Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Халықаралық құқық / International law/ Международное право

Review article
IRSTI 10.81.71
https://doi.org/10.32523/2616-6844-2026-156-3-220-232

Comparative Legal Analysis of National and International Experience in Preventing Crimes Committed Using Artificial Intelligence Technologies

A. Kenzhebek[1]*, Sh. Ormanova[2], L. Bertovskii[3]

[1]Kazakh-American Free University, Ust-Kamenogorsk, Kazakhstan
[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Lomonosov Moscow State University, Moscow, Russia

(e-mal:[1]aziza_96.kenjebek@list.ru, [2]kmeyram@mail.ru, [3]bgl1980@yandex.ru)

Abstract. The rapid development of artificial intelligence (AI) creates new opportunities for public and economic development while increasing the risks of criminal misuse. The purpose of this study is to compare national and foreign approaches to preventing offenses in which AI is used as a substantial instrument and to identify mechanisms applicable to Kazakhstan. The research employs comparative legal, formal legal, systemic-structural, analysis and synthesis, and content-analysis methods. Its materials include Kazakhstan's legislation and strategic documents, international instruments, and approaches used in the European Union, the United States, the United Kingdom, China, and the Republic of Korea. The findings show that AI-enabled crime should be distinguished from cybercrime generally and that effective prevention increasingly combines risk-based regulation, technological audits, algorithmic transparency, data protection, institutional coordination, public-private cooperation, and specialized law-enforcement training. The study proposes a coordinated preventive model for Kazakhstan integrating criminal justice policy with cybersecurity, AI governance, data protection, and human-rights safeguards. Its practical value lies in recommendations on interagency coordination, technological capacity, preventive cooperation, and statistical recording of AI-enabled offenses.

Keywords: artificial intelligence, crime prevention, cybercrime, legal regulation, digital security, technological risks, Kazakhstan.

Received: 11.03.2026. Accepted: 25.09.2026. Available online: 30.09.2026.

***corresponding author**

А.С. Кенжебек[1]*, Ш.Ш. Орманова[2], Л.В. Бертовский[3]
[1]Қазақстан-Американдық еркін университеті, Өскемен, Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
[3]М.В. Ломоносов атындағы Мәскеу мемлекеттік университеті, Мәскеу, Ресей
(e-mail: [1]aziza_96.kenjebek@list.ru, [2]kmeyram@mail.ru, [3]bgl1980@yandex.ru)

Жасанды интеллект технологияларын қолдана отырып жасалатын қылмыстардың алдын алудың ұлттық және шетелдік тәжірибесін салыстырмалы-құқықтық талдау

Аңдатпа. Жасанды интеллект (ЖИ) технологияларының жедел дамуы экономиканы, мемлекеттік басқаруды және қоғамдық қатынастарды өзгертумен қатар, оларды қылмыстық мақсатта пайдалану тәуекелдерін де күшейтуде. Зерттеудің мақсаты – ЖИ тех-нологияларын елеулі құрал ретінде пайдалану арқылы жасалатын құқық бұзушылықтардың алдын алудың ұлттық және шетелдік тәсілдерін салыстыру және Қазақстан үшін бейімдеуге болатын құқықтық әрі институционалдық тетіктерді анықтау. Зерттеуде салыстырмалы-құқықтық, формальды-құқықтық, жүйелік-құрылымдық, талдау және синтез, сондай-ақ контент-талдау әдістері қолданылды. Материалдық база Қазақстан Республикасының заңнамасы мен стратегиялық құжаттарын, халықаралық ұйымдардың материалдарын және АҚШ, Еуропалық Одақ, Ұлыбритания, Қытай мен Оңтүстік Корея тәжірибесін қамтиды. Нәтижелер ЖИ көмегімен жасалатын қылмыстарды жалпы киберқылмыстан ажыратудың маңызын көрсетті: мұнда ЖИ қылмыстық әрекеттің ауқымына, жылдамдығына, жасырынуына немесе сенімділігіне елеулі әсер етеді. Шетелдік тәжірибеде тәуекелге негізделген реттеу, алгоритмдік ашықтық, технологиялық аудит, деректерді қорғау және мемлекеттік-жекеменшік ынтымақтастық кең қолданылады. Қазақстан үшін қылмыстық саясатты киберқауіпсіздікпен, деректерді қорғаумен, ЖИ-ді басқарумен және адам құқықтарының кепілдіктерімен ұштастыратын үйлестірілген алдын алу моделі ұсынылады. Зерттеудің практикалық маңызы құқық қорғау органдарының технологиялық және кадрлық әлеуетін арттыруға, ведомствоаралық үйлестіруді күшейтуге және ЖИ қолданылған құқық бұзушылықтарды статистикалық есепке алу тәсілдерін жетілдіруге арналған ұсыныстармен айқындалады.

