system's owner or operator, as well as allow precautionary measures against the software system itself to make it impossible for that criminal act to ever happen again [23], [24], [25].

Fourth: Legal Challenges Confronting the Application of Criminal Liability for Artificial Intelligence in Iraqi Law

The Iraqi legislator is experiencing a huge challenges, represented by his inability to meet the developments of the era in which we live under the supremacy of Penal Code No. 111 of 1969. The challenges can be consolidated as follows:

The Challenge of Legal Characterization and the Inadequacy of General Rules:

The root of the problem is the Iraqi legislator's attachment to or use of the canonical paradigm (of human) perpetrator. According to Al-Haidari, 2023, his study of the penal liability in Iraqi law states that autonomous smart systems will create a legal vacuum (lacuna legis). Since they are not considered traditional natural or legal persons, it is impossible to attribute a criminal act to them according to existing provisions in the law.

The Crisis of "Criminal Intent" (*Mens Rea*) in Self-Learning Systems:

The mental element (mens rea) is essential for the aggrievement (Articles 33 and 34) according to Iraqi law. The biggest difficulty comes with something called genetic algorithms, a system that can continue to test itself and make decisions humans have not coded into it, writes Yasser Al-Mamai [26]. In such cases, the "mental link" between programmer and criminal outcome is broken; classical standards of Iraqi law as someone

with a direct connection to it however make proving "criminal fault" or "intent" (dolus) incredibly difficult in these scenarios.

The Insufficiency of Traditional Punitive Measures:

In Iraq, the penal policy is based primarily on deprivation of liberty or fines. These penalties have no deterrent significance when applied to software entities, argues Khaled Mustafa Fahmy in his comparative study. Iraq does not currently have preventative or punitive countermeasures for AI (such as temporary suspension, erasure of criminal data, forced modification of algorithms) which prevent the existing penal system from fulfilling its objectives.

The Dilemma of "Independent Legal Personhood":

The idea of "electronic personhood" is gaining currency in international law (European Parliament), yet the possibility of recognizing legal agency for all entities is still far off in Iraq. According to the research of Adel Abdul Aziz Al-Senussi, this reluctance in legislation brings an extra onus upon the "user" or "owner" because they are liable to commit acts even if such actions do not move from their free will. This runs counter to the deep-seated principles of “justice of punishment” and “personal liability” in the Arab legal systems.

The Shortcomings of Anti-Cybercrime Laws:

Though Iraq had made legislative attempts to have cybercrimes regulated, that has always been failed as it tries to scour the "means" rather than the "smart perpetrator (hacker). As Yasser Al-Mamai writes, current legislation does not take note of the different types and levels of "deterministic software" or "autonomous systems that have separate technological wills". As a result, not all aspects of smart crime are covered by the law [27].

Subsection Two: The Essential Components of Technological Autonomy (An Analytical Jurisprudential Vision)

First: The Concept of Technological Autonomy

Al-Shafei asserts that the autonomy is the system's inherent ability to follow behavioral trajectories without accompanying guidance, which consequently ascribes to the machine the description of a "perpetrator" over a simple "tool [28]." Specifically, Zayed captures the essence of this idea here: 'This autonomy does not exist in a vacuum; it is enriched via Environmental Interaction through which the robot perceives its environment and adjusts its behavior according to material variables.' Al-Haddad, also clarifies this, stating that this interaction, by necessity ends up being what we understand as "Machine Learning," the process allowing algorithms to produce what are known as "non-patentable" rules of conduct that did not exist when the initial plan was drawn up.

On the other hand, Zarad states that in merging autonomy and machine learning there is an enhanced ability to predict and Decision Making embedded in the system. It is here that the artificial intelligence comes to a critical juncture, weighing its options and selecting an act which may become criminalized under the law. Eventually, this results in confirmation of Al-Hashik a Loss of Control or not being subordinated to the human programmer, that is to say: the machine's will is different from its creator's. These five

concepts, the researcher claims, are organically linked; autonomy without any aspect of machine learning as well as loss of control could not be recognized unless it had been confirmed that the system indeed made an independent decision i.e., their interaction with the environment allowed it. This creates a need for the legislator to reevaluate the traditional rules of criminal responsibility and fit them to this new technological being [29].

