

Appropriate Sanctions for Crimes Involving Artificial Intelligence Systems

Mohammad Ali Haji Deh Abadi^{1*}, Ahmad Rahman Dawood Haider²

^{1*}*Associate Professor, Department of Criminal Law, University of Qom, Qom, Islamic Republic of Iran | Email: Dr-hajidehabadi@yahoo.com*

²Ph.D. Candidate in Criminal Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran
| Email: ahmed.rahman@au.edu.iq

***Corresponding Author:** Mohammad Ali Haji Deh Abadi, Associate Professor, Department of Criminal Law, University of Qom, Qom, Islamic Republic of Iran | Email: Dr-hajidehabadi@yahoo.com

Abstract

Artificial intelligence-related crime is expanding in parallel with rapid technological development, creating an urgent need for appropriate sanctions that safeguard individuals and society. Such offences include the use of artificial intelligence systems to commit fraud, violate privacy, disseminate misinformation, and carry out cyberattacks. The applicable sanctions should be proportionate to the gravity of the harm caused and the degree of the offender's criminal responsibility. They may include financial penalties, custodial sanctions in serious cases, and compensation for the damage sustained by victims. A clear legal framework can curb the misuse of artificial intelligence technologies and promote their responsible use.

Keywords

Artificial Intelligence Systems; Cybercrime; Criminal Liability; Criminal Sanctions

Introduction

The central question in this context concerns the criminal sanctions that may be imposed in connection with artificial intelligence systems. Should the traditional sanctions applicable to natural persons be extended to such systems, or should a distinct category of sanctions be devised to reflect their technical nature? Similar questions arose when legal systems began to recognise the criminal liability of legal persons. One possible response is to enact legislation specifically governing artificial intelligence systems and prescribing sanctions suited to their distinctive characteristics. Under the principle of legality—*nullum crimen, nulla poena sine lege*—no conduct may be criminalised and no person may be punished for an act in the absence of a prior legal provision. Although conventional criminal sanctions may not correspond to the nature of artificial intelligence systems, punishment, like every other component of criminal law, must evolve in response to emerging social needs and technological developments. Pending the enactment of legislation regulating criminal liability arising from artificial intelligence systems, this research proposes sanctions tailored to such systems, together with sanctions appropriate to the criminal liability of the other parties involved.

Significance of the Research

The significance of this research stems from the accelerating development of artificial intelligence technologies and their increasing use across all areas of life. Advanced programming may enable certain AI-driven machines to reach levels of autonomy at which they can make decisions independently. This development creates the prospect that artificial intelligence applications may engage in conduct producing criminal consequences and may, in the future, act independently of their owners or programmers. It is therefore necessary to examine the criminal liability arising from such offences, identify the person or entity legally responsible, and determine the sanction that should be imposed.

Research Problem

To what extent are the legal sanctions currently in force adequate and effective in addressing crimes associated with artificial intelligence devices and systems and in achieving deterrence and justice amid the rapid development of these technologies? A further methodological difficulty lies in structuring the research in a manner that organises its interrelated issues logically and enables the reader to access the relevant legal analysis clearly and systematically.

Research Methodology

This research adopts a descriptive and analytical methodology. It first describes the concepts and developments generated by artificial intelligence technologies and then analyses the legislative approaches adopted at the international, regional, and national levels in order to identify the most appropriate legal rationale. It also seeks to determine the most applicable legal characterisation in light of relevant doctrinal theories and judicial decisions. The research is prospective in nature, as it examines the legal frameworks that may regulate criminal liability arising from the unlawful use of artificial intelligence systems.

Structure of the Research

The subject is examined through two sections. The first addresses the proposed sanctions applicable to programmers, manufacturers, owners, users, and external actors involved with artificial intelligence systems. The second examines the sanctions that may be specifically imposed on artificial intelligence systems themselves.

First Section

Sanctions Applicable to External Actors in Relation to Artificial Intelligence Systems

No conduct may be regarded as a criminal offence, nor may any person be punished for an act committed, unless that act has been expressly criminalised by legislation in force¹. This proposition embodies one of the fundamental components of the criminal-law principle of legality. It has been adopted by numerous legal systems, including the Egyptian and Iraqi systems. The Egyptian Constitution provides that: "Punishment is personal. There shall be no crime or punishment except pursuant to law; no punishment shall be imposed except by a judicial judgment; and punishment shall apply only to acts committed after the law enters into force"². Similarly, Article 1 of Iraqi Penal Code No. 111 of 1969 states: "No act or omission shall be punishable unless a law in force at the time of its commission provides for its criminalisation, and no penalty or precautionary measure may be imposed unless prescribed by law"³. The Egyptian Supreme Constitutional Court has affirmed this principle in numerous judgments. Consequently, conduct cannot be treated as criminal unless an explicit legal provision has been enacted by the competent legislative authority or promulgated by a decree-law issued by the President of the Republic in accordance with the Constitution⁴.