Түйін сөздер: жасанды интеллект, қылмыстың алдын алу, киберқылмыс, құқықтық реттеу, цифрлық қауіпсіздік, технологиялық тәуекел, Қазақстан.

А.С. Кенжебек[1]*, Ш.Ш. Орманова[2], Л.В. Бертовский[3]
[1]Казахстанско-Американский свободный университет, Усть-Каменогорск, Казахстан
[2]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан
[3]Московский государственный университет имени М.В. Ломоносова, Москва, Россия
(e-mail: [1]aziza_96.kenjebek@list.ru, [2]kmeyram@mail.ru, [3]bgl1980@yandex.ru)

Сравнительно-правовой анализ национального и зарубежного опыта предотвращения преступлений, совершаемых с применением технологий искусственного интеллекта

Аннотация. Стремительное развитие технологий искусственного интеллекта (ИИ) трансформирует экономику, государственное управление и общественные отношения, одновре-

менно повышая риски их использования в преступных целях. Цель исследования состоит в сравнении национальных и зарубежных подходов к предупреждению правонарушений, в которых ИИ используется как существенный инструмент, и в определении правовых и институциональных механизмов, применимых в Казахстане. Использованы сравнительно-правовой, формально-юридический, системно-структурный методы, анализ и синтез, а также контент-анализ. Материалы исследования включают законодательство и стратегические документы Республики Казахстан, документы международных организаций и опыт США, Европейского Союза, Великобритании, Китая и Республики Корея. Результаты показывают необходимость разграничивать преступления с существенным использованием ИИ и киберпреступность в целом: в первом случае ИИ заметно влияет на масштаб, скорость, скрытность либо убедительность противоправного поведения. Зарубежная практика демонстрирует переход к риск-ориентированному регулированию, алгоритмической прозрачности, технологическому аудиту, защите данных и государственно-частному взаимодействию. Для Казахстана предлагается координированная профилактическая модель, объединяющая уголовную политику, кибербезопасность, защиту данных, управление ИИ и гарантии прав человека. Научная ценность исследования заключается в комплексном сопоставлении уголовно-правовых и превентивных механизмов с инструментами управления технологическими рисками. Практическое значение результатов состоит в предложениях по усилению межведомственной координации, технологического и кадрового потенциала правоохранительных органов, а также по совершенствованию статистического учета правонарушений, совершенных с использованием ИИ.

Ключевые слова: искусственный интеллект, предупреждение преступлений, киберпреступность, правовое регулирование, цифровая безопасность, технологические риски, Казахстан.

Introduction

Modern artificial intelligence (AI) technologies, including machine learning, neural networks, robotics, big-data analytics, and automated decision-making systems, are increasingly used across the economy and public administration. Their applications now extend to education, health care, finance, law enforcement, public services, and the digital economy [1].

The expansion of AI capabilities also creates new opportunities for criminal misuse. AI can increase the speed, scale, personalization, and concealment of unlawful conduct, thereby creating new challenges for criminology, criminal law, cybersecurity, and digital evidence.

Offenses in which AI plays a material role may display several features: technological complexity, a potential transboundary dimension, scalability, enhanced concealment, and difficulties in collecting, authenticating, and evaluating digital evidence [2, 5, 18].

A growing range of unlawful acts can be facilitated by AI, including the creation of deepfake video and audio, AI-assisted phishing, unlawful data processing, financial fraud, automated cyberattacks, and algorithmic manipulation of information. For the purposes of this study, AI-enabled crime is not treated as synonymous with cybercrime. Cybercrime is a broader category covering offenses committed against or through information systems and networks. AI-enabled crime refers to offenses in which AI capabilities materially contribute to the preparation,

commission, concealment, scaling, personalization, or evasion of detection. This distinction is important because the preventive response must address not only the digital channel of the offense but also the specific risks created by generative, predictive, or semi-autonomous AI functions. Deepfake-enabled fraud illustrates this problem: synthetic audio or video can be used to impersonate individuals, bypass conventional verification procedures, and accelerate the movement of unlawfully obtained funds through banking or cryptocurrency channels. Such practices complicate attribution, authentication of evidence, and the application of traditional investigative methods.

Because these threats may affect financial and information security, prevention requires a combination of technical and organizational measures. Deepfake-detection tools, multi-factor identity verification, transaction-risk monitoring, and multi-level authorization can reduce opportunities for fraud, while clear procedures for preserving and assessing digital evidence can strengthen subsequent investigation [2].

