ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Criminal Responsibility for Artificial Intelligence-Related Crimes under International Criminal Law: A Comparative Study of the Legal Systems of Iran and Iraq

Aree. Abbas Qadir[1], Anwar. Ahmadi[2*], Tayebeh. Bijani Mirza[2], Ebad. Rouhi[3]

[1] PhD Student, Department of Law, SR.C., Islamic Azad University, Tehran, Iran
[2] Department of Law, Sa.C., Islamic Azad University, Sanandaj, Iran
[3] Assistant Professor, Department of Law, Cihan University of Sulaymaniyah, Kurdistan, Iraq

*** Corresponding author email address**: ahmadiyas@ymail.com

Received: 2025-09-18 **Revised:** 2026-01-07 **Accepted:** 2026-01-15 **Initial Publish:** 2026-09-02 **Final Publish:** 2026-01-30

Artificial intelligence increasingly shapes military operations, security governance, surveillance, data analysis, cyber activities, and automated decision-making, creating new challenges for the attribution of criminal responsibility. This article examines criminal responsibility arising from artificial intelligence-related crimes under international criminal law and comparatively evaluates the legal systems of Iran and Iraq. Using a doctrinal, analytical, and comparative methodology, the study investigates whether existing principles governing individual criminal responsibility, causation, mens rea, complicity, indirect perpetration, aiding and abetting, command responsibility, and corporate liability can adequately address crimes committed through, facilitated by, or resulting from artificial intelligence systems. The analysis shows that artificial intelligence should not presently be treated as an independent bearer of criminal responsibility because current systems lack moral agency, legal consciousness, and meaningful responsiveness to punishment. Instead, responsibility should remain centered on human and organizational actors who design, authorize, deploy, supervise, control, or knowingly benefit from high-risk systems. Existing international criminal-law doctrines can address many intentional and knowing uses of artificial intelligence, particularly where the technology functions as an instrument of genocide, crimes against humanity, war crimes, or other serious offences. However, significant accountability gaps arise when harmful outcomes result from opaque algorithms, autonomous learning, distributed decision-making, negligent development, or fragmented institutional control. The comparative analysis indicates that Iranian and Iraqi law contain general rules concerning intention, negligence, causation, perpetration, complicity, omission, and legal-person liability that may partially govern artificial intelligence-related harm. Nevertheless, neither system provides a comprehensive framework for high-risk artificial intelligence, autonomous military systems, algorithmic evidence, or responsibility throughout the technological life cycle. The article proposes a multi-layered model allocating liability among intentional users, operators, developers, manufacturers, corporate managers, military commanders, and civilian superiors according to their knowledge, control, contribution, risk creation, and failure to prevent harm. It concludes that legislative reform should preserve personal culpability while introducing clear duties of human oversight, testing, auditability, documentation, cybersecurity, and evidence retention.

Keywords: *Artificial Intelligence; Criminal Responsibility; International Criminal Law; AI-Related Crimes; Autonomous Systems; Command Responsibility; Iranian Criminal Law; Iraqi Criminal Law*

How to cite this article:
Abbas Qadir, A., Ahmadi, A., Bijani Mirza, T., & Rouhi, E.(2026). Criminal Responsibility for Artificial Intelligence-Related Crimes under International Criminal Law: A Comparative Study of the Legal Systems of Iran and Iraq. *Interdisciplinary Studies in Society, Law, and Politics, 5*(1), 1-18. https://doi.org/10.61838/kman.isslp.548

1. Introduction

Artificial intelligence has moved from a specialized field of computer science to a pervasive infrastructure influencing economic transactions, security operations, public administration, criminal investigation, military decision-making, communication, surveillance, and the production and distribution of information. Contemporary artificial intelligence systems are capable of processing enormous datasets, identifying patterns that may be invisible to human observers, generating predictions, selecting operational options, and executing decisions with varying degrees of human intervention. These technological capacities have produced substantial social and institutional benefits, yet they have also generated new forms of risk that traditional criminal-law doctrines were not designed to address. The criminal use of artificial intelligence may involve systems intentionally employed as instruments for fraud, cyberattacks, political repression, automated surveillance, disinformation, military targeting, or the identification of individuals and groups. Artificial intelligence may also contribute to harmful conduct because of defective programming, biased training data, insufficient testing, inadequate human supervision, or autonomous adaptation after deployment. The resulting legal difficulty is not merely whether harm has occurred, but how criminal responsibility should be attributed when the causal process involves human developers, corporations, commanders, public authorities, operators, and technologically complex systems whose internal decision-making may not be fully explainable. Sachoulidou argues that the growing use of artificial intelligence in activities capable of producing serious harm exposes structural weaknesses in criminal-law models that continue to assume a relatively direct connection between a human actor, a prohibited act, and a culpable mental state (Sachoulidou, 2024). The emergence of artificial intelligence therefore requires an examination of whether traditional principles of responsibility can be interpreted in a technologically neutral manner or whether new doctrines are necessary to prevent accountability gaps.

The problem becomes particularly significant within international criminal law because the crimes addressed by this field are distinguished by their scale, gravity, collective dimensions, and relationship to state or organizational power. Genocide, crimes against humanity, war crimes, and the crime of aggression are rarely committed through the isolated conduct of a single individual. They commonly involve political authorities, military hierarchies, administrative structures, economic actors, intelligence institutions, and numerous individuals whose contributions differ in form and intensity. International criminal law has consequently developed doctrines of direct perpetration, indirect perpetration, co-perpetration, ordering, inducing, aiding and abetting, superior responsibility, and participation in collective criminal activity. Ambos explains that international criminal responsibility must be understood through modes of participation capable of connecting senior decision-makers and indirect contributors to crimes physically carried out by others (Ambos, 2021). Artificial intelligence adds another layer to these already complex structures by allowing decisions to be delegated, mediated, accelerated, or partially automated. A military commander may authorize an AI-enabled targeting system without personally selecting each target. A governmental authority may deploy predictive systems to identify alleged political opponents, while the discriminatory or repressive outcome results from the combined operation of data selection, algorithmic classification, administrative implementation, and coercive enforcement. A technology company may provide analytical software to an organization known to be involved in widespread attacks against civilians. In each of these situations, the system may become a crucial causal mechanism, but the fundamental question remains whether responsibility belongs to the human and organizational actors who designed, authorized, supplied, controlled, supervised, or failed to restrain its operation.

The central challenge arises from the apparent tension between technological autonomy and the principle of personal culpability. Criminal law traditionally requires proof that the accused engaged in conduct attributable to them and possessed the mental element required for the relevant offence. International criminal law similarly emphasizes individual responsibility and rejects the imposition of punishment solely because an individual holds a political, military, or organizational position. Werle and Jeßberger explain that the attribution of international crimes depends on a legally defined

relationship between the accused, the criminal conduct, and the requisite subjective element (Werle & Jeßberger, 2020). Yet advanced artificial intelligence systems may generate outputs that were not specifically predicted by their developers or operators. Machine-learning systems may modify their operational strategies through experience, produce conclusions that cannot be fully reconstructed, or act on correlations that no human participant consciously selected. Matthias describes this phenomenon as a responsibility gap arising when learning systems exercise a degree of operational independence that prevents their conduct from being straightforwardly attributed either to the programmer or to the user (Matthias, 2004). The responsibility gap does not necessarily mean that no person should be held liable. It indicates that familiar concepts of intention, knowledge, causation, foreseeability, and control may become difficult to apply when decision-making is distributed across a technological network.