Second: The Severance of the Causal Link and the "Black Box" Dilemma in Iraqi Legislation

Under Iraqi criminal law, the liability of the defendant is subject to two conditions: causality between his act and the criminal result. This is the gap: if a system produces "criminal" behavior that wasn't planned for or programmed by the programmer (the "Black Box" dilemma), does this sever ongoing cause-effect linkage of effect with human?

Under Iraqi law, criminal liability is dependent upon the relation between the perpetrator's conduct and the criminal consequence being direct and material, meaning that there needs to be a direct effect of this course of conduct resulting in an outcome. Artificial intelligence has revolutionized the belief of "sufficient causation". If the system takes on autonomous criminal behavior due to self-learning, we find ourselves facing a case of severance of the causal link (novus actus interveniens) as far as the programmer or user is concerned since the harmful behavior can no longer be attributed to human volition but rather to an “autonomous algorithm”.

Also, Zayed highlights that "Black Box" problem makes it even more complex; the human has no way to visualize how conclusion of the system reached generalization, which make prediction impossible. Al-Haddad (argued that when the Iraqi judiciary relies on general rules, it may struggle to prove that, in this case, that the programmer did commit an intentional crime due to a foreign "technological factor" beyond its expectations intervening and changing the chain of events. Al-Hashik similarly describes this as generating an "impunity gap," because the machine cannot be punished according to law and there is insufficient evidence to show culpability on behalf of the human who designed it.

On the other hand, Zarad argues that the causal connection might persist in "unintentional crimes" under the heading of negligence or insufficient technical supervision [30], [31], [32]. The researcher believes that the Iraqi legislator needs as much as possible to adopt the theory of "liability for risk" (strict liability) without "fault-based liability" in relation to crimes by artificial intelligence. This ensures the protection of victims’ rights and prevents them from being compromised under the guise of cause severance or black box opaqueness, especially as there is no guidance in Article 111/1969 of the Iraqi Penal Code that may assist a judge to classify acts undertaken by any open system through pure automation.

Third: Characterization as an "Indirect Perpetrator" (*Perpetrator-by-Means*)

The researcher had attempted to clarify the legal entanglement that follows with regard to "who did it" in a smart crime, as he believes that technology applications in Iraqi universities and institutions has provided us with a form of legal characterization

referred to as "the indirect perpetrator (perpetrator-by-means). This is where the AI is a mere technological illusion behind which the programmer or human user hides, moving its end and bloodthirsty targets like a puppet.

However, the legal landscape will change fundamentally once we enter the stage of "Artificial General Intelligence" (AGI), a phase in which decision-making is no longer limited by some prior instruction and no longer limited to any cognitive capacities present amongst humans. Here our filter is the need to move from the logic of "subordination"to that of "autonomy,"something being echoed by Al-Haddad (2024, p. 1776) who argues that in parallel with this we must reckon with a reality wherein the continued deprivation of legal personhood will erode and ultimately creates us a penal vacuum not least noted because both Peacock et al as well see law most properly situated within human desire.

"Virtual perpetrator", thus, could be considered an urgent legislative vector for the future if crimes are to be prevented from attaining impunity (considering Nihal Zarad's dream vision). According to Zayed the virtual perpetrator is considered a design mechanism in order to assign liability while Al-Hashik maintains that this concept will enable the Iraqi judiciary to apply penalties on software system, and thus there is no need to demonstrate material fault of the programmer, who may have been even removed from the connection with the system since long ago. The researcher argues that based on this theory, establishing "electronic financial liability" (compensation funds) and "technical sanctions" (reprogramming/reprogramming) will become a practical solution to fill the gap left by the ineffectiveness of traditional provisions in the Iraqi Penal Code, allowing AI to transform from being an irresponsible loophole for criminality into an accountable entity before the law.

Subsection Three: The Analytical Approach to the Correlational Relationship Between Research Variables

In this research, the correlational relationship is therein defined through the dialectical tension between technological expansion and regulatory stagnation, from which emerges following dimensions that intertwine both variables:

First: The Impact of Technological Autonomy in Destabilizing General Rules:

Al Shafei, argues that the relationship between artificial intelligence and criminal liability is a "direct correlation" (positive correlation) as it grows from self-learning systems to analytical algorithms; where the gap in attributing blame to the human programmer becomes larger. Specifically, Zayed observed that technological autonomy is a "disruptive variable" with respect to the linear cause-effect condition. Such is the machine’s predictive and decision-making power that human volition subsumes into digital volition, which complicates the problem of mens rea for courts.