The emergence of AI-enabled offenses exposes limitations in prevention models designed for conventional forms of criminal activity. The key challenge is therefore to develop preventive mechanisms that can identify technology-related risks at an early stage without undermining fundamental rights, lawful innovation, or the admissibility and reliability of digital evidence.

The study of national and international approaches to AI-enabled offending is particularly relevant for Kazakhstan because technological change is developing faster than many conventional legal and institutional responses. Foreign regulatory models increasingly combine criminal-law measures with AI governance, cybersecurity, data protection, technical standards, and preventive oversight. The theoretical significance of the topic lies in distinguishing the broader category of cybercrime from offenses in which AI plays a material instrumental role and in identifying preventive mechanisms that can be adapted to Kazakhstan's legal and institutional context [15, 17].

In the European Union, AI regulation is structured around a risk-based model. Regulation (EU) 2024/1689 (the Artificial Intelligence Act) establishes differentiated obligations according to the level and type of risk posed by AI systems, including requirements concerning risk management, data governance, transparency, human oversight, and post-market monitoring for relevant high-risk systems [4]. These rules are not criminal-law provisions as such, but they are important for crime prevention because they introduce ex ante safeguards for the development and deployment of AI.

The United States does not rely on a single comprehensive AI statute equivalent to the EU AI Act. Instead, AI governance combines sector-specific law, agency enforcement, voluntary standards, and public-private risk-management mechanisms. A prominent example is the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0), which provides a voluntary framework for identifying, measuring, and managing AI risks throughout the AI lifecycle [21]. This decentralized model illustrates the role of technical standards and cooperation between public authorities and private actors in preventive AI governance.

In Asia, regulatory and law-enforcement approaches vary considerably and should not be treated as a single model. Recent research on China and Southeast Asia describes AI-supported fraud prevention through public-private cooperation, digital identity verification, behavioral biometrics, financial intelligence, and cross-border law-enforcement coordination [9]. These practices also raise questions concerning privacy, proportionality, transparency, and human oversight, which must be considered when adapting technological prevention measures to other jurisdictions.

In the Republic of Kazakhstan, prevention of AI-enabled crime is developing within a broader framework of criminal law, informatization, cybersecurity, personal-data protection, and digital transformation. The current framework does not establish a separate category of 'AI crime'; therefore, unlawful conduct involving AI is generally assessed under existing offense definitions depending on the protected interest, method, and consequences. At the strategic level, the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029, approved by Government Resolution No. 269 of 28 March 2023, provides for the development of cybersecurity, digital infrastructure, data governance, and technological capacity [19]. The Concept for the Development of Artificial Intelligence for 2024-2029, approved by Government Resolution No. 592 of 24 July 2024, further develops the national AI policy and links AI development with data governance, infrastructure, human capital, governance, and ethics [20]. These documents create an important policy basis for prevention, although specialized mechanisms for identifying, recording, and assessing offenses in which AI plays a substantial role still require further development.

The legal framework has been further developed by the Law of the Republic of Kazakhstan «On Artificial Intelligence» dated 17 November 2025 No. 230-VIII, which entered into force on 18 January 2026. The Law establishes a dedicated framework for the creation, deployment and use of AI systems and expressly links their operation with human well-being, autonomy, accountability, data protection, safety and risk management. In particular, Articles 9–11 recognize the priority of human rights and freedom of decision-making, require protection of personal data and confidentiality, and oblige owners and operators to manage risks and take measures against potential threats. Article 17 differentiates AI systems by risk level and prohibits specified harmful practices, including manipulative uses that undermine informed choice and certain discriminatory biometric classification. Article 20 provides for AI-specific audit elements, while Article 21 requires users to be informed when goods, works or services are produced or provided using AI and requires synthetic AI outputs to be marked in machine-readable form and accompanied by a perceptible warning [22]. These statutory requirements make the prevention of AI-enabled offenses an immediate legal and institutional issue for Kazakhstan: they provide preventive safeguards relevant to fraud, deepfake impersonation, unlawful data use and algorithmic manipulation, while also raising practical questions of compliance monitoring, audit, risk classification and coordination with law-enforcement bodies.

Literature Review

Kazakhstani legal scholarship increasingly addresses the regulation of artificial intelligence, its use in judicial and law-enforcement activities, and the legal risks associated with emerging technologies. This literature treats AI not merely as a technical instrument but as a factor capable of affecting legal relations, criminal-law qualification, evidence, institutional design, and the protection of fundamental rights.