A second problem concerns the legal status of artificial intelligence itself. Some scholars have examined whether sufficiently advanced systems could be treated as legal persons or even as criminal subjects. Solum's early analysis of legal personhood for artificial intelligences considered whether the legal system might recognize artificial entities as holders of rights and duties when they acquire capacities traditionally associated with agency (Solum, 1992). Hallevy later developed models under which artificial intelligence could be treated as a direct perpetrator, an innocent agent used by a human offender, or an entity whose conduct creates liability for others (Hallevy, 2010). The attraction of direct AI responsibility is that it appears to address situations in which no human actor fully controls or predicts the harmful outcome. Nevertheless, imposing criminal liability on an artificial system raises profound objections. Criminal punishment is traditionally connected to blameworthiness, moral agency, deterrence, rehabilitation, condemnation, and the capacity to understand legal norms. Abbott and Sarch demonstrate that although punishment of artificial intelligence can be imagined through deactivation, modification, asset deprivation, or restrictions on operation, these measures do not necessarily perform the same normative functions as punishment imposed on human offenders (Abbott & Sarch, 2019). Recognizing artificial intelligence as the primary offender may also create opportunities for human actors and corporations to externalize blame onto systems they developed or deployed. The more defensible approach is therefore to distinguish regulatory treatment of artificial intelligence from criminal responsibility and to maintain the primary focus on human and organizational accountability.

The relevance of this debate is especially evident in relation to autonomous weapon systems and AI-supported military operations. The use of algorithms in intelligence analysis, target recognition, threat assessment, navigation, and weapons control has intensified concerns about compliance with the principles of distinction, proportionality, precaution, and military necessity. Schmitt and Thurnher argue that autonomous weapons are not necessarily unlawful merely because they operate without continuous human control, but their legality depends on whether they can be used consistently with the law of armed conflict (Schmitt & Thurnher, 2013). Asaro emphasizes that the delegation of lethal decision-making to machines risks weakening human responsibility and undermining the moral and legal significance of decisions to use deadly force (Asaro, 2012). Sparrow similarly argues that autonomous weapons create a serious accountability problem because responsibility for an unlawful killing may be difficult to assign among commanders, programmers, manufacturers, and the machine itself (Sparrow, 2007). These concerns extend beyond the battlefield. AI-enabled systems may facilitate widespread persecution, discriminatory detention, forced displacement, suppression of civilian populations, or systematic attacks conducted through digital surveillance and predictive identification. The potential role of AI in international crimes therefore requires an analytical framework broad enough to encompass both military and civilian applications.

The comparative focus on Iran and Iraq is justified by the geographical, legal, political, and security context in which both states operate. Their legal systems contain established principles governing criminal intent, negligence, causation, participation, complicity, liability for organizational conduct, and offences against national or public security. Both systems have also confronted the increasing significance of cyber activity, digital evidence, automated surveillance, and technologically mediated threats. At the same time, neither legal system has developed a comprehensive criminal-liability

framework specifically addressing advanced artificial intelligence. The comparative analysis is important not because Iran and Iraq have identical legal traditions, but because they confront related regulatory questions within legal orders influenced by codified criminal law, Islamic legal principles, state-security concerns, and the need to harmonize domestic criminal justice with international obligations. The study therefore evaluates whether existing doctrines can accommodate AI-related crimes and identifies points at which legislative clarification is required.

The objective of this article is to determine how criminal responsibility should be attributed when artificial intelligence is used to commit, facilitate, organize, or contribute to conduct falling within international criminal law. It examines whether AI should be regarded as an instrument, an intervening causal mechanism, an independent legal subject, or a source of heightened duties for human actors. It also evaluates the liability of developers, programmers, manufacturers, corporate managers, military commanders, governmental officials, operators, and end users. The comparative component seeks to identify the strengths and deficiencies of Iranian and Iraqi criminal law in relation to AI-mediated conduct, particularly concerning the material element of offences, the mental element, causation, complicity, command responsibility, legal-person liability, and electronic evidence. The article adopts a doctrinal and comparative method. It analyzes the conceptual foundations of international criminal responsibility, applies them to technologically mediated conduct, and compares the general structures of responsibility in the two domestic systems.

The central hypothesis is that existing principles of international criminal law can address many intentional and knowing uses of artificial intelligence because the involvement of technology does not eliminate the responsibility of persons who design, authorize, deploy, or control criminal operations. Cryer, Robinson, and Vasiliev emphasize that international criminal law attributes responsibility according to the accused's contribution and mental state rather than according to whether the accused personally performed every physical element of the crime (Cryer et al., 2019). However, existing doctrines are less effective where harmful conduct emerges from distributed decision-making, opaque learning processes, negligent development, inadequate supervision, or uncertain chains of causation. Chengeta identifies a comparable accountability gap in relation to autonomous weapons, particularly when responsibility is divided among commanders, operators, manufacturers, and programmers (Chengeta, 2016). The article therefore proposes a multi-layered model of responsibility based on knowledge, control, risk creation, supervision, and contribution. Under this model, the law should neither treat AI autonomy as an automatic defence nor impose liability solely because a person was remotely connected to the system. Responsibility should correspond to the actor's role in creating, maintaining, directing, or failing to prevent a legally significant risk.

2. Conceptual Foundations and the International Legal Framework of AI-Related Crimes

A legally useful definition of artificial intelligence must focus less on the technical architecture of a particular system and more on the characteristics that influence the attribution of responsibility. Artificial intelligence may broadly be understood as a computational system capable of performing functions commonly associated with human cognition, including learning, classification, prediction, planning, language generation, perception, and decision support. The category includes systems with very different levels of sophistication. Some operate according to fixed rules established in advance, while others learn from data and modify their outputs according to patterns identified during training or operation. The legal significance of these systems lies in their capacity to influence or determine conduct in a manner that may not be reducible to a single human instruction. Hallevy explains that the conventional view of machines as passive instruments becomes less satisfactory when a system can select among alternatives and respond dynamically to changing circumstances (Hallevy, 2013). Nevertheless, autonomy should not be treated as an absolute condition. Most existing systems remain dependent on human choices concerning their objectives, design, training data, deployment environment, access permissions, operational limits, and termination mechanisms. The degree of autonomy is therefore better understood as a spectrum that affects the intensity of human control rather than as a complete separation between machine and human agency.

The concept of AI-related crime should also be distinguished from the narrower category of cybercrime. Cybercrime generally concerns offences directed against computer systems, data, networks, or digital infrastructure, as well as conventional crimes committed through digital means. Artificial intelligence-related crime may include cybercrime, but it extends further because AI can influence decision-making in physical, administrative, military, and social environments. An AI system may be used to identify vulnerable victims, automate fraudulent communication, generate deceptive evidence, select targets for violence, coordinate surveillance, optimize unlawful military operations, or conceal the origin of criminal conduct. AI can also become the object of crime through data poisoning, model manipulation, unauthorized access, or the corruption of safety mechanisms. More importantly for criminal responsibility, AI may generate harm through a combination of human design choices and autonomous processing. Sachoulidou observes that criminal law must distinguish between artificial intelligence used as a deliberate tool and artificial intelligence that produces harmful consequences through unexpected or insufficiently supervised operation (Sachoulidou, 2024). This distinction affects whether liability is based on intention, knowledge, recklessness, negligence, or a failure to fulfil a legal duty.

When AI is used as an instrument of crime, attribution is comparatively straightforward. A person who intentionally employs an AI system to conduct a cyberattack, fabricate evidence, identify members of a protected group, or coordinate unlawful violence cannot avoid responsibility merely because the immediate operation was performed by software. The system functions as a technologically sophisticated means through which the offender's purpose is implemented. Hallevy's perpetration-by-another model treats an intelligent system as an innocent agent when it lacks legal capacity but is intentionally used by a human actor to commit an offence (Hallevy, 2010). This model resembles indirect perpetration because the human controls the relevant criminal objective while the system performs the operational act. The difficulty increases when the user provides only a broad objective and the system independently determines the means. If the user directs an autonomous system to eliminate a population, suppress a civilian protest, or select targets without regard to protected status, criminal responsibility remains strongly connected to the user's instruction. If the system is instructed to perform a lawful objective but selects an unlawful method because of defects or learning behavior, responsibility will depend on whether the harmful outcome was intended, known, foreseeable, or negligently disregarded.