Second: Criminal Liability and its Response to Digital Transformations:

Arguing that criminal liability is no longer simply an "effect of the act" but is now a technical respondent in need of redefinition, Al-Hashik contended. The correlation here, according to al-Haddad, relates to the transfer of liability from logic based on "personal fault" to logic of the "virtual perpetrator" so that social interests can be secured.

The academic holds that this correlation forces the legal system to shed the idea of "inanimate object" and embrace “electronic personhood” as a necessity with which to fill the penal vacuum left in the wake of human control.

Third: The Iraqi Legislative Shortcoming as an Impediment to Keeping Pace:

Comparing it to the statutory provisions, Zarad found that the imposition of liability in "natural and legal persons" as prescribed by (art. 80 of the Iraqi Penal Code) poses a "barrier" which preventing prosecution for smart cybercrimes. In a comparable fashion, Zayed asserts that this mediating variable (legislation) needs immediate synchronicity to move AI away from being an “indirect perpetrator” (perpetrator-by-means) one of which the programmer hides behind into a legal entity for virtual accountability purposes.

Fourth: Conclusion of the Researcher's Correlational Vision:

The researcher believes that the relationship between the research variables is an "imperative complementary relationship". With its inherent characteristics (learning, interaction and autonomy), artificial intelligence acts as a pressure on the classical programming of criminal liability, and then Iraqi legislation appears trapped in the middle between two contradictory requirements: enhancing the principle of legality (Nullum crimen, nulla poena sine lege) and responding to the dictates of digital justice. Such a relationship entails the shift from “liability based on the act” to “liability for technical risks” (strict liability), in order that the exercise of technological progress does not turn into a refuge for organized crime.

Section Three: Methodological Strategy and the Logic of Legal Treatment

In this sense, breaking away from boring, expert style of traditional research frameworks, "the criminal liability of artificial intelligence" the discussion needs to move into the "composite methodology", where stable text technology moves together. In this section, the methodology adopted and the mechanism used by the legislative system in Iraq to fill the cognitive and legal gap is reviewed.

Subsection One: The Adopted Methodology and Tools of Academic Deduction

Polyline, in constricting its thesis this study adopted a multidimensional methodological strategy that manifests itself in the following features:

1. **Deductive Analytical Approach:** Instead of offering a mere descriptive overview of the texts, the study focused on the philosophy behind Iraqi Penal Code No. 111 of 1969 and sought to engage with the broad principles underpinning liability or embodiment in legal terms. That is how this method was used to analyze the "crime", in light of what they classify as "self-learning" phenomenon, leading to a legal paradox: "The Iraqi penal text receives an authentic human will; however, the reality of digital crime imposes an autonomous algorithmic perpetrator."
2. **Prospective Comparative Approach:** The study used a cross-sectional comparative approach based on Iraqi national legislation and recent global legislative developments, especially European directives and strict jurisprudential trends in neighboring countries. The purpose of this comparison is not to replicate, rather it is to extract a legal model that will surpass existing shortcomings. This

enabled the treatise to theorize AI as a "virtual perpetrator," an attribution born from balancing legal scholarly opinions inclined toward the establishment of an electronic legal personality.

Subsection Two: Addressing the Dilemma and Decoupling the Text from Digital Reality

The legal treatment of the research problem centers primarily on four trajectories that bridge the "knowledge gap" which is left by the evolution of smart systems in light of the slow legislative adaptation in Iraq as follows:

First: Re-characterizing the Causal Link (Addressing the Black Box Problem):

The difference is in the general rules that apply to general intelligence, and do not have the capacity to interpret the independent decisions of AI that were never considered by their creator. Here the treatment is made according to "Liability for Technical Risks" (strict liability) theory. Some entity with an institutional face developed a system ideally suited to self-learning, and it is responsible for the likely results of that process. That keeps perpetrators from achieving impunity on the grounds of broken causation or algorithmic opacity.