Galiakbarova examines foreign and Kazakhstani approaches to the legal regulation of artificial intelligence from a comparative legal perspective. The study analyzes regulatory approaches developed in different jurisdictions and considers the possibilities of adapting relevant international practices to the national legal system of Kazakhstan. An important aspect of the research is its attention to the gap between the rapid development of AI technologies and the capacity of existing legislation to respond to emerging technological challenges. From

this perspective, the prevention of offenses committed through the use of artificial intelligence should not be limited exclusively to criminal law measures but should also be integrated with mechanisms for personal data protection, algorithmic transparency, identification of responsible actors, and preliminary assessment of technological risks [16].

The criminal-law dimension is examined more specifically by Fazilov and Amanzholova. Using Uzbekistan and Kazakhstan as comparative cases, the authors analyze criminal liability for offenses committed with AI technologies and the broader legal regulation of AI. Their study highlights difficulties in applying conventional criminal-law concepts to technologically mediated conduct and emphasizes the need to adapt criminal-law responses consistently with international standards and human-rights principles [17]. Dulatbekov and Bachurin, by contrast, focus on the use of AI tools within Kazakhstan's judicial and law-enforcement system and emphasize the need to define the scope, objectives, safeguards, and institutional conditions of such use [16].

A comparison of the reviewed studies shows three interconnected research directions in Kazakhstan. The first concerns general AI regulation and the adaptation of international regulatory experience to national legislation. The second addresses the criminal-law qualification of conduct committed through AI technologies. The third examines the legal foundations for using AI tools in judicial and law-enforcement activities. However, the literature still pays insufficient attention to a comprehensive prevention model that combines these directions. In particular, gaps remain regarding preventive monitoring, early identification of algorithmic and technological risks, standardized recording of AI-enabled offenses, cooperation between law-enforcement agencies and technology companies, and adaptation of international prevention practices to Kazakhstan's institutional context.

The reviewed scholarship therefore provides the theoretical basis for the present study but does not fully resolve the problem addressed here. The scientific contribution of this article lies in linking criminal-law analysis with AI governance and crime-prevention policy through a comparative assessment of Kazakhstan and selected foreign jurisdictions. The study focuses specifically on mechanisms that operate before or at the early stages of offending - risk assessment, monitoring, technical safeguards, institutional coordination, data collection, and public-private cooperation - rather than treating AI-related crime solely as a matter of post-offense qualification and punishment.

On this basis, the study proceeds from the proposition that an effective model for preventing AI-enabled crime should combine legal regulation, early risk identification, technical controls, institutional coordination, and public cybersecurity awareness. The analysis is intended to determine which elements of foreign practice can be adapted to Kazakhstan without mechanically transferring regulatory models developed in different legal and institutional environments.

Research Methods and Materials

The purpose of this research is to examine national and international approaches to preventing offenses committed with the use of artificial intelligence and to identify mechanisms that may be adapted to Kazakhstan. The research has an interdisciplinary character, integrating jurisprudence, criminology, information security, and information-technology perspectives.

The study uses comparative legal, formal legal, systemic-structural, analysis and synthesis, and content-analysis methods. The comparative legal method is used to identify differences between Kazakhstan and selected foreign approaches; formal legal analysis is applied to legislation and

strategic documents; the systemic-structural method is used to model prevention as a multilevel system; and content analysis is applied to materials of international organizations and academic literature. The results are synthesized to formulate legal and practical recommendations.

The empirical and theoretical materials include the Criminal Code of the Republic of Kazakhstan; the Law 'On Informatization'; the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029; the Concept for the Development of Artificial Intelligence for 2024-2029; the EU Artificial Intelligence Act; the NIST AI Risk Management Framework; Council of Europe guidance; and academic studies concerning AI-enabled offending, cybercrime, deepfakes, digital evidence, and AI governance. The study is limited by the absence of a separate official statistical category for AI-enabled crime in Kazakhstan and by differences in terminology and data availability across jurisdictions. These limitations are taken into account when drawing comparative conclusions.

Results and Discussion

First, analysis and synthesis identify the principal categories of unlawful conduct in which AI can play a material instrumental role. These include AI-assisted cyberattacks, financial fraud, deepfake-enabled impersonation and manipulation, unlawful processing or profiling of personal data, and automated information attacks [6, 14]. Common features may include scalability, personalization, automation, concealment, and rapid adaptation. Deepfake and online-fraud research demonstrates how synthetic media and social-engineering techniques can complicate authentication, qualification, evidence collection, and cross-border enforcement [2, 5, 18].

Accordingly, prevention should focus not only on punishment after an offense has occurred but also on reducing opportunities for misuse, strengthening authentication and monitoring, and improving the capacity to detect synthetic or automated criminal activity at an early stage.