Where criminal liability is established against programmers, owners, and users of artificial intelligence systems for unlawful conduct, such liability must entail a sanction proportionate to the dangerousness and gravity of the conduct, as explained below.

First: Sanctions Applicable to the Manufacturer and Programmer

As previously indicated, a distinction may be drawn between the manufacturer and the programmer in the development of artificial intelligence systems. They may be separate persons, or both roles may be performed by the same person. Accordingly, criminal liability and the applicable sanctions must be determined in each case as follows.

Section 1: Sanctions Applicable to the Manufacturer as the Party Responsible for Manufacturing and Programming

¹ Ahmed Fathi Sorour, *Constitutional Criminal Law*, 2nd ed., Dar Al-Shorouk, Cairo, p. 31.

² The Egyptian Constitution, as amended in 2019.

³ Article 1, Iraqi Penal Code No. 111 of 1969.

⁴ Mahmoud Ahmed Taha, *Commentary on the Penal Code: General Part, Part Two, General Theory of Criminal Responsibility and Criminal Sanction*, university textbook, n.d., p. 78.

The manufacturer of an artificial intelligence system bears primary responsibility for designing its operational architecture and is therefore best positioned to control its performance and anticipate its actions. The manufacturer should consequently be legally required to incorporate safety and security mechanisms enabling the user to regain control if the system behaves unpredictably or escapes ordinary supervision⁵. This obligation requires the manufacturer to adopt the technical and legal precautions necessary to protect users, particularly because certain systems may possess self-learning or adaptive capabilities. Producing such systems without compliance with applicable safety and security standards should therefore constitute conduct capable of attracting criminal liability.

Criminal legislation should accordingly establish clear statutory provisions defining mandatory quality and safety standards, criminalising their violation, and specifying appropriate sanctions where those obligations are breached during the manufacturing process⁶.

The manufacturer's criminal liability varies according to the legal classification of the offence generated through the system, whether a felony, misdemeanour, or contravention⁷. Relevant considerations include the gravity of the harm and the manufacturer's state of mind, including whether the absence of effective control mechanisms resulted from negligence or whether the system was intentionally designed to facilitate criminal conduct. Accordingly, the sanctions prescribed by criminal law may apply, ranging, where legally available, from capital punishment and life or fixed-term imprisonment to detention, fines, and ancillary or supplementary penalties. The manufacturer may also be a legal person; in that event, sanctions appropriate to legal persons should apply once its responsibility for the offence has been established⁸.

Section 2: Sanctions Applicable to the Programmer

In some cases, the programmer is a natural person who operates independently of the manufacturer. This requires a distinction between two principal forms of criminal liability according to the nature of the programming conduct.

A. Liability for Intentional Offences and Their Foreseeable Consequences

A programmer may intentionally develop code that enables an artificial intelligence system to commit a criminal offence, such as programming a robot to carry out a robbery against a banking institution. In such a case, the programmer is criminally responsible for the principal offence, namely robbery, under the applicable penal provisions.

The legal position becomes more complex where the intelligent system exceeds the limits of its original programming, for example by killing a security guard during the robbery even though the programmer did not specifically intend that result. In such circumstances, the programmer may be held responsible for the intentional offence of robbery and for the killing as a foreseeable or probable consequence of the original criminal conduct, notwithstanding the absence of a direct intention to cause death⁹.

B. Liability for Unintentional Offences

Where an offence is committed through an artificial intelligence system because of an unintended programming error, including negligence, recklessness, inattention, failure to exercise due care, or breach of applicable regulations, instructions, or technical standards during the programming process¹⁰, the programmer's liability is based on unintentional fault. The programmer is then criminally liable according to the nature of the resulting offence, and the statutory provision governing the corresponding negligent offence should be applied.

⁵ Moussa Omri and Bilal Ouis, *The Legal Consequences of the Use of Artificial Intelligence*, Master's thesis submitted to the Faculty of Law and Political Science, Ziane Achour University of Djelfa, Algeria, 2020–2021, p. 44.

