The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.06 Issue06 2026
PAGE NO. 81-91
DOI 10.37547/ijlc/Volume06Issue06-16

Crimes Committed by Means of Artificial Intelligence: Concept, Features and Legal Nature

Saidov Abdumannon G‘ayrat o‘g‘li

Master's degree, Cabinet Manager, Department of Criminal Legal Sciences, Academy of Justice of the Republic of Uzbekistan, Tashkent, Uzbekistan

Received: 04 May 2026; **Accepted:** 02 June 2026; **Published:** 30 June 2026

Abstract: Purpose. Autonomous, self-learning artificial intelligence (AI) systems strain the core categories of criminal law: act, causation, guilt and the subject of crime. This article clarifies the concept, features and legal nature of crimes committed by means of AI and proposes a doctrinal definition for the criminal law of Uzbekistan.

Design/methodology. Doctrinal, comparative-legal, systemic and formal-logical methods are applied to the definitions of AI in the OECD Recommendation (2019, amended 2024), the UNESCO Recommendation (2021), the EU AI Act (2024), the Chinese Interim Measures on generative AI (2023), US and UK sources, and Uzbek Law No. ZRU-1115 of 21 January 2026. These are then tested against the General Part of the Criminal Code of Uzbekistan and the international literature.

Findings. Four properties of AI carry criminal-law weight: autonomy, self-learning, unpredictability of outputs and algorithmic opacity (the "black box"). AI-enabled crime differs from computer crime and cybercrime because harm results from the system's autonomous algorithmic decision-making, not from a passive digital tool. Five specific features are identified: partial autonomy of the means; remoteness and transnationality; scale and automation; high latency and evidentiary difficulty; and limited foreseeability of consequences.

Originality/value. The article offers an author's definition of AI-enabled crime and a liability-allocation model grounded in existing provisions of the Uzbek Criminal Code (Articles 9, 17, 20–24, 28 and 41). It argues that AI is a high-risk autonomous instrument, not a subject of crime, and that "electronic personhood" would shield developers, operators and users from responsibility.

Keywords: Artificial intelligence; AI-enabled crime; criminal liability; responsibility gap; black box; electronic personhood; causation; Uzbekistan.

1. Introduction: Artificial intelligence has moved from research laboratories into everyday economic and social life, and offenders have followed. Generative models now draft convincing phishing messages, synthesise voices and faces for fraud, and automate attacks at a scale no individual could reach (Caldwell et al., 2020; King et al., 2020). What is new is not that a computer is involved. For the first time, the means used to commit a crime is not a passive, pre-programmed algorithm but a system that can learn from data and choose its own course of action within a task.

This shift reaches the foundations of criminal law. A doctrine built around human conduct must now answer three questions. Can an act performed by an autonomous system be attributed to a person? How is causation established when the decisive step was taken inside an opaque model? How is guilt assessed when the outcome was not foreseen even by the system's developer (Abbott & Sarch, 2019; Matthias, 2004)? For investigators and courts, the practical result is uncertainty about how to qualify the conduct, whom to hold liable, and how to distribute responsibility among

developers, owners, operators and users.

Uzbekistan illustrates both the momentum and the gap. AI was recognised as a driver of the digital economy in Presidential Decree No. PF-6079 of 5 October 2020 and Presidential Resolution No. PQ-4996 of 17 February 2021. Law No. ZRU-1115 of 21 January 2026 then added the first statutory definition of AI to Article 3 of the Law "On Informatization" and introduced administrative liability for the unlawful processing of personal data using AI (Law No. ZRU-1115, 2026). The Criminal Code, however, contains no provisions addressed to AI. National scholarship has concentrated on whether AI itself could bear liability (Bozarov, 2021; Voxidov, 2025). It has not et produced a criminal-law concept of AI-enabled crime with defined features.

This article addresses that gap through four research questions:

1. What do international and national normative definitions of AI contribute to criminal-law analysis?
2. What distinguishes a crime committed by means of AI from computer crime and cybercrime?
3. What general and specific features characterise such crimes, and how do they map onto the elements of the corpus delicti?
4. What is the legal nature of AI in criminal law, and on whom should liability fall?