Table 1. Main Types of Crimes Committed Using Artificial Intelligence

Type of Crime	AI Technologies Involved	Key Risks
Cybercrime	Machine learning, automated scripts	Mass attacks, anonymity, scalability
Financial fraud	AI-driven bots, data analytics	Rapid loss of funds, low detectability
Deepfake manipulation	Generative AI, neural networks	Reputational damage, political instability
Data misuse	Predictive analytics, AI profiling	Privacy violations, discrimination
Information attacks	Natural language generation	Social polarization, misinformation

The comparative analysis reveals important differences between Kazakhstan and selected foreign approaches. The European Union has adopted a binding risk-based AI regulatory framework, while the United States relies more heavily on sector-specific regulation, agency practice, voluntary risk-management standards, and public-private cooperation. Kazakhstan has adopted strategic documents on digital transformation, cybersecurity, and AI development, but specialized procedures for identifying and recording the material use of AI in offenses remain less developed [4, 19-21].

Risk-based AI governance shifts part of the regulatory focus from ex post response to ex ante risk management. Depending on the jurisdiction and the type of AI system, preventive mechanisms may include risk assessment, data-governance requirements, transparency obligations, human oversight, testing, monitoring, and technical safeguards. The EU AI Act provides a binding example of this approach, whereas the U.S. NIST AI RMF offers a voluntary framework organized around the functions Govern, Map, Measure, and Manage [4, 21].

Table 2. Comparative Characteristics of AI Crime Prevention Policies

Criterion	Kazakhstan	European Union / USA
Legal framework	General cybercrime norms	Specialized AI regulations
Risk assessment	Limited	Mandatory and systematic
Monitoring of AI systems	Fragmented	Continuous oversight
Ethical standards	Not clearly defined	Codified and enforceable
Private sector involvement	Insufficient	Institutionalized

Formal legal analysis shows that Kazakhstan's criminal and information-security legislation can apply to many unlawful acts committed with AI, but it does not generally distinguish offenses according to whether AI materially facilitated their commission [10, 11]. This does not necessarily create a gap in criminalization: existing offense definitions may remain applicable. The preventive difficulty is different - authorities may lack standardized criteria for identifying the role of AI, recording such cases, assessing technology-specific risks, and selecting appropriate technical safeguards. A clearer distinction between ordinary cybercrime and AI-enabled offending would therefore improve prevention, statistics, evidence assessment, and institutional coordination without automatically requiring a separate offense for every use of AI.

The Law «On Artificial Intelligence» adds an important sector-specific layer to this framework. Its risk-based classification and continuous risk-management approach can support earlier identification of systems and practices that may facilitate unlawful conduct; its requirements concerning data protection, security, transparency and audit are also relevant to preserving trustworthy digital evidence and reducing opportunities for abuse. At the same time, the Law does not itself create a separate criminal offense category called «AI crime» or replace the Criminal Code. Accordingly, the preventive task is to coordinate the Law's governance and compliance mechanisms with criminal-law qualification, incident reporting and investigation, and to develop consistent criteria for recording when AI has materially contributed to an offense [22].

Foreign AI regulation also should not be equated directly with criminal-law regulation. Instruments such as the EU risk-based model primarily govern the development and deployment of AI systems, but they may have preventive relevance where they require risk management, transparency, data governance, human oversight, or post-deployment monitoring. For Kazakhstan, the comparative value of these mechanisms lies in their ex ante orientation. Adaptation should therefore focus on compatible safeguards and institutional procedures rather than mechanical transplantation of foreign rules.

The systemic-structural method makes it possible to conceptualize the prevention of AI-enabled crime as a multilevel system rather than as the exclusive responsibility of law-enforcement agencies. Effective prevention requires coordinated action at the legal,

technological, institutional, and social levels, including clear rules, technical safeguards, interagency cooperation, professional competence, and public digital literacy [7].

Table 3. Levels of AI Crime Prevention

Level	Key Actors	Preventive Functions
Legal	Legislators, regulators	Norm-setting, liability
Technological	IT companies, developers	Secure design, monitoring
Institutional	Law enforcement, courts	Detection, investigation
Social	Educational institutions, media	Awareness, digital literacy

Comparative materials indicate that prevention is more effective when public authorities, law-enforcement agencies, technology companies, academic institutions, and civil society have established channels for cooperation. Such cooperation may include information exchange, joint risk assessment, technical assistance, incident reporting, and development of tools for detecting AI-enabled fraud or synthetic content. In Kazakhstan, relevant interaction exists within broader digitalization and cybersecurity initiatives, but a specialized and standardized coordination mechanism for AI-enabled crime prevention is not yet clearly established. This limits early detection, consistent data collection, and rapid technical response [13].