Second: Transitioning from the "Indirect Perpetrator" to the "Virtual Perpetrator":

The current reality of technological applications in Iraqi institutions offers us an indirect perpetrator (perpetrator-by-means) behind whom the programmer might flee since he does not directly cause the act. The solution to this dilemma clearly lies in AGI, our very own "Virtual Perpetrator" as it were. This is a legal treatment that allows for the imposition of some sanctions (technical or financial) on the system itself, according to the analogy of liability for a legal person in Article (80) of the Penal Code, and thus guarantees a just balance between technological progress and criminal protection.

Third: Bridging the Legislative Gap via "Electronic Financial Liability" (*Independent Patrimony*):

There is an urgent need for a legal regime that ensures the operators of these systems create compensation funds, or independent financial liabilities (electronic patrimony) when smart crimes are perpetrated to compensate victims and prevent loss of victims' rights. This treatment does not merely tend to the punitive dimension, but also ensures material reparation (restitution), separating Iraqi legislation from its paralysis over "crimes without a direct human agent."

The methodology used in this research have proven that solving this dilemma under the provisions of Iraqi law does not mean "demolition" of general rules, but it is evident about their digital adaptation. The shift from the idea of «robot as tool», to "robot as a virtually responsible agent" is the only practical path towards ensuring rule of law in the age of machine intelligence. Thus, the knowledge gap shifts from being a legal barrier to an opportunity to refresh of the Iraqi penal system upon those imperatives for the third millennium.

Table 1. Summary of Addressing Gaps and Dilemmas Before, During, and After the Study

The Gap Before Research	The Proposed Treatment in the Research	The Legal Outcome
Vagueness of the Iraqi Statutory Text	Presenting a critical reading of the draft law.	Criminalizing the "Autonomous Smart Act."
Impunity of the Perpetrator under the Pretext of Machine Autonomy	The "Apportioned Liability" Model.	Safeguarding against the loss of rights (The Virtual Perpetrator).
Difficulty in Proving Criminal Intent (*Mens Rea*)	Transforming "Self-Learning" into a Legal Presumption.	Proving the "Conditional Intent" (*Dolus Eventualis*) of the operator.

CONCLUSION

Fundamental Finding: The indicated research has proved that provisions of the Iraqi Penal Code No. 111 of 1969 in its purely applied applications have become ineffective before prosecution regarding “smart crimes”. Because they rely solely on conscious human volition, while Artificial General Intelligence (AGI) makes decisions based on autonomous algorithms that are outside the realm of their creator's prediction. The study ruled that in the case of "Black Box" dilemma, programmer's act is detached from its criminal outcome (novus actus interveniens). It creates a "penal vacuum" that makes it impossible to establish the mental element (mens rea / criminal intent) under extant legal standards. It concluded from the research that any shift in defining AI as a, “tool,” toward viewing it as a, “virtual perpetrator,” was the only feasible exit point for relevant law to protect institutional crimes from achieving impunity, especially across self-learning systems. **Implication:** The researcher proposes the expansion of corporate liability in a way that it can include “autonomous software entities,” thereby constituting some type of virtual legal personality. That would allow for the drafting of technical sanctions, such as deletion, reprogramming or even financial penalties against their independent patrimony. The researcher also urges the Iraqi judiciary to shift from fault-based liability (for wrongful acts) to one based on technical risk (strict liability). This would mean that under this approach, the programmer (or user) could be found at fault for harmful consequences of the system as a presumed risk stemming from the functioning of highly autonomous technologies. Corporations and institutions deploying AI systems should also be mandated to reserve an independent insurance-based financial patrimony (electronic patrimony or compensation fund) for each smart system. This would allow victims to be compensated without delay in instances where the humans lost control over the system. **Limitation:** The study showed how the draft Iraqi law on cybercrimes is still missing a clear affiliation with what would be "an autonomous criminal liability" of local smart systems, thus allowing it to become outdated in a very short time frame due to rapid advances in technology. **Future Research:** As a last resort, the study proposes that the Supreme Judicial Council create special courts for “smart

cybercrimes," staffed by judges and tech experts who can examine the technological "black box" and figure out whether to assign criminal responsibility to human actors as opposed to autonomous systems.

REFERENCES

[1] W. Al Hanaineh, J. Matas, and J. M. Guerrero, "A Comparative Study of Smart THD-Based Fault Protection Techniques for Distribution Networks," *Sensors*, vol. 23, no. 10, p. 4874, May 2023, doi: 10.3390/s23104874.