AI may facilitate international crimes in ways that do not involve physical execution. International crimes often depend on information, coordination, classification, communication, and institutional organization. AI systems may process large databases to identify ethnic, religious, political, or social groups. They may analyze communication networks to locate opponents, predict movement, or assist authorities in planning detention operations. They may generate propaganda, automate incitement, conceal unlawful transactions, or optimize the allocation of resources used in attacks. Crootof emphasizes that autonomous and algorithmic systems may alter the scale and speed of armed operations, making it possible to conduct actions that exceed the practical capacities of human decision-makers (Crootof, 2015). The same logic applies to crimes against humanity. A widespread or systematic attack against a civilian population may be supported by automated systems that classify individuals, coordinate surveillance, or recommend coercive measures. The AI system need not itself satisfy the contextual elements of the international crime. Those elements relate to the broader attack, policy, armed conflict, or genocidal intent. The legal question is whether the persons who designed, deployed, or used the system made a sufficiently significant contribution with the required mental element.

The principle of legality is central to determining whether existing criminal-law rules can be applied to AI-mediated conduct. International criminal law prohibits retroactive punishment and requires criminal offences and modes of liability to be sufficiently accessible and foreseeable. Schabas explains that the Rome Statute's legality provisions require strict construction and prohibit extending criminal definitions by analogy to the detriment of the accused (Schabas, 2016). This principle does not mean that criminal law must identify every possible technological method by which an offence can be committed. A prohibition against intentionally attacking civilians may apply whether the attack is

conducted with conventional artillery, remotely operated systems, or AI-enabled weapons. Similarly, persecution, murder, deportation, torture, or genocide do not cease to be crimes because algorithmic tools are used in their execution. Technology-neutral interpretation is consistent with legality when the prohibited conduct and mental element remain within the established meaning of the offence. The legality problem becomes more serious when courts attempt to create new forms of liability, presume mental states from system design, or punish actors who could not reasonably foresee that their technological contribution would be connected to an international crime.

The individual character of international criminal responsibility is another foundational principle. International criminal law was developed to prevent state structures, military hierarchies, or organizational complexity from shielding individuals who plan, order, facilitate, or fail to prevent atrocities. Werle and Jeßberger note that the system concentrates on the personal contribution and culpability of the accused, even when the crime arises from collective conduct (Werle & Jeßberger, 2020). Artificial intelligence does not alter this normative foundation. It may complicate the identification of the relevant contribution, but it should not replace the inquiry into human responsibility. A developer who creates a general-purpose system without knowledge of its later criminal use occupies a different legal position from a developer who intentionally modifies a system to identify civilian targets. A corporate manager who receives credible evidence that a product is being used to facilitate persecution and continues specialized support may be differently situated from an employee who lacks access to operational information. A military commander who deploys an unreliable autonomous weapon in a densely populated area may bear responsibility on a different basis from an operator who reasonably relies on lawful instructions and has no capacity to detect the system's defect. The principle of personal culpability therefore requires differentiated assessment rather than collective blame.

The possible legal personality of artificial intelligence must be approached with caution. Legal systems recognize entities such as corporations as legal persons even though they do not possess biological consciousness. This analogy has encouraged arguments that AI could also be granted a form of personality. Solum's analysis shows that legal personhood is not necessarily limited to human beings and may be constructed when doing so serves institutional purposes (Solum, 1992). Yet corporate personality does not mean that a corporation possesses human consciousness. It functions as a mechanism for assigning rights, duties, assets, and liability to an organized entity. Artificial intelligence systems generally lack comparable organizational independence, property, legally structured decision-making bodies, and durable institutional identity. More importantly, criminal personhood cannot be justified solely by functional convenience. Criminal responsibility ordinarily expresses condemnation of a subject capable of understanding norms and being guided by them. An AI system may be modified in response to sanctions, but modification is not equivalent to moral learning or recognition of wrongdoing.

Hallevy proposes models in which an artificial intelligence entity could satisfy both the external and internal elements of an offence if it possesses sufficient processing capacity to represent knowledge and intention (Hallevy, 2013). This approach relies on a functional understanding of mental states. If a system can represent circumstances, predict outcomes, select actions, and pursue goals, its computational state might be treated as legally equivalent to knowledge or intention. The difficulty is that legal intention is not merely the production of goal-directed behavior. It is a normative concept used to evaluate the relationship between an agent, an act, and a prohibited consequence. Abbott and Sarch argue that although artificial intelligence may be treated as a legal fiction for certain purposes, punishment becomes problematic when the entity lacks experiences, interests, or assets that can be meaningfully affected (Abbott & Sarch, 2019). Deactivation, deletion, or reprogramming may protect society, but these are preventive or regulatory measures rather than punishment in the traditional sense. Treating them as criminal penalties may obscure the responsibility of the humans who made the system dangerous.

The preferable approach is a hybrid model in which artificial intelligence is recognized as a legally relevant causal and operational entity without being treated as the primary bearer of criminal blame. Under this

approach, AI systems may be subjected to registration, audit, restriction, confiscation, suspension, deactivation, or mandatory redesign. These measures can respond to danger even when no human actor satisfies the requirements of criminal liability. Human and corporate actors remain subject to criminal responsibility when their conduct and mental state justify punishment. Matthias's responsibility-gap analysis demonstrates why regulatory mechanisms are necessary: some harmful outcomes may result from learning systems even when no individual specifically intended or predicted the precise result (Matthias, 2004). The existence of such cases does not justify fictionalizing machine culpability. It supports the creation of preventive duties, technical standards, documentation requirements, and civil or administrative liability alongside criminal law.

International criminal law provides several modes of responsibility that can be adapted to AI-mediated crimes. Direct perpetration applies when an individual personally uses or controls a system to execute prohibited conduct. Indirect perpetration may apply when a person uses the system as an instrument or acts through an organizational structure that depends on algorithmic operations. Co-perpetration may apply when several actors share control over essential components of the criminal plan, such as data collection, system development, operational deployment, and coercive enforcement. Ordering and inducing may apply when officials direct subordinates to use AI systems for unlawful purposes. Aiding and abetting may apply to technical providers who knowingly facilitate international crimes. Superior responsibility may apply when commanders or civilian superiors fail to prevent or repress crimes committed by subordinates using AI systems. Ambos explains that modes of liability should not be treated as interchangeable because each reflects a different relationship between the accused and the offence (Ambos, 2021). This requirement is especially important in technological cases, where the temptation to impose broad liability on everyone connected to a system must be resisted.

Autonomous weapon systems illustrate the relationship between AI, international humanitarian law, and international criminal responsibility. Schmitt and Thurnher maintain that autonomy does not itself determine legality; the decisive issue is whether the weapon can be used in compliance with applicable rules (Schmitt & Thurnher, 2013). A system capable of reliably distinguishing military objectives from civilians in a limited environment may raise different concerns from a system operating in a complex urban setting. Asaro argues that removing meaningful human control from lethal decisions undermines accountability and risks reducing individuals to data points processed by machines (Asaro, 2012). Chengeta further contends that traditional responsibility doctrines may fail when the conduct of an autonomous weapon cannot be attributed to a particular human decision at the moment of attack (Chengeta, 2016). These concerns suggest that legal review must occur before deployment and continue throughout the operational life of the system. Commanders and political authorities should not be permitted to rely on initial approval when later evidence reveals systematic errors, discriminatory performance, or unpredictable behavior.