Section 2 describes the materials and methods. Section 3 presents the results: a comparison of definitions, the criminally relevant properties of AI, the author's definition, the features of AI-enabled crime and the competing doctrinal concepts. Section 4 sets out the case against electronic personhood and shows how existing provisions of the Uzbek Criminal Code can close the responsibility gap. Section 5 concludes.

2. METHODS

The study is doctrinal legal research with a comparative component. Its materials fall into three groups:

- **International and foreign instruments:** the OECD Recommendation of the Council on Artificial Intelligence (OECD, 2024), the UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021), Regulation (EU) 2024/1689 (the AI Act), the Chinese Interim Measures for the Management of Generative AI Services (Cyberspace Administration of China et al., 2023), the US National Artificial Intelligence Initiative Act of 2020 and the UK white paper on AI regulation (Department for Science, Innovation and Technology, 2023).
- **Legislation of Uzbekistan:** Decree No. PF-6079 (2020), Resolution No. PQ-4996 (2021), the Law "On Informatization" as amended by Law No. ZRU-1115 (2026), and the Criminal Code of 22 September 1994 as amended to 2026.
- **Doctrine in English, Russian and Uzbek:** the leading Western works on AI and criminal liability (Abbott & Sarch, 2019; Bryson et al., 2017; Hallevy, 2010, 2015; King et al., 2020; Matthias, 2004; Pagallo, 2013) and post-Soviet scholarship (Bakhteev, 2024; Begishev & Khisamova, 2018; Bozarov, 2021; Laptev, 2019; Morhat, 2017; Ponkin & Redkina, 2018; Voxidov, 2025).

Five methods were applied. The **comparative-legal method** compared definitions of AI on five criteria: technological basis, autonomy, adaptiveness, type of output and imitation of human cognition. The **formal-dogmatic method** was used to interpret the General Part of the Criminal Code, in particular Articles 9 (principle of guilty liability), 14 (concept of crime), 17 (natural persons as subjects), 20–24 (forms of guilt and innocent infliction of harm), 28 (perpetration through other means) and 41 (justified professional risk). The **systemic method** mapped the features of AI-enabled crime onto the elements of the corpus delicti. **Critical analysis** was applied to the competing concepts of the legal nature of AI. The **formal-logical method** (definition by genus and specific difference) was used to construct the author's definition.

Translations of Uzbek and Russian sources are the author's own. The study is doctrinal and does not include an empirical analysis of judicial practice.

3. RESULTS

3.1 Normative definitions of artificial intelligence

No universal definition of AI exists, and this remains one of the weakest points of legal regulation. The instruments compared below converge on three elements — a machine-based system, inference or learning, and outputs that affect the environment — but differ in emphasis, and the differences matter for criminal law (Table 1).

The OECD Recommendation, adopted in 2019 and amended in 2024, describes an AI system as a machine-based system that, for explicit or implicit objectives, infers from its input how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments; systems vary in autonomy and adaptiveness after deployment (OECD, 2024). The UNESCO Recommendation of 2021 instead stresses the capacity to process information, learn and perform cognitive tasks, that is, to imitate human intellectual activity (UNESCO, 2021). Article 3(1) of the EU AI Act turns the OECD approach into a binding, risk-based definition: a machine-based system designed to operate with varying levels of autonomy, which may exhibit adaptiveness after deployment and infers outputs that influence physical or virtual environments (Regulation (EU) 2024/1689). US federal law emphasises predictions and decisions made for human-defined objectives (National Artificial Intelligence Initiative Act, 2020), and the UK government defines AI by its adaptivity and autonomy (Department for Science, Innovation and Technology, 2023). Chinese regulation of generative AI makes the automatic generation of content its key legal criterion (Cyberspace Administration of China et al., 2023).

In Uzbekistan the legal definition developed in stages. Decree No. PF-6079 (2020) and Resolution No. PQ-4996 (2021) treated AI as a technological field driving the digital economy. Law No. ZRU-1115 (2026) then inserted the first conceptual statutory definition into Article 3 of the Law "On Informatization": AI is a set of technological solutions that makes it possible to imitate human knowledge and skills, including independent learning and the search for solutions, and to obtain, when performing specific tasks, results comparable to those of human intellectual activity.