International and European guidance emphasizes that measures addressing AI-related risks should remain compatible with human rights, data protection, due process, and responsible innovation. The Council of Europe's Guidelines on Artificial Intelligence and Data Protection, for example, place human dignity, privacy, data protection, risk mitigation, and meaningful control at the center of AI governance [3,8]. The preventive objective is therefore not to restrict AI as such, but to reduce foreseeable misuse through proportionate safeguards.

The analysis supports a comprehensive prevention model combining legal, institutional, technological, and educational measures. For Kazakhstan, priorities include clearer procedures for identifying the material role of AI in offenses, stronger technical and human capacity in law-enforcement bodies, structured cooperation with technology providers, and continued improvement of public digital literacy. These measures should complement, rather than automatically replace, existing criminal-law provisions.

The prevention of AI-enabled offending therefore extends beyond criminal law. It also concerns cybersecurity, data protection, national security, digital governance, evidentiary reliability, and the protection of fundamental rights.

Adapting international experience while taking national specificities into account and forming an integrated prevention model is therefore of strategic importance for the Republic of Kazakhstan.

Comparative analysis shows that foreign approaches increasingly use ex ante risk-management mechanisms alongside conventional criminal-law responses. Kazakhstan has already established strategic frameworks for digital transformation, cybersecurity, and AI development [19, 20]. The next step is not simply to reproduce foreign regulation, but to develop proportionate national procedures for risk assessment, institutional coordination, technical safeguards, and reliable recording of AI-enabled conduct.

Available open-source and expert materials indicate growth in digital fraud, synthetic-content abuse, and other technology-enabled offenses; however, these trends should not be

presented as official statistics on 'AI crime.' In Kazakhstan, offenses involving AI are not recorded as a separate statistical category. Consequently, the scale and dynamics of AI-enabled offending cannot currently be measured with sufficient precision. Establishing standardized indicators for recording the material use of AI in reported and investigated offenses would improve evidence-based prevention and policy evaluation.

Taken together, the findings indicate that effective prevention requires a multifaceted state policy. Priorities include maintaining an up-to-date legal framework, strengthening the technical infrastructure and specialist competence of law-enforcement agencies, improving mechanisms for digital-evidence authentication, expanding public digital literacy, and establishing structured cooperation with the private sector and civil society.

Conclusion

The study shows that offenses committed with the material use of artificial intelligence constitute a developing prevention challenge at the intersection of criminal law, cybersecurity, data governance, and human rights. Their distinctive risks arise not simply from the use of digital technologies but from AI capabilities that can automate, personalize, scale, or conceal unlawful conduct. This makes it necessary to distinguish AI-enabled offending from cybercrime in general while avoiding the assumption that every offense involving AI requires a new criminal-law provision.

The comparative analysis demonstrates a broader international shift toward preventive and risk-based mechanisms, including ex ante risk assessment, transparency requirements, technical audits, monitoring, data-governance safeguards, and institutional cooperation. These instruments complement rather than replace criminal-law and criminal-procedural measures. Their relevance for Kazakhstan lies in strengthening prevention before harm occurs and in improving the detection and evidentiary assessment of technology-enabled offenses.

Kazakhstan already has a strategic basis for this development in the Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029 and the Concept for the Development of Artificial Intelligence for 2024-2029. At the same time, the national system would benefit from more specific procedures for identifying the material use of AI in offenses, collecting comparable statistics, assessing technology-specific risks, and coordinating law-enforcement agencies with regulators and technology companies.

Crime prevention in Kazakhstan therefore requires a coordinated approach that cannot be reduced to law-enforcement measures alone. Sustainable prevention should combine legal regulation, cybersecurity tools, reliable data collection, specialized training, public-private cooperation, digital literacy, and safeguards for fundamental rights. Particular attention should be paid to authentication technologies, deepfake detection, preservation and verification of digital evidence, and mechanisms for rapid information exchange between competent authorities and technology providers [12].

The absence of separate official statistics on offenses in which AI plays a substantial role remains a methodological and policy limitation. Introducing a standardized statistical marker for AI-enabled conduct, without creating an overly broad legal category, would make it possible to assess trends, identify recurring methods of misuse, and evaluate the effectiveness of preventive measures.