The international legal framework therefore supports a human-centered model of responsibility combined with technology-specific duties. Existing offences can generally apply to AI-mediated conduct without violating legality, provided that courts do not expand the substantive definitions beyond their established meaning. Existing modes of liability can connect planners, commanders, developers, suppliers, and operators to crimes when their contribution and mental state are proven. At the same time, the distinctive characteristics of AI justify heightened obligations concerning testing, transparency, human oversight, record retention, risk assessment, and intervention. These duties are not substitutes for criminal responsibility. They provide the standards against which negligence, recklessness, knowledge, and failure to prevent may be evaluated. The central task is therefore not to invent an artificial offender but to reconstruct the chain of human and organizational decisions surrounding the system.

3. Attribution of Criminal Responsibility for AI-Related International Crimes

The attribution of criminal responsibility begins with the identification of conduct. In conventional criminal cases, conduct is usually associated with a physical act or omission performed directly by the accused. In AI-mediated crimes, the immediate physical or digital operation may be performed by a system that selects

targets, generates commands, manipulates information, or activates a weapon. The relevant human conduct may have occurred earlier and may consist of programming, training, authorizing, deploying, configuring, supplying, supervising, or failing to deactivate the system. Criminal responsibility should therefore not be limited to the last observable act in the causal sequence. Cryer, Robinson, and Vasiliev explain that international criminal responsibility can attach to contributions made at different levels of a criminal operation, provided that the legal requirements of the relevant mode of liability are satisfied (Cryer et al., 2019). The conduct of a programmer who knowingly creates a discriminatory classification function, a commander who authorizes its use, and an operator who applies its outputs may each be legally significant, but their responsibility must be evaluated separately.

When AI is deliberately used to commit an international crime, the system should generally be treated as an instrument. A political official who orders the use of an AI platform to identify members of an ethnic group for detention acts through the system and the personnel implementing its outputs. A commander who directs an autonomous weapon to attack civilians cannot rely on the machine's execution of the order to avoid responsibility. Hallevy's innocent-agent model is useful in these cases because the artificial system lacks independent criminal capacity and operates as the means through which the human objective is realized (Hallevy, 2010). The fact that the system selects the precise victim or timing does not necessarily break attribution if the human actor established the unlawful objective and knowingly accepted the operational method. The law already attributes consequences to offenders who use animals, mechanical devices, intermediaries, or organizational structures. Artificial intelligence increases technological complexity but does not fundamentally alter the principle that a person may commit an offence through an external instrument.

The problem becomes more difficult where the system is given a lawful or ambiguous objective but produces an unlawful outcome through autonomous processing. In such cases, responsibility depends on the relationship between the actor's conduct and the risk that materialized. Matthias argues that learning automata may create situations in which neither the programmer nor the operator can fully predict the system's future behavior (Matthias, 2004). However, unpredictability should not be accepted as a general defence. The legal inquiry must distinguish between outcomes that were genuinely unforeseeable and outcomes that became possible because the responsible actors failed to test, monitor, constrain, or understand the system. A manufacturer who deploys a high-risk military AI without adequate validation may not intend civilian deaths, but the decision may constitute culpable risk creation. An operator who continues using a system after repeated false identifications may possess knowledge or recklessness concerning future harm. A commander who ignores expert warnings may be responsible for failing to take necessary measures. The relevant issue is not whether the precise sequence was predicted, but whether the type of prohibited harm was foreseeable and whether the accused possessed the mental state required by the applicable offence or mode of responsibility.

Causation in AI-related crimes may involve multiple actors and intervening processes. The system's output may be influenced by training data, model architecture, updates, user prompts, environmental conditions, sensor errors, adversarial manipulation, and operational settings. No single factor may be sufficient to explain the result. Criminal law therefore requires a distinction between factual contribution and normative attribution. A person's conduct may be factually connected to the crime but too remote or insignificant to justify responsibility. Ambos emphasizes that participation in international crimes requires a contribution of a legally relevant nature, not merely a historical connection to the events (Ambos, 2021). A general-purpose software engineer whose code is incorporated into a weapon years later may not be responsible for its unlawful use. By contrast, a contractor who customizes a targeting system for an organization known to attack civilians may make a substantial contribution. The degree of causal proximity, the importance of the contribution, the actor's knowledge, and the availability of alternatives should all be considered.

AI autonomy should not automatically be treated as a novus actus interveniens that breaks the chain of causation. An intervening event breaks attribution only when it is sufficiently independent and abnormal in relation to the defendant's conduct. If an autonomous system behaves within the range of risks associated with

its design and deployment, its operation remains part of the causal mechanism created by human actors. Crootof notes that autonomous weapons can produce legal consequences even when their individual actions are not directly selected by humans, because the decision to deploy the system establishes the conditions under which those actions occur (Crootof, 2015). The causal chain may be broken where a third party hacks the system in an unforeseeable manner, fundamentally changes its operation, and uses it for an unrelated criminal purpose. Even then, responsibility may remain if cybersecurity failures were known and deliberately ignored. Causation must therefore be evaluated in light of the system's intended function, known vulnerabilities, deployment environment, and the actor's capacity to intervene.

The mental element is particularly challenging because international crimes commonly require intention and knowledge, while domestic offences may also recognize recklessness or negligence. The use of AI may obscure what the accused actually knew about the system's internal operation. Yet lack of technical understanding should not automatically exclude knowledge of risk. A political official may not understand the algorithm but may know that it is being used to identify a civilian population for persecution. A commander may not know the source code but may know that the system repeatedly fails to distinguish civilians from combatants. A corporate executive may not understand model architecture but may receive reports that the company's software is assisting unlawful detention. Werle and Jeßberger explain that knowledge may be established through circumstantial evidence and need not depend on direct admission (Werle & Jeßberger, 2020). Internal reports, warnings, performance data, user complaints, testing records, and prior incidents may demonstrate that an accused was aware of the relevant circumstances. Wilful blindness is especially relevant where actors deliberately avoid obtaining information about high-risk systems. A commander cannot insulate themselves by refusing to review evidence of malfunction. A corporate manager cannot avoid knowledge by creating organizational barriers that prevent reports from reaching senior decision-makers. An operator cannot rely on automated outputs without question when the surrounding circumstances strongly indicate unlawful results. Sachoulidou argues that criminal law must respond to situations in which human actors place excessive reliance on algorithmic systems and then invoke the system's opacity to deny responsibility (Sachoulidou, 2024). The appropriate response is not to presume knowledge automatically but to examine whether the accused consciously avoided information that was readily available and legally significant. Deliberate ignorance may support an inference of knowledge where the accused suspected the relevant circumstances and intentionally avoided confirmation.

Direct intent exists where an actor uses AI for the purpose of committing an international crime. Indirect intent may arise where the prohibited consequence is accepted as a virtually certain result of the operation. Knowledge may exist where the actor is aware that the system's contribution will facilitate a broader criminal campaign. Recklessness and negligence are more controversial within international criminal law because the required mental element varies according to the offence and mode of liability. Schabas notes that the Rome Statute generally adopts a demanding standard of intent and knowledge unless otherwise provided (Schabas, 2016). Consequently, negligent development of AI may not by itself establish responsibility for genocide or crimes against humanity. It may, however, support domestic criminal liability, professional liability, or regulatory sanctions. Negligence may also become relevant to superior responsibility, weapons review obligations, or offences that expressly permit a lower mental threshold. The law should therefore avoid collapsing all forms of technological failure into international criminality.

Direct perpetration is most applicable where a person operates or controls an AI system and uses it to execute the material elements of the offence. The operator's physical distance from the result is irrelevant. A person who launches an AI-enabled attack remains a direct perpetrator even if the system autonomously navigates and selects the moment of impact. Indirect perpetration may apply where the accused controls the crime through an organized apparatus that uses AI as part of its administrative or military structure. Ambos explains that indirect perpetration can extend to situations in which a senior actor controls the commission of crimes through organized power structures rather than through personal execution (Ambos, 2021). An authoritarian official who creates an automated system for identifying

and removing political opponents may control the crime through institutions that treat algorithmic outputs as mandatory. The AI system does not replace the organization; it becomes part of the mechanism through which the senior actor exercises control.