Table 1. Definitions of AI in international, foreign and national instruments

Instrument	Year	Core elements of the definition	Relevance for criminal law
OECD Recommendation on AI (OECD/LEGAL/0449)	2019, amended 2024	Machine-based; infers outputs from input; varying autonomy and adaptiveness; influences physical or virtual environments	Output-based; ties the system's output to effects in the world, i.e. to causation
UNESCO Recommendation on the Ethics of AI	2021	Information processing; learning; performance of cognitive tasks	Imitation of cognition explains why AI outputs resemble human decisions
EU AI Act, Art. 3(1)	2024	Machine-based; varying autonomy; adaptiveness after deployment; inferred outputs	Binding and risk-based; autonomy and adaptiveness raise the foreseeability problem
US National AI Initiative Act, 15 U.S.C. § 9401(3)	2020	Machine-based; human-defined objectives; predictions, recommendations, decisions	Functional; objectives remain with humans
UK white paper on AI regulation	2023	Adaptivity and autonomy	Functional; no statutory definition

Instrument	Year	Core elements of the definition	Relevance for criminal law
China, Interim Measures on Generative AI Services	2023	Models generating text, images, audio, video and other content	Content generation; relevant to deepfakes and disinformation
Uzbekistan, Law "On Informatization", Art. 3 (as amended by ZRU-1115)	2026	Technological solutions; imitation of human knowledge and skills; self-learning; results comparable to human intellectual activity	First national statutory definition; basis for treating AI as a means of crime

Three observations follow. First, the Uzbek definition follows the cognitive-imitation model closest to UNESCO's. It does not mention autonomy expressly, but "independent learning and the search for solutions" implies it. Second, Law No. ZRU-1115 also provides that legally significant decisions affecting human rights and freedoms may not rest solely on the conclusions of AI-based systems. This is a human-in-the-loop principle consistent with the human-centred model of liability defended below. Third, for criminal law the technical parameters of AI matter less than the properties that generate criminogenic risk.

3.2 Criminally relevant properties of AI

Four properties distinguish AI from conventional software, and each strains a different category of criminal law.

1. **Autonomy.** Conventional programs execute a fixed algorithm and human commands. AI systems select the sequence of actions and intermediate decisions themselves within a given task. Category strained: attribution of the act to a person.
2. **Self-learning and adaptiveness.** Neural networks draw inferences from incoming data and dynamically change their own model. Category strained: causation, because the system that caused harm is no longer the system that was released.
3. **Unpredictability of outputs.** Deep-learning systems and large language models with billions of parameters may develop behaviour that neither the developer nor the operator foresaw (Matthias, 2004). Category strained: foreseeability, on which negligence depends.
4. **Opacity (the "black box").** It is often impossible to establish objectively which factors and internal processes led the system to a harmful decision. The logical chain linking a given input to a given output cannot be fully explained by external observers, including programmers and law-enforcement experts (Bozarov, 2021; Burrell, 2016; Pasquale, 2015). Category strained: proof of causation and guilt, and identification of the liable person.

Taken together, these properties explain why AI-enabled crime cannot be treated simply as computer crime committed with a more powerful tool.

3.3 Terminology and the author's definition

AI-enabled crime is a distinct category: the harm results from the system's autonomous decision-making, not from the use of a passive digital tool.

The literature uses several overlapping terms: "AI crime", crimes committed using AI capabilities, crimes committed with the help of AI, "AI-related crimes", "cybercrimes" and "crimes in the field of information technology". Russian criminologists tend to treat AI-related criminality as a further, higher stage of information-technology crime (Begishev & Khisamova, 2018; Khisamova et al., 2019). The international literature speaks of "AI-crime" (King et al., 2020) and "AI-enabled crime" (Caldwell et al., 2020).

A useful distinction separates two situations. In the first, AI is an auxiliary tool that makes a traditional offence easier, for example by drafting phishing texts.

In the second, the offence relies on an algorithmic system and could not be committed without AI at all. The distinction parallels the division of cybercrime into cyber-enabled and cyber-dependent offences (McGuire & Dowling, 2013) and the typology in which AI may be the tool, the target or the context of a crime (Caldwell et al., 2020).