[2] M. A. R. Khalid, M. A. A. Shahid, and S. Murali, "Antidiabetic Activity of Methanolic Extracts of Leaves of Tylophora neglecta Leaves in Alloxan Induced Diabetes in Rats," *International Journal of Allied Medical Sciences and Clinical Research*, vol. 11, no. 4, pp. 511–522, Dec. 2023, doi: 10.61096/ijamscr.v11.iss4.2023.511-522.

[3] E. Nerantzi and G. Sartor, "Crimes without criminals: in search of criminal liability for harms caused by AI systems," in *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, 2025, pp. 329–348. doi: 10.4337/9781035316496.00024.

[4] B. Qadir and A. Muhammad, "The Legal Classification of Civil Liability for Private Medical Laboratories for the Act of Others (A Comparative Analytical Study)," *AL-Qadisiya Journal For Law and Political Sciences*, vol. 16, no. Issue: 2 part 1, pp. 829–858, Sep. 2025, doi: 10.63677/jqlap.2025.159418.1315.

[5] S. W. Buell, "Corporate criminal liability," in *Research Handbook on Corporate Liability*, Edward Elgar Publishing, 2023, pp. 100–115. doi: 10.4337/9781800371286.00013.

[6] K. Bancroft, "Domestic Violence Legislation, Virtual Legal Methods and Researching One Female Teacher's Lived Experiences of Recovery from Intimate Partner Violence During the COVID-19 Global Pandemic," *Journal of Legal Research Methodology*, vol. 1, no. 1, pp. 84–109, Aug. 2021, doi: 10.19164/jlrm.v1i1.1164.

[7] J. G. FERNÁNDEZ TERUELO, "Personas jurídicas instrumentales como sujetos inimputables a efectos del régimen legal del art. 31 bis CP: posibilidades de respuesta penal," *Revista Penal*, no. 55, pp. 96–111, Feb. 2025, doi: 10.36151/rp.55.07.

[8] G. Ferrazzi, "Regional planning reform in Indonesia: Keeping pace with decentralisation?," *Third World Plann. Rev.*, vol. 23, no. 3, pp. 249–272, Aug. 2001, doi: 10.3828/twpr.23.3.w041710121r15351.

[9] F. Maia Alexandre, "The Legal Status of Artificially Intelligent Robots: Personhood, Taxation and Control," *SSRN Electronic Journal*, 2017, doi: 10.2139/ssrn.2985466.

[10] D. A. R. Y. Al-Mazouri, "Criminal liability provisions arising from traffic accidents within the framework of the profession of teaching driving," *Journal of Legal and Political Studies*, vol. 12, no. 1, pp. 8–56, Jun. 2024, doi: 10.17656/jlps.10251.

[11] R. Ho, "Baby Reindeer: How police could have prevented Martha's stalking from getting worse," Jun. 2024, doi: 10.64628/aam.ukgn39san.

[12] D. Ormerod and K. Laird, "5. Crimes of strict liability," in *Smith, Hogan, and Ormerod's Criminal Law*, Oxford University Press, 2021, pp. 146–179. doi: 10.1093/he/9780198849704.003.0005.

[13] S. Kaltenbrunner, "Human in control: Shared decision-making with clinical decision-support systems under the Artificial Intelligence Act," *Computer Law & Security Review*, vol. 61, p. 106281, Jul. 2026, doi: 10.1016/j.clsr.2026.106281.

[14] E. N. Rakhmanova, "Aging Offenders from the Standpoint of Criminal Law," *Pravosudie / Justice*, vol. 2, no. 1, pp. 189–206, Mar. 2020, doi: 10.37399/issn2686-9241.2020.1.189-206.

[15] S. Samuel, "Electoral Law Reform in Nigeria: Proposals for Amendment of the Electoral Act 2010 and the Imperative of ICT," *International Journal of Legislative Drafting and Law Reform*, Oct. 2024, doi: 10.61955/myozdn.

[16] T. M. SHIYAB, "Special Criminal Measures in Combating Terrorist Crimes in the Light of Federal Law No. (7) of 2014 Concerning Combating Terrorist Crimes," *AAU Journal of Business and Law*, pp. 1–14, 2022, doi: 10.51958/aaujbl2022v6i1p5.