Co-perpetration may be relevant when several participants jointly control essential elements of an AI-enabled criminal plan. One group may collect personal data, another may design the classification model, another may authorize detention, and another may implement coercive measures. No participant may individually control the entire operation, but each may possess an essential role. International criminal law requires more than parallel conduct. Cryer, Robinson, and Vasiliev emphasize that co-perpetration depends on a common plan and a level of contribution that gives the accused control over the crime or an essential part of its execution (Cryer et al., 2019). The use of AI may make organizational roles less visible because technical personnel appear removed from the physical harm. Their responsibility depends on whether they shared the criminal plan and whether their contribution was essential. Technical expertise alone does not establish co-perpetration, but intentional design of the system's criminal function may do so.

Ordering, soliciting, inducing, and instigating are particularly relevant where senior officials direct others to use AI systems. An order need not describe every technical step. A commander who instructs subordinates to deploy an autonomous system against a civilian area may be responsible even if the system independently selects specific targets. A government official who orders security agencies to use predictive analytics to identify and eliminate members of a political group may similarly be liable. The causal and mental connection lies in the direction of the criminal operation. The use of AI as an intermediary does not remove the authority relationship between the superior and the subordinates. Werle and Jeßberger observe that ordering liability reflects the influence of a person in authority over the commission of crimes by others (Werle & Jeßberger, 2020). Evidence may include official directives, operational protocols, procurement decisions, deployment orders, and communications concerning the system's intended use.

Aiding and abetting presents more difficult questions for developers, manufacturers, data providers, cloud-service companies, and technical contractors. These actors may contribute essential infrastructure without participating in the final decision to commit the crime. International criminal law generally requires practical assistance, encouragement, or moral support that has a substantial effect on the crime, together with the required knowledge. Chengeta argues that suppliers and programmers of autonomous weapons may bear responsibility when they knowingly contribute to unlawful operations, although the precise mental threshold remains contested (Chengeta, 2016). A company that sells general-purpose software in an ordinary commercial transaction should not become criminally responsible merely because the purchaser later misuses it. The position changes when the company knows that the system is being adapted to facilitate atrocities, provides specialized support, and continues assistance despite clear evidence of criminal use.

The substantial-effect requirement should be evaluated in context. A technical contribution may appear small in isolation but become indispensable to a large-scale criminal operation. Continuous software updates, access to proprietary servers, maintenance of targeting databases, or provision of specialized training may enable crimes that could not otherwise be committed at the same scale or speed. Crootof's analysis of autonomous weapons illustrates how technological systems may transform the operational capacity of military organizations (Crootof, 2015). The same principle applies to surveillance and population-control systems. Nevertheless, criminal responsibility requires proof of the actor's personal knowledge. Corporate involvement should not lead to automatic liability for every employee. Responsibility should concentrate on individuals who knew the relevant circumstances and possessed decision-making authority over the contribution.

Command and superior responsibility are central to AI-mediated international crimes. These doctrines address the failure of military commanders or civilian superiors to prevent or punish crimes committed by subordinates. The introduction of AI does not eliminate the subordinate relationship when human personnel deploy, monitor, maintain, or act upon the system. A commander may be responsible where subordinates use AI-enabled weapons unlawfully and the commander knew or should have known of the crimes. The more difficult case arises when the harmful act is executed autonomously and no

subordinate makes the final targeting decision. Schmitt and Thurnher maintain that commanders remain responsible for decisions to deploy autonomous systems and must assess whether their use can comply with the law of armed conflict (Schmitt & Thurnher, 2013). Command responsibility should therefore focus on the commander's control over deployment, operational parameters, supervision, suspension, and investigation.

The knowledge requirement may be satisfied by evidence that the commander received reports of systematic errors, discriminatory outputs, or repeated unlawful attacks. Asaro argues that meaningful human control is necessary to preserve accountability in lethal decision-making (Asaro, 2012). Meaningful control should not be understood as a requirement that a human press a button before every action. It requires sufficient understanding, authority, information, and opportunity to supervise the system and intervene when necessary. A commander who deploys a system without knowing its limitations may be negligent if the lack of knowledge results from inadequate preparation. A commander who continues deployment after clear warnings may possess the degree of awareness necessary for criminal responsibility. The duty to take necessary and reasonable measures may include suspending the system, modifying operational parameters, conducting an investigation, preserving technical records, notifying higher authorities, and disciplining responsible personnel.

Civilian superiors may also be responsible for AI-enabled crimes committed by security agencies, intelligence organizations, or administrative bodies. A minister who authorizes an algorithmic surveillance program that becomes part of a systematic campaign of persecution may have authority to prevent or repress unlawful conduct. The degree of effective control must be established factually. Formal position alone is insufficient. Schabas emphasizes that superior responsibility depends on a genuine ability to exercise control and take preventive or punitive measures (Schabas, 2016). In AI cases, control may include authority over procurement, system access, data use, operational policies, and institutional compliance. Evidence of control may be dispersed across administrative structures, making documentation and organizational analysis essential.

Corporate and organizational responsibility must be considered separately from individual responsibility. International criminal law primarily prosecutes natural persons, but corporations may be subject to domestic criminal, civil, or administrative liability. Abbott and Sarch note that artificial intelligence may complicate corporate accountability because responsibility can be distributed across teams, automated processes, and hierarchical decision-making (Abbott & Sarch, 2019). A corporation may create incentives to release unsafe systems, conceal defects, or continue supplying products despite evidence of criminal use. Domestic law can respond through legal-person liability, compliance offences, confiscation, fines, exclusion from public contracts, and dissolution. Individual managers may also be liable where they personally authorize, facilitate, or knowingly tolerate criminal contributions. Organizational liability is especially important when no single employee possesses all relevant information but the corporation collectively benefits from fragmented knowledge.

Defences and grounds excluding responsibility require careful assessment. A mistake of fact may arise where an operator reasonably believes that the AI system has identified a lawful military target. The reasonableness of that belief depends on the reliability of the system, available warnings, operational context, and the operator's duty to verify. A mistake of law concerning the legality of autonomous weapons will rarely excuse conduct where the underlying prohibition, such as intentionally attacking civilians, is clear. Superior orders do not automatically exclude responsibility and are particularly weak where the order is manifestly unlawful. System malfunction may exclude liability if it was genuinely unforeseeable and the actor complied with all relevant duties. Third-party hacking may similarly break attribution where the intervention was independent and not reasonably preventable. The mere assertion that "the algorithm decided" should never constitute a defence. It is a factual claim requiring investigation of design, control, warning systems, and human decision-making.

Evidentiary challenges may determine whether responsibility can be proven. AI systems produce complex technical records, including training datasets, source code, model versions, user prompts, system logs, confidence scores, sensor data, and update histories.

These materials may be proprietary, classified, distributed across jurisdictions, or intentionally deleted. The black-box character of some systems may prevent complete reconstruction of the reasoning behind an output. Matthias's responsibility-gap thesis demonstrates that lack of explainability can obstruct attribution even when harm is clear (Matthias, 2004). Legal systems should therefore require high-risk systems to maintain tamper-resistant audit trails, document model changes, preserve operational logs, and record human interventions. Courts will need independent experts capable of explaining both the technical and legal significance of the evidence. Rules governing disclosure, confidentiality, national security, and commercial secrets must be balanced against the accused's right to challenge the prosecution's case.

The attribution of AI-related international crimes should ultimately follow a layered analysis. The first inquiry concerns the underlying offence and its contextual elements. The second identifies the human and organizational acts that contributed to the crime. The third determines the applicable mode of liability. The fourth examines the accused's mental state. The fifth evaluates causation, control, foreseeability, and the availability of preventive measures. This method avoids two opposing errors: treating AI as a legal vacuum that eliminates responsibility, and imposing liability on every person connected to the technology. International criminal law remains capable of addressing intentional uses, knowing assistance, and culpable failures of command. Its principal weakness lies in cases of distributed negligence and opaque autonomous behavior, where regulatory duties and domestic criminal law must supplement international doctrine.