The boundaries with neighbouring categories matter for qualification. "Computer crimes" and "crimes in the field of information technology" cover direct attacks on computer systems and information security, or the use of a computer as a passive, automatic instrument. "Cybercrime" covers the broad set of acts committed through cyberspace and information and communication networks. AI-enabled crime differs from both in quality. The point is not the mere use of digital technology but the causation of socially dangerous consequences through the system's autonomy, algorithmic decision-making and imitation of human cognition. Nor is AI-enabled crime simply a subset of cybercrime: an autonomous vehicle or industrial robot can cause harm offline, while most cybercrime involves no AI. The two categories overlap rather than nest.

Existing doctrinal definitions show two opposite weaknesses. Some authors present AI as an independent subject or "perpetrator" of crime (Hallevy, 2010; Morhat, 2017). This contradicts the principles of guilt and of the human-centred nature of criminal liability. Others reduce AI to an ordinary technical instrument. This overlooks the "responsibility gap" created by autonomy and unpredictability (Matthias, 2004; Santoni de Sio & Mecacci, 2021).

On this basis the following definition is proposed:

> **Definition.** A crime committed by means of artificial intelligence is a socially dangerous act prohibited by the Criminal Code, committed through the intentional or negligent use by a human being of an artificial intelligence system possessing the properties of cognitive imitation, autonomy and algorithmic decision-making, or through a failure to exercise due control over the operation of such a system, and culpably causing harmful consequences.

The definition rests on three grounds:

1. It characterises AI not as an independent subject but as an autonomous and complex **means** of committing a crime.
2. It fixes the **human being** — developer, operator or user — as the sole bearer of guilt and criminal liability.
3. It covers not only intentional use but also criminogenic situations arising from a failure to maintain proper **control and audit** over the algorithm, that is, negligence.

The definition is built as a species of the statutory genus in Article 14 of the Criminal Code, which defines a crime as a culpable, socially dangerous act prohibited by the Code under threat of punishment.

3.4 Features of AI-enabled crime

AI-enabled crime shares the general features of every crime but also has five specific features, each bearing on a particular element of the corpus delicti.

Among the general features, **social danger** is heightened: unlike offences resting on individual human effort, AI allows deliberate harm on a mass scale. **Unlawfulness** lies in committing an act described in the Special Part of the Criminal Code through algorithmic means. **Culpability and punishability** follow the principle of guilty liability (Article 9) and the forms of guilt (Article 20). They are expressed solely through the mental attitude of the natural person who created, configured or used the algorithm.

Table 2. Specific features of AI-enabled crime and the elements they affect

Feature	Content	Element of the corpus delicti affected	Typical scenario
1. Partial autonomy of the means	The system chooses intermediate actions and decisions itself	Objective side: the act and the causal link	A self-learning trading agent develops a manipulative strategy
2. Remoteness and transnationality	The algorithm acts in several jurisdictions at once	Place and time of the crime; jurisdiction (Arts. 11, 13)	A phishing campaign run from abroad

Feature	Content	Element of the corpus delicti affected	Typical scenario
			against victims in Uzbekistan
3. Scale and automation	Mass, simultaneous execution with minimal tactical human involvement	Objective side; degree of social danger	Botnets, automated phishing, deepfakes reaching millions of users within seconds
4. High latency, digital traces and evidentiary difficulty	The black box and hidden layers prevent reconstruction of the decision	Proof of causation and guilt	Experts cannot explain why a model produced a harmful output
5. Limited foreseeability of consequences	A self-learning system performs actions its creator did not foresee	Subjective side: foreseeability (Arts. 22, 24)	Model behaviour drifts after deployment and causes unforeseen harm

Three of these features need comment. The autonomy of the means complicates the causal chain between the human act and the harmful result (Bakhteev, 2024). Transnationality is partly addressed by Article 11 of the Criminal Code, under which an act counts as committed in Uzbekistan if it began, ended or produced its criminal result there. Limited foreseeability brings Matthias's (2004) responsibility gap into the subjective side. When a self-learning algorithm does something its creator did not anticipate, the question becomes whether a human had the duty and the ability to foresee it. That is precisely the test of carelessness in Article 22 ("should have and could have foreseen") and of innocent infliction of harm in Article 24.

Systematised by the elements of the corpus delicti, AI-enabled crime looks as follows:

- **Object:** traditional social relations (property, life and health, public security) together with algorithmic information security and digital infrastructure.
- **Objective side:** automated execution and algorithmic causation.
- **Subject:** only a sane natural person who has reached the statutory age (Article 17).
- **Subjective side:** direct or indirect intent (Article 21) or negligence in the form of self-confidence or carelessness (Article 22).