⁶ Mahmoud Mohammed Sweif, *Artificial Intelligence Crimes (The New Criminals)*, Dar Al-Jamiaa Al-Jadida, Alexandria, 2022, p. 14.

⁷ Article 23, Iraqi Penal Code No. 111 of 1969.

⁸ Mahmoud Mohammed Sweif, *Artificial Intelligence Crimes (The New Criminals)*, Dar Al-Jamiaa Al-Jadida, Alexandria, 2022, p. 14.

⁹ Ahmed Ibrahim Mohammed Ibrahim, *Criminal Liability Arising from Artificial Intelligence Errors under UAE Legislation*, 1st ed., Al-Muttahida Publishing and Distribution, Sharjah, 2022, p. 138.

¹⁰ See Article 35, Iraqi Penal Code No. 111 of 1969.

Second: Criminal Liability and Sanctions Applicable to the Owner or User and to External Actors

In certain cases, offences are committed through the use of artificial intelligence systems by their owner or user. In other cases, an external actor may exploit technical vulnerabilities in such systems for criminal purposes. The resulting forms of criminal liability and the corresponding sanctions may be classified as follows:

1. Sanctions Applicable to the Owner or User

A person who possesses an artificial intelligence system, whether as its owner or user, may incur criminal liability because that person is ordinarily capable of controlling the system and benefiting from its functions. Accordingly, the owner or user may bear the consequences of criminal conduct carried out through the system, whether the conduct is intentional or results from negligence. This liability may arise in two principal forms:¹¹

A. Liability for Intentional Offences and Their Foreseeable Consequences

Where the owner or user employs an artificial intelligence system with the intention of committing an offence—for example, by activating a robot to carry out a homicide—that person is criminally liable under the provisions governing the offence of homicide. The same principle applies where the system is intentionally used to assault another person with the purpose of causing injury, beating, or other bodily harm; the sanctions prescribed by criminal law apply according to the legal classification of the offence. Criminal liability also extends to foreseeable consequences arising during the execution of the principal offence, even where the owner or user did not expressly intend those additional consequences.¹²

B. Liability for Unintentional Offences

Where an offence results from the owner's or user's misuse of the system without criminal intent—for example, through negligence, recklessness, inattention, failure to exercise due care, or non-compliance with applicable rules, instructions, or regulatory orders—liability is based on unintentional fault. In such a case, the penal provision governing the resulting negligent offence applies in accordance with its gravity and the harm caused.¹³

2. Sanctions Applicable to an External Actor

Where an external actor who neither owns the technology nor uses it lawfully exploits a defect or security vulnerability in an artificial intelligence system, whether through hacking or any other means, and redirects the system toward criminal conduct, that person is regarded as a principal offender in an intentional offence. The offender is therefore subject to the statutory sanctions governing the offence committed, whether theft, sabotage, assault, or another crime. Liability may also extend to an additional foreseeable offence occurring during the execution of the principal crime, even if it was not directly planned. The conduct cannot properly be characterised as unintentional because the external actor acts voluntarily and knowingly, exploiting the system's weakness to achieve a specific criminal purpose.¹⁴

Second Section

Sanctions Applicable to Artificial Intelligence Systems

Any discussion of imposing sanctions directly on artificial intelligence systems presupposes a fundamental condition: that such systems possess the capacity to make independent decisions and act with a meaningful degree of autonomy. Major advances in the manufacture and programming of AI systems have enabled certain technologies to learn from prior experience and retain accumulated data, thereby granting them a degree of operational independence. From this perspective, and particularly as conventional AI develops toward more advanced forms of machine cognition, it may theoretically become possible to attribute responsibility to AI systems for conduct

¹¹ Musa Omari and Bilal Weiss, *Legal Consequences Arising from the Use of Artificial Intelligence*, Master's thesis submitted to the Faculty of Law and Political Science, Ziane Achour University, Djelfa, Algeria, 2020–2021, p. 44.

¹² Imad al-Din Hamid Al-Shafi'i, "Criminal Liability for Artificial Intelligence Crimes," *Journal of Law for Legal and Economic Research*, Faculty of Law, Alexandria University, vol. 2, no. 3, 2019, p. 638.

¹³ See Iraqi Penal Code No. 111 of 1969, Article 35.