4. Comparative Analysis of the Legal Systems of Iran and Iraq

The comparative analysis of Iran and Iraq must begin with the recognition that both legal systems are based primarily on the criminal responsibility of human beings. Neither system currently treats artificial intelligence as an independent criminal subject possessing moral agency, intention, or capacity for punishment. This position is consistent with the dominant approach in international criminal law, which attributes crimes to natural persons according to their conduct and mental state. Werle and Jeßberger emphasize that personal culpability remains the foundation of international criminal responsibility even where crimes are committed through collective or institutional structures (Werle & Jeßberger, 2020). In both Iran and Iraq, AI-related harm would therefore initially be addressed through general doctrines concerning perpetration, complicity, causation, intention, knowledge, negligence, and liability for omissions. The principal comparative question is not whether the two systems contain any rules capable of application, but whether those rules are sufficiently clear and flexible to address autonomous, opaque, and distributed technological conduct.

The Iranian criminal-law framework provides general concepts capable of addressing intentional uses of artificial intelligence. Where a person deliberately uses an AI system to commit fraud, manipulate data, identify victims, facilitate violence, or execute a prohibited attack, the system can be treated as an instrument of the human offender. The human actor's responsibility derives from the decision to use the system and from the relationship between that decision and the prohibited result. Hallevy's analysis of AI as an innocent agent provides a conceptual model that can be adapted to this context (Hallevy, 2010). An Iranian court would not need to recognize the system as a legal person in order to attribute the conduct to the user. The same reasoning can apply where the AI system selects the precise means or victim within parameters intentionally established by the offender. The decisive factors would be whether the accused controlled the criminal objective, whether the system's conduct fell within the authorized operation, and whether the required mental element existed.

Iranian criminal law also contains general principles governing causation and the attribution of harmful results to persons whose acts or omissions contribute to the outcome. These principles can address relatively direct AI cases, such as the use of automated systems to carry out a predetermined criminal act. More complex cases arise where several individuals contribute to the system's design and deployment. A programmer may create the model, a company may supply the infrastructure, a public authority may authorize use, and an operator may implement the output. The law must distinguish principal participation from assistance and remote contribution. Ambos explains that international criminal law requires the characterization of each participant's role rather than the undifferentiated

attribution of the entire crime to all contributors (Ambos, 2021). The same analytical discipline is necessary in Iranian law. A person should not be held criminally responsible solely because their work formed part of the technological chain. Liability requires a legally significant contribution and the mental element associated with that contribution.

The treatment of intention and negligence is particularly important. Intentional deployment of AI for unlawful purposes can be addressed through existing rules with limited conceptual difficulty. The greater challenge concerns systems that cause harm because of inadequate testing, defective design, biased data, or insufficient supervision. Sachoulidou argues that criminal-law systems must clarify when negligent development or deployment of AI crosses the threshold from regulatory failure to criminal culpability (Sachoulidou, 2024). Iranian law can potentially address negligent conduct where the accused violated a duty of care and caused a prohibited result. However, the absence of specialized statutory duties for AI developers, manufacturers, and operators makes it difficult to determine the standard of care. Without clear obligations concerning testing, auditability, human oversight, cybersecurity, and incident reporting, courts may struggle to decide whether the accused's conduct constituted criminal negligence or merely technical error.

Legal-person liability is another important component of the Iranian framework. AI systems are often developed and deployed by corporations, governmental organizations, and other legal entities rather than by isolated individuals. Corporate structures may fragment information and decision-making so that no single person appears to possess complete knowledge. Abbott and Sarch show that AI complicates conventional theories of punishment because decision-making may be distributed between humans and artificial systems (Abbott & Sarch, 2019). Iranian law's recognition of legal-person liability in defined circumstances provides a possible foundation for addressing organizational wrongdoing. A corporation that knowingly develops an AI system for unlawful surveillance, conceals dangerous defects, or continues providing support for criminal operations may be subject to sanctions. Nevertheless, effective liability requires clear rules connecting the conduct of managers, representatives, and employees to the legal person. It also requires sanctions capable of changing organizational behavior, including fines, confiscation, suspension of activities, exclusion from contracts, and mandatory compliance measures.

The Iranian system faces a significant challenge in relation to international crimes. Domestic criminal law may address acts such as murder, assault, unlawful detention, destruction of property, or offences against national security, but international criminal law requires additional contextual elements. Crimes against humanity require a widespread or systematic attack against a civilian population. Genocide requires specific intent to destroy a protected group. War crimes depend on the existence and classification of an armed conflict and the protected status of persons or objects. Cryer, Robinson, and Vasiliev emphasize that international crimes cannot be reduced to ordinary domestic offences because their contextual elements and modes of liability are distinct (Cryer et al., 2019). AI may contribute to these crimes through targeting, surveillance, propaganda, or administrative organization. Iranian law would benefit from explicit incorporation of international-crime definitions and modes of responsibility so that AI-enabled conduct can be prosecuted according to its full legal character rather than only as separate domestic offences.

The treatment of military AI also requires clarification. Autonomous and semi-autonomous systems may be used for intelligence, surveillance, target selection, navigation, defensive operations, and weapons control. Schmitt and Thurnher argue that legal responsibility depends not on autonomy alone but on whether the system is used in a manner consistent with the law of armed conflict (Schmitt & Thurnher, 2013). Iranian military and criminal law can apply general rules concerning unlawful attacks, disobedience, negligence, and command responsibility, but specialized provisions would improve foreseeability. Commanders should be required to understand the capabilities and limitations of systems under their authority. They should have duties to verify legal review, establish operational restrictions, monitor performance, suspend defective systems, and preserve records. Asaro's emphasis on meaningful human control is particularly relevant because human supervision must be substantive rather than symbolic (Asaro, 2012).

The Iraqi criminal-law framework similarly relies on human conduct, culpability, and causal attribution.

Intentional use of AI to commit an offence can generally be addressed by treating the system as a means. A person who uses an algorithm to identify victims, automate attacks, manipulate evidence, or organize unlawful detention remains the responsible actor. Hallevy's instrumental model is therefore equally applicable to Iraq (Hallevy, 2013). The system's sophistication does not transform it into an independent offender. Responsibility depends on the accused's use of the system, the scope of control, and the required mental state. Iraqi law can also apply general rules of complicity to persons who assist the principal offender by providing technical support, infrastructure, or data. The challenge lies in determining when technical assistance becomes sufficiently connected to the crime and whether the provider possessed the necessary knowledge.

Iraq's experience with armed conflict, terrorism, organized violence, and internationalized criminal proceedings makes the regulation of AI-enabled security operations particularly important. AI systems may be used in counterterrorism, intelligence analysis, border control, biometric identification, and military targeting. These applications may produce legitimate security benefits but also risks of wrongful identification, discriminatory profiling, arbitrary detention, and unlawful use of force. Crootof observes that autonomous systems may accelerate military action and reduce the time available for human legal judgment (Crootof, 2015). In the Iraqi context, where security decisions may involve multiple institutions and international partners, responsibility can become divided among domestic authorities, foreign contractors, technology providers, and military personnel. Clear rules are needed to determine which actor controlled the system, who received warnings, who had authority to intervene, and who benefited from the operation.