3.5 Competing concepts of the legal nature of AI

Three concepts compete: AI as an instrument, as a target and as a subject of crime. Only the first is compatible with the principle of guilt.

AI as an instrument. This concept is supported by Hallevy's "perpetration-via-another" and "natural-probable-consequence" models (Hallevy, 2010, 2015) and by Laptev (2019), Begishev and Khisamova (2018), Bozarov (2021) and Voxidov (2025). However complex and autonomous, AI remains a material and software means of committing a crime. Uzbek law already provides a hook for this view: Article 28(2) of the Criminal Code defines a perpetrator as a person who commits a crime directly or by using other persons not subject to liability, "or other means".

AI as a target. Here the AI system is itself the object of the attack. Unlawful interference with algorithms — data poisoning, tampering with model parameters, adversarial attacks or algorithmic sabotage — makes AI the target of the offence (Caldwell et al., 2020; King et al., 2020).

AI as a subject ("electronic person"). Morhat (2017) and Hallevy's direct-liability model (Hallevy, 2010) allow autonomous algorithms a degree of legal capacity and of capacity to bear liability. In 2017 the European Parliament invited the Commission to consider a specific legal status of "electronic persons"

for the most sophisticated autonomous robots (European Parliament, 2017, para. 59(f)). Pagallo (2013), drawing on the Roman-law institution of the peculium, proposed a "digital peculium": a dedicated fund from which damage caused by robots would be compensated.

4. DISCUSSION

4.1 Why AI cannot be a subject of crime

Recognising AI as a subject of crime, or as an "electronic person", is unfounded and dangerous. The objections are both doctrinal and practical.

Bryson, Diamantis and Grant (2017) show that synthetic legal persons would open a legal lacuna that could be exploited to shield the humans behind them. The 2018 open letter to the European Commission, signed initially by 156 experts in AI, robotics, law and ethics and by 257 signatories by June 2018, made the same point: an electronic-person status would let manufacturers, programmers and owners disclaim responsibility for the systems they create (Robotics Open Letter, 2018). National scholars reach the same conclusion (Bozarov, 2021; Voxidov, 2025).

The doctrinal objection is decisive. AI has no consciousness, will, moral self-awareness or mental attitude to its conduct. The Uzbek Criminal Code makes liability depend on sanity, defined as awareness of the socially dangerous nature of one's actions and the ability to control them (Article 18), and on guilt in the form of intent or negligence (Article 20). Neither concept can be applied to an algorithm. Punishment, moreover, pursues correction and the prevention of new crimes (Article 42), aims that are meaningless for a machine. Abbott and Sarch (2019), after examining the case for punishing AI, conclude that more modest changes to existing law are preferable. Granting legal or criminal personhood to AI would hand large IT corporations and developers a way to escape liability and would reduce the corrective and restorative functions of criminal law to a formality.

The legal nature of AI is therefore that of a **high-risk autonomous software-and-material means** used under human control. The chain of criminal liability, built on the principle of guilt, must lead only to human beings: the developer who created the algorithm, the owner of the system, its operator or its user.

4.2 Closing the responsibility gap within existing law

The responsibility gap can largely be closed with the existing General Part of the Criminal Code by matching each scenario to the corresponding form of guilt (Table 3).

Table 3. Allocation of liability for harm caused by means of AI

Scenario	Liable person	Form of guilt or regime	Basis in the Criminal Code
AI used deliberately as an instrument (e.g. deepfake-based fraud)	User or operator	Direct or indirect intent	Arts. 21, 28(2) and the relevant Special Part offence
System designed or modified to cause harm	Developer, and the user where acting in concert	Intent; complicity	Arts. 21, 27–28
Risk foreseen but unjustifiably assumed not to materialise (e.g. known defects ignored)	Developer, owner or operator	Negligence: self-confidence	Art. 22
Harm not foreseen although it should and could have been (e.g.	Owner or operator	Negligence: carelessness	Art. 22

Scenario	Liable person	Form of guilt or regime	Basis in the Criminal Code
no monitoring or audit)			
Risk taken in development consistent with current scientific and technical knowledge, with necessary precautions	No one	Justified professional risk excludes criminality	Art. 41
Harm neither foreseeable nor avoidable, caused by an algorithmic defect	No criminal liability	Innocent infliction of harm; civil (product) liability	Art. 24; civil law