The principal recommendation is to integrate criminal-justice policy with national cybersecurity, AI governance, data protection, and human-rights safeguards. International experience should be adapted to Kazakhstan's legal and institutional context rather than copied mechanically. A consistent prevention model based on proportionate risk assessment, institutional coordination, technical capacity, reliable data, and public awareness can strengthen both digital security and public trust in the responsible use of artificial intelligence.

The contribution of the authors

A. Kenzhebek: Conceptualization, methodology, investigation, formal analysis, data curation, and writing – original draft preparation. The author developed the research concept, analyzed the national legislation of the Republic of Kazakhstan, conducted the comparative analysis, and formulated recommendations for preventing crimes committed using artificial intelligence technologies.

Sh. Ormanova: Legal analysis, investigation, validation, and writing – review and editing. The author contributed to the comparative legal assessment of national and international legislation, examined the criminal-law aspects of AI-enabled offenses, and reviewed the legal accuracy and academic content of the manuscript.

L. Bertovskii: Methodology, formal analysis, validation, and writing – review and editing. The author contributed to the criminological and forensic analysis of AI-enabled crimes, examined issues related to digital evidence, identification, and investigation of offenses, and contributed to the development of preventive recommendations.

All authors contributed to the discussion of the research findings, critically reviewed the manuscript, and approved the final version for publication.

Conflict of interest

There are no conflicts of interest to disclose.

Funding

This study has not received funding.

References

1. Russell, S. and Norvig, P. (2021) Artificial Intelligence: A Modern Approach. 4th edn. Pearson. Available at: https://www.pearson.com/en-us/subject-catalog/p/artificial-intelligence-a-modern-approach /P200000003500 (Accessed: 30 October 2025).

2. Smanova, A.B., Muratova, A.Zh. and Zhumagulova, Sh.R. (2025) 'Deepfake technologies and social engineering in online fraud forms, mechanisms, and legal challenges', BULLETIN of L.N. Gumilyov Eurasian National University Law Series, 152(3), pp. 188-211. doi: https://doi.org/10.32523/2616-6844-2025-152-3-188-211.

3. Floridi, L. and Cowls, J. (2019) 'A unified framework of five principles for AI in society', Harvard Data Science Review, 1(1). doi: https://doi.org/10.1162/99608f92.8cd550d1.

4. European Parliament and Council of the European Union (2024) Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, 12 July 2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Accessed: 30 October 2025).

5. Beaver, K.M. (2025) 'International and domestic legal frameworks on online fraud and deepfake technologies: a comparative criminal law analysis', BULLETIN of L.N. Gumilyov Eurasian National University Law Series, 152(3), pp. 212-228. doi: https://doi.org/10.32523/2616-6844-2025-152-3-212-228.

6. OECD (2021) OECD Business and Finance Outlook 2021: AI in Business and Finance. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/oecd-business-and-finance-outlook-2021_ba682899-en.html (Accessed: 29 October 2025).

7. United Nations Office on Drugs and Crime (UNODC) (2025) The use of artificial intelligence in the judiciary and prosecution services, CAC/COSP/WG.4/2025/4. Vienna: United Nations. Available at: https://track.unodc.org/uploads/documents/UNCAC/WorkingGroups/workinggroup4/2025-June-17-20/BD-Judicial_Integrity/CAC-COSP-WG.4-2025-4_E.pdf (Accessed: 28 October 2025).

8. Council of Europe (2019) Guidelines on Artificial Intelligence and Data Protection, T-PD(2019)01. Strasbourg: Council of Europe. Available at: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (Accessed: 12 November 2025).

9. Sun, J., Gu, S. and Su, R. (2026) 'AI-Empowered Responsive Regulation for Preventing Future Crimes: An Empirical Inquiry into the Regulatory Pyramid to Combat Future Crimes in China and Southeast Asia', Asian Journal of Criminology, 21, article 8. doi: https://doi.org/10.1007/s11417-025-09477-x.

10. Republic of Kazakhstan (2014) Criminal Code of the Republic of Kazakhstan, Code No. 226-V of 3 July 2014. Available at: https://adilet.zan.kz/eng/docs/K1400000226 (Accessed: 25 September 2026).

11. Republic of Kazakhstan (2015) Law of the Republic of Kazakhstan 'On Informatization', No. 418-V of 24 November 2015. Available at: https://adilet.zan.kz/rus/docs/Z1500000418 (Accessed: 15 November 2025).

12. Doszhanova, A.B. and Begaliyev, Ye.N. (2025) 'Information and communication technologies of the Smart City in the system of identification: forensic aspect', Bulletin of the Karaganda University. Law Series, 30(2/118), pp. 125-133. doi: https://doi.org/10.31489/2025L2/125-133.