Iraqi law also faces difficulties concerning negligence and foreseeability. A system may misidentify civilians as combatants, classify lawful political activity as a security threat, or produce biased outputs because of incomplete data. Matthias's responsibility-gap analysis is relevant because harmful results may emerge without a single actor intending the precise outcome (Matthias, 2004). Iraqi criminal law can potentially address negligent conduct, but specialized standards are necessary to define the duties of those who develop and deploy high-risk AI. The absence of technical standards may allow defendants to argue that the result was unforeseeable or that no recognized duty was breached. Legislation should therefore establish obligations concerning testing in local conditions, data quality, cybersecurity, human review, documentation, and suspension after serious incidents.

Corporate responsibility presents another area of comparative concern. AI products may be supplied by foreign or domestic companies whose internal structures make individual attribution difficult. Chengeta's examination of autonomous weapons demonstrates that accountability may be dispersed among states, commanders, manufacturers, programmers, and operators (Chengeta, 2016). Iraqi law needs mechanisms capable of addressing companies that knowingly contribute to serious crimes or recklessly ignore the unlawful use of their systems. Corporate sanctions should not replace individual liability, but they can respond to organizational failures that cannot be reduced to one employee. Effective regulation should also address procurement contracts, due diligence, transparency, audit access, and the preservation of technical evidence.

Iran and Iraq share several structural similarities. Both rely heavily on codified criminal-law concepts and require a connection between the accused's conduct and the prohibited result. Both recognize distinctions between intentional and negligent wrongdoing. Both contain doctrines addressing principal offenders and accomplices. Both can treat technology as an instrument without granting it legal personality. Both also face the absence of a comprehensive AI statute specifically defining criminal responsibility across the AI life cycle. This shared gap means that prosecutors and courts would need to apply general rules to technologies characterized by opacity, autonomy, and distributed control. Sachoulidou's call for legislative action reflects the risk that purely traditional concepts may produce uncertainty when applied to advanced systems (Sachoulidou, 2024). The need for reform is therefore common to both jurisdictions.

The systems also differ in their institutional environments, legislative structures, and experiences with international criminal law. Iraq has had direct engagement with a specialized tribunal addressing genocide, crimes against humanity, and war crimes arising from past state violence. Iran's legal system has

developed within a different institutional and doctrinal context, with a stronger integration of Islamic criminal-law principles and domestic statutory categories. These differences may influence the interpretation of intention, causation, punishment, legal-person responsibility, and the relationship between domestic and international law. The comparative objective is not to declare one system superior but to identify how each can develop rules consistent with its own legal foundations while meeting the requirements of accountability.

The principle of legality presents a common obstacle to judicial innovation. Courts should not create entirely new offences or impose criminal responsibility by analogy. Schabas emphasizes that international criminal law requires strict interpretation and foreseeability (Schabas, 2016). Iran and Iraq should therefore address AI through legislation rather than relying exclusively on expansive judicial interpretation. Statutes should define high-risk AI, specify the duties of developers and operators, establish conditions for corporate liability, and clarify the relationship between system autonomy and causation. The legislation should remain technologically neutral enough to survive rapid innovation while identifying the functions that create heightened risk.

A comprehensive framework should distinguish categories of actors. The first category consists of intentional users who employ AI to commit or facilitate crimes. Their liability should generally follow existing doctrines of perpetration, ordering, and complicity. The second category includes operators and supervisors who control deployment and possess duties to monitor the system. Their liability may arise from intentional conduct, recklessness, negligence, or omission. The third category includes developers and manufacturers. They should be liable when they intentionally create unlawful functions, knowingly supply systems for criminal purposes, conceal serious defects, or recklessly disregard foreseeable risks. The fourth category includes corporate managers and legal persons. Their liability should depend on authorization, benefit, organizational policy, defective compliance, or failure to respond to known criminal use. The fifth category includes military commanders and civilian superiors whose responsibility arises from control, knowledge, and failure to prevent or repress crimes.

This layered model is consistent with the differentiated modes of liability recognized in international criminal law. Ambos emphasizes that responsibility should correspond to the actor's actual role in the crime (Ambos, 2021). A programmer should not be treated as a commander merely because their code was used in a military operation. A commander should not avoid responsibility by claiming lack of technical expertise. A corporate manager should not be liable for every employee's action, but may be responsible for policies that deliberately conceal risk. An operator should not be punished for an unforeseeable malfunction, but may be liable for ignoring obvious warning signs. The model therefore combines accountability with the principle of personal culpability.

Iran and Iraq should also establish mandatory human oversight for high-risk systems. Meaningful oversight requires that a human decision-maker possess sufficient information, competence, time, and authority to evaluate the system's output. Asaro's criticism of dehumanized lethal decision-making demonstrates that nominal human involvement is not enough (Asaro, 2012). A person who merely confirms an algorithmic recommendation without access to the underlying evidence does not provide meaningful control. Legislation should require explainable outputs where feasible, independent verification for high-impact decisions, and the ability to suspend operation. In military contexts, systems should not be deployed where their limitations prevent compliance with distinction and proportionality.

Auditability and evidence preservation are equally important. High-risk AI should generate records identifying the system version, training data sources, operational inputs, outputs, confidence levels, human interventions, and modifications. These records are essential for criminal investigation and defence rights. The black-box problem described by Matthias can otherwise make responsibility practically impossible to prove (Matthias, 2004). Iran and Iraq should develop specialized digital-forensics units and procedures for obtaining evidence from private companies, foreign service providers, and military institutions. Courts should have access to independent technical experts, while defendants should receive sufficient disclosure to challenge the evidence. Commercial secrecy and national

security cannot be permitted to eliminate fair-trial guarantees.

The regulation of autonomous weapons requires specific attention. Schmitt and Thurnher's approach suggests that weapon legality depends on capability, environment, and intended use rather than on a categorical assessment of autonomy (Schmitt & Thurnher, 2013). Iran and Iraq should require pre-deployment legal review, operational testing, geographic and temporal restrictions, human override mechanisms, and post-incident investigation. Commanders should be trained to understand system limitations and should not deploy systems in environments where reliable distinction is impossible. Sparrow's concern about the accountability gap supports a presumption that decisions concerning lethal force must remain traceable to responsible human authorities (Sparrow, 2007). This does not require manual control of every technical function, but it does require identifiable decision-makers who accept legal responsibility for deployment.

The proposed framework should also address cross-border cooperation. AI-related crimes may involve data stored abroad, software supplied by foreign companies, cloud infrastructure located in another jurisdiction, and operations affecting multiple states. Iran and Iraq need procedures for mutual legal assistance, preservation requests, extradition, expert cooperation, and transfer of electronic evidence. International crimes may also trigger universal or extraterritorial jurisdiction. Cryer, Robinson, and Vasiliev explain that jurisdictional rules are essential to preventing serious crimes from escaping prosecution because of territorial fragmentation (Cryer et al., 2019). AI increases this fragmentation by separating development, deployment, operation, and harm across jurisdictions.

The strongest comparative conclusion is that neither Iran nor Iraq needs to abandon the foundations of traditional criminal law. Existing doctrines remain capable of addressing deliberate and knowing uses of artificial intelligence. The principal reform need concerns clarification, evidence, preventive duties, and allocation of responsibility across complex technological systems. Neither country should recognize AI as a substitute offender. Solum's analysis of artificial personhood is valuable as a theoretical inquiry, but legal personality should not become a mechanism for transferring blame away from humans and organizations (Solum, 1992). The preferable approach is to treat AI as a regulated technological agent and to assign criminal responsibility to persons according to their knowledge, control, contribution, and failure to fulfil legally defined duties.

5. Conclusion

Artificial intelligence has altered the practical conditions under which crimes may be planned, facilitated, executed, concealed, and expanded. It allows individuals, corporations, military institutions, security agencies, and governmental authorities to process information and implement decisions at a scale and speed that were previously impossible. These capabilities can support legitimate public and private objectives, but they can also intensify the commission of serious crimes. The central legal problem is not that artificial intelligence makes responsibility conceptually impossible. The problem is that it redistributes decision-making among numerous actors and technological processes, making responsibility more difficult to identify and prove.