The model translates the author's position into the categories of the Code. Intentional use leads to liability for an intentional crime; indifference and negligence lead to liability for a negligent crime; and unexpected harm caused by a defect in the algorithm leads to strict civil liability for a defective product rather than to criminal punishment. Article 41 deserves particular attention. Its criteria for justified risk — consistency with current scientific and technical knowledge and experience, and the taking of necessary precautions — can serve as a benchmark for the standard of care expected of AI developers. A developer who fails to meet that benchmark loses the justification, and a risk knowingly involving a threat to human life is never justified.

4.3 Implications for law and practice

Three implications follow for Uzbekistan. First, guidance from the Plenum of the Supreme Court on qualifying AI-enabled offences would help investigators and courts establish causation and use expert evidence on model behaviour. Second, the list of aggravating circumstances in Article 56 is closed, and courts may not treat circumstances not listed there as aggravating. The use of AI can therefore aggravate punishment only where it fits an existing ground, such as commission "by a generally dangerous method" (Article 56(1)(e)). Whether the deliberate use of AI should become a separate aggravating circumstance deserves further study. Third, the negligence branch of the proposed definition presupposes clear duties of human oversight and algorithmic audit. These duties should be specified in sectoral regulation adopted under Law No. ZRU-1115.

4.4 Limitations

The study is doctrinal and does not analyse judicial practice, which remains scarce. Both the technology and its regulation are changing quickly, so the comparison of definitions reflects the state of law in 2026. Future research should test the proposed definition and liability model against investigative and judicial practice and compare them with the approaches of other post-Soviet jurisdictions.

5. CONCLUSION

AI is a means of crime, not its subject, and liability for AI-enabled harm must rest on the causal and culpable involvement of human beings. The analysis supports five conclusions.

1. The autonomy and self-learning capacity of AI create the "responsibility gap" and "black box" problems in criminal law, which call for doctrinal clarification of the concept and criminogenic features of AI-enabled crime.
2. International and national definitions describe AI as a set of technological solutions. In criminal law it is not an independent subject but a complex, autonomous and high-risk means of committing a crime.
3. A crime committed by means of AI is a socially dangerous act committed through the use of an AI

system capable of cognitive imitation and algorithmic decision-making, or through a failure to exercise proper control over such a system, and culpably causing harm.

4. Granting AI the status of an "electronic person" or subject of crime is legally and ethically unfounded and would leave the real culprits in the shadows. Criminal liability must fall only on human beings — developers, operators and users — on the basis of causal and culpable involvement.
5. These conclusions, together with the liability-allocation model built on Articles 9, 17, 20–24, 28 and 41 of the Criminal Code, provide a methodological basis for classifying AI-enabled crimes in criminal-law doctrine and for qualifying them correctly under the Criminal Code of Uzbekistan.

Further research should examine investigative and judicial practice, the role of expert evidence on algorithmic behaviour, and whether the deliberate use of AI should be recognised as an aggravating circumstance.

Declarations

Funding. [State the funding source and grant number, or: "This research received no external funding."]

Conflict of interest. The author declares no conflict of interest.

Data availability. Not applicable; no datasets were generated or analysed in this study.

Author contribution. The author is solely responsible for the conception, analysis and writing of the article.

Use of generative AI. [Disclose, as the journal's policy requires, any AI tools used for translation or language editing, and confirm that the author reviewed and takes responsibility for the content.]