[17] A. Jabłoński and M. Jabłoński, "Artificial Intelligence as a Research Object in Management and Climate Sciences and as a Practical Tool for Modern Business Solutions," in *Artificial Intelligence for Climate Hazards*, CRC Press, 2026, pp. 9–33. doi: 10.1201/9781003434016-2.

[18] C. M, "Corporate Criminal Liability and Artificial Intelligence: Doctrinal Overview, Problems and Perspectives," *Open Access Journal of Criminology Investigation & Justice*, vol. 2, no. 1, 2024, doi: 10.23880/oajcij-16000122.

[19] D. L. Ross, "Overview of Civil Liability," in *Civil Liability in Criminal Justice*, Routledge, 2023, pp. 1–27. doi: 10.4324/9781003170792-1.

[20] O. RADUTNIY, "Liability of a legal entity in criminal law in the refraction of legal personality of artificial intelligence," *INFORMATION AND LAW*, no. 2(49), pp. 138–150, Jun. 2024, doi: 10.37750/2616-6798.2024.2(49).306193.

[21] B. Parry, "Spectral Personas: Exploring the Constitution and Legal Standing of 'Virtual Personhood,'" in *Personhood in the Age of Biolegality*, Springer International Publishing, 2019, pp. 21–38. doi: 10.1007/978-3-030-27848-9_2.

[22] S. Bankins and P. Formosa, "Ethical AI at Work: The Social Contract for Artificial Intelligence and Its Implications for the Workplace Psychological Contract," in *Redefining the Psychological Contract in the Digital Era*, Springer International Publishing, 2021, pp. 55–72. doi: 10.1007/978-3-030-63864-1_4.

[23] J. De Snaijer, "Trusting Robots: Limiting Due Diligence Obligations in Robot-Assisted Surgery under Swiss Criminal Law," in *Human–Robot Interaction in Law and Its Narratives*, Cambridge University Press, 2024, pp. 49–72. doi: 10.1017/9781009431453.006.

[24] S. Kerroum, "Jurisprudential renewal in social Nawāzil: A study of al-Mahdi al-Wazzani's legal responses," *Intercontinental Journal of Social Sciences*, vol. 2, no. 4, pp. 163–181, Jul. 2025, doi: 10.62583/n3q8vt65.

[25] A. Priya, "CRIMINAL ACCOUNTABILITY FOR AI: MENS REA, ACTUS REUS, AND THE CHALLENGES OF AUTONOMOUS SYSTEMS," *LawFoyer International Journal of Doctrinal Legal Research*, vol. 3, no. 1, pp. 273–303, Apr. 2025, doi: 10.70183/lijdlr.2024.v03.13.

[26] P. Bennett, "Reform from within: the Grendon example: Peter Bennett discusses how people working within the criminal justice system can walk a line between conformity and change," *Criminal Justice Matters*, vol. 77, no. 1, pp. 14–15, Sep. 2009, doi: 10.1080/09627250903139082.

[27] W. Liu, "Three hurdles through which artificial intelligence cannot go," in *Integrated Human-Machine Intelligence*, Elsevier, 2023, pp. 71–93. doi: 10.1016/b978-0-323-99562-7.00004-8.

[28] P. Connor, "Mens Rea (State of Mind) and Actus Reus (Criminal Conduct)," in *Blackstone's Police Investigators' Workbook 2018*, Oxford University Press, 2017. doi: 10.1093/law/9780198806387.003.0001.

[29] Z. Barlas, "When robots tell you what to do: Sense of agency in human- and robot-guided actions," *Conscious. Cogn.*, vol. 75, p. 102819, Oct. 2019, doi: 10.1016/j.concog.2019.102819.

[30] V. Piddubna, "Legal approaches to the concept of the state as a legal entity of public law," *Analytical and Comparative Jurisprudence*, no. 2, pp. 313–318, Apr. 2025, doi: 10.24144/2788-6018.2025.02.43.

[31] D. French, *5. Corporate personality*. Oxford University Press, 2018. doi: 10.1093/he/9780198815105.003.0005.

[32] A. Singh, "From Legal Fiction to Constitutional Actor: Corporate Personhood and Governance in India," 2025, doi: 10.2139/ssrn.5700803.

*** Maher Tariq Abbas (Corresponding Author)**
Independent Research, Iraq
Email: mahertarek7279@gmail.com