The analysis demonstrates that international criminal law remains capable of addressing many AI-related crimes through its existing principles. A person who intentionally uses an AI system to commit genocide, crimes against humanity, war crimes, or other serious offences remains criminally responsible. The system can be treated as an instrument through which the human actor implements a criminal purpose. Responsibility may also extend to persons who order, induce, facilitate, or knowingly assist the use of AI in a broader criminal operation. Military commanders and civilian superiors may be liable when they possess effective control, receive information indicating unlawful conduct, and fail to take necessary and reasonable measures. The involvement of a technologically autonomous system does not in itself eliminate the responsibility of the persons who selected, authorized, deployed, or supervised it.

The most serious difficulty concerns cases in which the harmful result was not specifically intended by any individual. Machine-learning systems may produce unexpected outputs, adapt to changing conditions, or operate through processes that cannot be fully explained. In such cases, criminal responsibility depends on whether the harm was foreseeable, whether the accused created or increased the risk, whether a legal

duty existed, whether warnings were ignored, and whether preventive measures were reasonably available. The law must distinguish genuine unpredictability from manufactured ignorance. A developer, commander, operator, or manager should not be able to invoke algorithmic opacity when the opacity resulted from inadequate testing, poor documentation, deliberate secrecy, or refusal to investigate known dangers.

Recognizing artificial intelligence as an independent criminal offender is not an adequate solution. Criminal responsibility is based on personal blameworthiness, legal capacity, and the normative significance of punishment. Current AI systems do not possess moral agency in the human sense, and sanctions such as deletion, deactivation, or reprogramming are better understood as preventive and regulatory measures. Granting AI criminal personhood could also weaken accountability by allowing human actors and corporations to attribute wrongdoing to the system. Artificial intelligence should therefore be treated as a legally relevant instrument, causal mechanism, and object of regulation rather than as the primary bearer of criminal blame.

The comparative analysis shows that the legal systems of Iran and Iraq contain general doctrines capable of addressing intentional AI-enabled conduct. Both systems can apply principles of perpetration, complicity, causation, intention, negligence, and omission. Both can treat AI as a means through which a human offender acts. Both also face significant gaps because their existing rules were developed before the emergence of highly autonomous and opaque systems. These gaps concern the definition of high-risk AI, the duties of developers and operators, the liability of corporate managers, the responsibility of legal persons, the treatment of algorithmic evidence, and the regulation of military AI.

The most appropriate reform is a multi-layered model of responsibility. Intentional users should be liable when they employ AI to commit or facilitate crimes. Operators and supervisors should be responsible when they knowingly or negligently fail to control high-risk systems. Developers and manufacturers should be liable when they deliberately create unlawful functions, conceal serious defects, or disregard foreseeable risks. Corporations and senior managers should be responsible when organizational policies facilitate criminal use or prevent effective oversight. Military commanders and civilian superiors should be accountable when they control deployment and fail to prevent or repress unlawful outcomes.

Legislation in Iran and Iraq should define high-risk artificial intelligence according to function and potential harm rather than according to a single technical model. It should establish mandatory testing, documentation, cybersecurity, human oversight, auditability, and incident-reporting obligations. It should require that autonomous systems used in military and security contexts remain subject to identifiable human authority. It should also clarify how causal responsibility is attributed when several actors contribute to the same technological process. These rules should preserve the principle of legality by providing clear standards before criminal liability is imposed.

Evidentiary reform is equally essential. Criminal responsibility cannot be established when technical records are unavailable, proprietary, classified, or deliberately destroyed. High-risk AI systems should preserve secure logs of their inputs, outputs, model versions, operational parameters, and human interventions. Investigators and courts should have access to qualified independent experts, while defendants should receive sufficient information to challenge the reliability and interpretation of technical evidence. National-security and commercial-secrecy claims should be managed through protective procedures rather than used to prevent judicial scrutiny.

The regulation of AI-related crimes must also protect against overcriminalization. Not every malfunction, programming error, or unexpected output should result in criminal punishment. Criminal liability should remain reserved for conduct involving the required degree of culpability and a sufficiently significant connection to the prohibited result. Civil, administrative, professional, and regulatory mechanisms should address lower levels of fault. This differentiated approach protects innovation while ensuring that serious risk creation and knowing contribution to criminal conduct do not escape accountability.

The ultimate principle is that technological autonomy must not produce legal irresponsibility. As artificial intelligence becomes more capable, the duties of those who design, deploy, control, and benefit from it must become more precise. The law should follow the

distribution of knowledge, power, and risk across the AI life cycle. Responsibility should remain human-centered, evidence-based, and proportionate to each actor's contribution. Iran and Iraq can respond effectively to AI-related international crimes by modernizing their domestic frameworks, strengthening institutional capacity, and aligning criminal responsibility with the realities of technologically mediated decision-making. The expansion of machine autonomy should therefore be accompanied by an equally significant expansion of human accountability, legal oversight, and enforceable duties of prevention.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Abbott, R., & Sarch, A. F. (2019). Punishing Artificial Intelligence: Legal Fiction or Science Fiction. *UC Davis Law Review*, *53*(1), 323-384. https://lawreview.law.ucdavis.edu/archives/53/1/punishing-artificial-intelligence-legal-fiction-or-science-fiction

Ambos, K. (2021). *Treatise on International Criminal Law, Volume I: Foundations and General Part* (2nd ed.). Oxford University Press. https://doi.org/10.1093/law/9780192844262.001.0001

Asaro, P. M. (2012). On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making. *International Review of the Red Cross*, *94*(886), 687-709. https://doi.org/10.1017/S1816383112000768

Chengeta, T. (2016). Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law. *Denver Journal of International Law and Policy*, *45*(1), 1-50. https://digitalcommons.du.edu/djilp/vol45/iss1/3/

Crootof, R. (2015). The Killer Robots Are Here: Legal and Policy Implications. *Cardozo Law Review*, *36*(5), 1837-1915. https://larc.cardozo.yu.edu/clr/vol36/iss5/6/

Cryer, R., Robinson, D., & Vasiliev, S. (2019). *An Introduction to International Criminal Law and Procedure* (4th ed.). Cambridge University Press. https://doi.org/10.1017/9781108680455

Hallevy, G. (2010). The Criminal Liability of Artificial Intelligence Entities: From Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*, *4*(2), 171-201. https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1/

Hallevy, G. (2013). *When Robots Kill: Artificial Intelligence under Criminal Law*. Northeastern University Press. https://books.google.com/books?id=9VvIMgEACAAJ

Matthias, A. (2004). The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata. *Ethics and Information Technology*, *6*(3), 175-183. https://doi.org/10.1007/s10676-004-3422-1

Sachoulidou, A. (2024). AI Systems and Criminal Liability: A Call for Action. *Oslo Law Review*, *11*(1), 1-10. https://doi.org/10.18261/olr.11.1.3

Schabas, W. A. (2016). *The International Criminal Court: A Commentary on the Rome Statute* (2nd ed.). Oxford University Press. https://doi.org/10.1093/law/9780198739777.001.0001

Schmitt, M. N., & Thurnher, J. S. (2013). Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict. *Harvard National Security Journal*, *4*(2), 231-281. https://harvardnsj.org/2013/05/22/out-of-the-loop-autonomous-weapon-systems-and-the-law-of-armed-conflict/

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231-1287. https://scholarship.law.unc.edu/nclr/vol70/iss4/4/

Sparrow, R. (2007). Killer Robots. *Journal of Applied Philosophy*, *24*(1), 62-77. https://doi.org/10.1111/j.1468-5930.2007.00346.x

Werle, G., & Jeßberger, F. (2020). *Principles of International Criminal Law* (4th ed.). Oxford University Press. https://global.oup.com/academic/product/principles-of-international-criminal-law-9780198826859