¹⁴ Haskar Murad Ben Ouda, "The Problem of Applying the Rules of Criminal Liability to Artificial Intelligence Crimes," *Journal of Law and Human Sciences*, University of Tlemcen, Algeria, vol. 15, no. 1, 2022, p. 199.

emanating from them. As scientific research continues to reduce the complete dependence of robots on natural persons, the foundations for holding highly autonomous AI systems criminally accountable for legally prohibited acts may emerge in the future.

The sanctions prescribed by traditional criminal legislation may not be sufficient to achieve deterrence or the punitive effect ordinarily associated with criminal punishment when applied to artificial intelligence systems. This requires reconsideration of the nature of the sanctions that could be imposed upon such systems. Any proposed sanction must correspond to their distinctive characteristics, especially if technological development results in highly intelligent and substantially autonomous machines. Criminal legislation must therefore keep pace with this development by introducing sanctions suited to these emerging offences and consistent with the systems' technical structure, functions, and potential consequences.

Artificial intelligence systems may be tangible, such as robots, autonomous vehicles, and unmanned or self-driving aircraft, or intangible, such as intelligent software and expert systems. Their functions vary according to the sectors in which they are deployed, while the effects of their operation depend on the degree of social need for them and the level of flexibility or risk associated with their use. If the legal conditions for criminal accountability were ultimately satisfied, a distinct category of sanctions specifically designed to address their technical and functional characteristics could be considered.¹⁵

First: Dismantling, Deactivation, or Confiscation

Dismantling an artificial intelligence system may be compared, by analogy, to the death penalty imposed on a natural person. Under this approach, the system would be permanently destroyed or deactivated where it has escaped effective control and poses a serious threat to human safety. Confiscation may also be ordered, resulting in the transfer of ownership of the system to the State.¹⁶

This proposal theoretically assumes that an artificial intelligence system would possess an independent legal status, including legal capacity and a separate financial patrimony, so that the sanction could be enforced against the system as an autonomous legal entity rather than against its owner.

Nevertheless, this form of sanction raises a significant legal difficulty because its practical effects fall directly upon the system's owner. Confiscation or permanent deactivation affects the owner's property rights and may therefore burden that person indirectly, even though the sanction is formally directed at the system itself.

Second: Financial Sanctions

A fine is one of the principal financial sanctions that might be contemplated. In theory, fines may be imposed on natural persons, legal persons, and, under a future legal framework, artificial intelligence systems. Such a sanction would require the system to pay a sum determined by the court into the State treasury, with payment drawn from the separate financial patrimony that the law would have to recognise for that entity.

Third: Rights-Restricting Sanctions

Measures tailored to the nature of artificial intelligence systems could also be imposed. One example is rehabilitation, which may be particularly suitable for such systems because it seeks to modify their conduct or functions and return them to operation in a safer form. This could be achieved through reprogramming, technical adjustment, or the restriction of specific capabilities. Another possible measure is the revocation or suspension of an operating licence, as in the case of autonomous vehicles, where withdrawal of the licence would prevent operation for the prescribed period. This sanction, however, creates a further difficulty because its actual consequences are borne by the owner or user, even though the measure is nominally directed at the system.

The researcher considers that the adverse effects suffered by owners or users as a result of sanctions imposed on artificial intelligence systems, despite the absence of any fault justifying their liability, provide an additional reason for legislative intervention. New provisions should be enacted, or existing provisions amended, to accommodate the distinctive nature of offences

¹⁵Dona Ibrahim Hilal, *Artificial Intelligence*, Master's thesis submitted to the Faculty of Law, Political and Administrative Sciences, Lebanese University, 2021, p. 110.

¹⁶The French legislature provides for dissolution as a sanction applicable to legal persons and treats it as analogous to the death penalty imposed on natural persons, being the most severe sanction that may be pronounced against a legal person. It also provides for prohibitions on public appeals for savings and the use of cheques, restrictions on professional or social activities, and publication of the judgment of conviction. See Rana Ibrahim Al-Atour, *Criminal Encyclopedia: Commentary on the UAE Federal Penal Code, General Part, A Comparative Study with Jordanian Law and the New French Penal Code*, Ministry of Justice, Institute of Training and Judicial Studies, United Arab Emirates, 2016, p. 374.

arising from the unlawful use of AI systems. Such legislation should define criminal responsibility precisely and confine the effects of punishment within a fair legal framework, so that sanctions do not extend to persons who bear no responsibility, just as the incidental effects of sanctions imposed on natural or legal persons must also be carefully limited.