REFERENCES

1. Abbott, R., & Sarch, A. (2019). Punishing artificial intelligence: Legal fiction or science fiction. UC Davis Law Review, 53(1), 323–384.
2. Bakhteev, D. V. (2024). Pravovoi status sistem iskusstvennogo intellekta i modeli differentsiatsii yuridicheskoi otvetstvennosti [Legal status of artificial intelligence systems and models for differentiating legal liability]. Lex Russica, 77(4), 9– [end page; verify title and DOI].
3. Begishev, I. R., & Khisamova, Z. I. (2018). Kriminologicheskie riski primeneniya iskusstvennogo intellekta [Criminological risks of using artificial intelligence]. Russian Journal of Criminology, 12(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775
4. Bozarov, S. S. (2021). Iskusstvennyi intellekt: vozmozhna li otvetstvennost' robotov? [Artificial intelligence: Is liability of robots possible?]. Yurisprudensiya, 1(5), 59–69. https://yurisprudensiya.tsul.uz/index.php/yurisprudensiya/article/view/253
5. Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. Artificial Intelligence and Law, 25(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9
6. Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. Big Data & Society, 3(1). https://doi.org/10.1177/2053951715622512
7. Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9, Article 14. https://doi.org/10.1186/s40163-020-00123-8
8. Criminal Code of the Republic of Uzbekistan. (1994, as amended 2026). Approved by Law No. 2012-XII of 22 September 1994. https://lex.uz/acts/111457
9. Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, & National Radio and Television Administration. (2023). Interim measures for the management of generative artificial intelligence services (effective 15 August 2023).
10. Decree of the President of the Republic of Uzbekistan No. PF-6079. (2020, October 5). On approval of the Strategy "Digital Uzbekistan-2030" and measures for its effective implementation. https://lex.uz
11. Department for Science, Innovation and Technology. (2023). A pro-innovation approach to

AI regulation (CP 815). HM Government.

12. European Parliament. (2017). Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Official Journal of the European Union, C 252, 239–257.
13. 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.
14. Hallevy, G. (2015). Liability for crimes involving artificial intelligence systems. Springer. https://doi.org/10.1007/978-3-319-10124-8
15. Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial intelligence and problems of ensuring cyber security. International Journal of Cyber Criminology, 13(2), 564–577.
16. King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. Science and Engineering Ethics, 26(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
17. Laptev, V. A. (2019). Ponyatie iskusstvennogo intellekta i yuridicheskaya otvetstvennost' za ego rabotu [Artificial intelligence and liability for its work]. Law. Journal of the Higher School of Economics, (2), 79–102. https://doi.org/10.17323/2072-8166.2019.2.79.102
18. Law of the Republic of Uzbekistan "On Informatization" No. 560-II. (2003, December 11; as amended 2026). https://lex.uz/acts/82956
19. Law of the Republic of Uzbekistan No. ZRU-1115. (2026, January 21). On amendments and additions to certain legislative acts of the Republic of Uzbekistan in connection with the regulation of relations arising from the use of artificial intelligence. https://lex.uz/docs/8011377
20. 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
21. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence (Home Office Research Report No. 75). Home Office.
22. Morhat, P. M. (2017). Iskusstvennyi intellekt: Pravovoi vzglyad [Artificial intelligence: A legal view]. Buki Vedi.
23. National Artificial Intelligence Initiative Act of 2020, Pub. L. No. 116-283, div. E, 15 U.S.C. § 9401 (2021).
24. OECD. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449; adopted 22 May 2019, amended 2023 and 2024). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
25. Pagallo, U. (2013). The laws of robots: Crimes, contracts, and torts. Springer. https://doi.org/10.1007/978-94-007-6564-1
26. Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
27. Ponkin, I. V., & Redkina, A. I. (2018). Iskusstvennyi intellekt s tochki zreniya prava [Artificial intelligence from the point of view of law]. RUDN Journal of Law, 22(1), 91–109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109
28. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). Official Journal of the European Union, L series. http://data.europa.eu/eli/reg/2024/1689/oj
29. Resolution of the President of the Republic of Uzbekistan No. PQ-4996. (2021, February 17). On measures to create conditions for the accelerated introduction of artificial intelligence technologies. https://lex.uz
30. Robotics Open Letter. (2018, April 5). Open letter to the European Commission: Artificial intelligence and robotics. http://www.robotics-openletter.eu/
31. Santoni de Sio, F., & Mecacci, G. (2021). Four responsibility gaps with artificial intelligence: Why they matter and how to address them. Philosophy & Technology, 34(4), 1057–1084. https://doi.org/10.1007/s13347-021-00450-x
32. UNESCO. (2021). Recommendation on the ethics of artificial intelligence (adopted 23 November 2021).

UNESCO.

33. Voxidov, F. M. (2025). Sun'iy intellekt va huquqiy javobgarlik [Artificial intelligence and legal liability]. International Journal of Scientific Researchers, 11(1), 560–564. https://doi.org/10.71337/inlibrary.uz.ijsr.107371