Conclusion

This research demonstrates that the rapid development of artificial intelligence systems has created new legal challenges for traditional criminal legislation. Such legislation was originally designed to address conduct committed by natural persons who possess legal capacity, awareness, and the ability to make decisions. In artificial intelligence systems, however, a criminal result may occur even where some of the conventional elements required for criminal liability are absent or difficult to establish.

Findings

1. Traditional rules of criminal liability are not capable of addressing all the legal problems arising from the use of artificial intelligence technologies.
2. Artificial intelligence systems do not currently possess a recognised legal personality to which criminal liability may independently be attributed.
3. Criminal liability is generally attributed to the programmer, owner, or user, according to the degree of control and supervision exercised over the system.
4. Establishing the causal link between human fault and the criminal result becomes increasingly difficult as artificial intelligence systems acquire greater autonomy and an enhanced capacity to make independent decisions.
5. The absence of clear technical standards and effective regulatory oversight governing artificial intelligence systems—from the manner in which they process commands to the extent of their decision-making autonomy and the ethical design of their algorithms—contributes to an increased risk of harm and criminal misuse.

Recommendations

1. Enact dedicated legislation regulating artificial intelligence and precisely defining the criminal liability arising from its design, development, operation, and use.
2. Introduce specialised technical sanctions proportionate to the nature of artificial intelligence systems, including temporary or permanent deactivation, restriction of particular functions, and confiscation of dangerous software.
3. Establish a specialised national authority responsible for supervising artificial intelligence applications and licensing high-risk systems.
4. Encourage the conclusion of international agreements regulating the use of artificial intelligence and addressing its cross-border risks.
5. Establish a national register of intelligent systems used in sensitive sectors, including security, health, transport, and financial services.

References

(1) Books

1. Ahmed Fathi Sorour, *Constitutional Criminal Law*, 2nd ed., Dar Al-Shorouk, Cairo.
2. Rana Ibrahim Al-Atour, *Criminal Encyclopaedia: Commentary on the Federal Penal Code of the United Arab Emirates, General Part: A Comparative Study with Jordanian Law and the New French Penal Code*, Ministry of Justice, Institute of Training and Judicial Studies, United Arab Emirates, 2016.

3. Ahmed Ibrahim Mohammed Ibrahim, Criminal Liability Arising from Artificial Intelligence Errors under UAE Legislation, 1st ed., Al-Muttahida Publishing and Distribution, Sharjah, 2022.
4. Mahmoud Mohammed Sweif, Artificial Intelligence Crimes (The New Criminals), Dar Al-Jamia Al-Jadida, Alexandria, 2022.
5. Mahmoud Mohammed Sweif, Artificial Intelligence Crimes (The New Criminals), Dar Al-Jamia Al-Jadida, Alexandria, 2022.
6. Mahmoud Ahmed Taha, Commentary on the Penal Code, General Part, Vol. II, General Theory of Criminal Liability and Criminal Sanctions, university textbook, n.d.

(2) Theses, Dissertations, Research Papers, and Journal Articles

1. Dona Ibrahim Hilal, Artificial Intelligence, Master's thesis submitted to the Faculty of Law, Political and Administrative Sciences, Lebanese University, 2021.
2. Haskar Mourad Ben Ouda, "The Problem of Applying the Rules of Criminal Liability to Artificial Intelligence Crimes," Journal of Law and Human Sciences, University of Tlemcen, Algeria, Vol. 15, No. 1, 2022.
3. Moussa Omari and Bilal Weiss, Legal Consequences Arising from the Use of Artificial Intelligence, Master's thesis submitted to the Faculty of Law and Political Science, Ziane Achour University of Djelfa, Algeria, 2020–2021.
4. Moussa Omari and Bilal Weiss, Legal Consequences Arising from the Use of Artificial Intelligence, Master's thesis submitted to the Faculty of Law and Political Science, Ziane Achour University of Djelfa, Algeria, 2020–2021.
5. Imad Al-Din Hamed Al-Shafie, "Criminal Liability for Artificial Intelligence Crimes," Journal of Law for Legal and Economic Research, Faculty of Law, Alexandria University, Vol. 2, No. 3, 2019.

(3) Legislation

1. Iraqi Penal Code No. 111 of 1969.
2. The Egyptian Constitution, as amended in 2019.