13. Satbayeva, A.M., Alimbetova, A.R. and Beissenbayeva, M.T. (2024) 'Cybercrime challenges: experience of international cooperation', Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, 3(78), pp. 211-221. doi: https://doi.org/10.52026/2788-5291_2024_78_3_211.

14. Gillespie, T. (2018) Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. New Haven: Yale University Press. Available at: https://yalebooks.yale.edu/book/9780300235029/custodians-of-the-internet/ (Accessed: 17 November 2025).

15. Galiakbarova, G.G. (2024) 'Some features of legal regulation of artificial intelligence: foreign and national experience', Journal of Actual Problems of Jurisprudence, 112(4), pp. 4-12. doi: https://doi.org/10.26577/JAPJ2024.112.i4.a1.

16. Dulatbekov, N.O. and Bachurin, S.N. (2024) 'Theoretical prerequisites for the use of artificial intelligence tools in the implementation of a three-tier model of judicial and law enforcement activities in the Republic of Kazakhstan', Bulletin of the Karaganda University. Law Series, 29(3/115), pp. 59-69. doi: https://doi.org/10.31489/2024l3/59-69.

17. Fazilov, F.M. and Amanzholova, B.A. (2025) 'Artificial intelligence and criminal law in Uzbekistan and Kazakhstan', Universum: Economics and Law, 10(132). Available at: https://7universum.com/en/economy/archive/item/20846 (Accessed: 4 November 2025).

18. Chesney, R. and Citron, D.K. (2019) 'Deep fakes: a looming challenge for privacy, democracy, and national security', California Law Review, 107(6), pp. 1753-1820. doi: https://doi.org/10.15779/Z38RV0D15J.

19. Government of the Republic of Kazakhstan (2023) Concept of Digital Transformation, Development of the Information and Communication Technology Industry and Cybersecurity for 2023-2029, approved

by Resolution No. 269 of 28 March 2023. Available at: https://adilet.zan.kz/rus/docs/P2300000269 (Accessed: 28 October 2025).

20. Government of the Republic of Kazakhstan (2024) Concept for the Development of Artificial Intelligence for 2024-2029, approved by Resolution No. 592 of 24 July 2024. Available at: https://adilet.zan.kz/rus/docs/P2400000592 (Accessed: 15 November 2025).

21. Tabassi, E. (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology. doi: https://doi.org/10.6028/NIST.AI.100-1.

22. Republic of Kazakhstan (2025) Law of the Republic of Kazakhstan 'On Artificial Intelligence', No. 230-VIII of 17 November 2025. Available at: https://adilet.zan.kz/eng/docs/Z2500000230 (Accessed: 20 November 2025).

Information about the authors:

Kenzhebek A. **–** corresponding author, PhD student at the Kazakh-American Free University, 76 M. Gorky Street, 070007, Ust-Kamenogorsk, Kazakhstan

Ormanova Sh. **–** Candidate of Legal Sciences, Associate Professor, Department of Constitutional and Civil Law, Faculty of Law, L.N. Gumilyov Eurasian National University, 2 Satpaeva Str., 010008, Astana, Kazakhstan

Bertovskii L. **–** Doctor of Law, Professor, Department of Criminalistics, Faculty of Law, Lomonosov Moscow State University, Leninskie Gory Street, 1, 4th educational building, 11999, Moscow, Russian Federation

Кенжебек А.С. **–** хат-хабар авторы, Қазақстан-Американдық еркін университетінің докторанты, М. Горький көшесі, 76, 070004, Өскемен, Қазақстан

Орманова Ш.Ш. **–** заң ғылымдарының кандидаты, Конституциялық және азаматтық құқық кафедрасының қауымдастырылған профессоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сатпаев көшесі 2, 010008, Астана, Қазақстан

Бертовский Л.В. – заң ғылымдарының докторы, Заң факультетінің криминалистика кафедрасының профессоры, М.В. Ломоносов атындағы Мәскеу мемлекеттік университеті, Ленин таулары көшесі 1-үй, 4-ші оқу корпусы, 11999, Мәскеу, Ресей Федерациясы

Кенжебек А.С. **–** автор для корреспонденции, докторант Казахстанско-Американского свободного университета, улица М. Горького, 76, 070004, Усть-Каменогорск, Казахстан

Орманова Ш.Ш. – кандидат юридических наук, доцент кафедры Конституционного и гражданского права, Евразийский национальный университет имени Л.Н. Гумилева, ул. Сатпаева, 2, 010008, Астана, Казахстан

Бертовский Л.В. – доктор юридических наук, профессор кафедры криминалистики, юридический факультет, Московский государственный университет имени М.В. Ломоносова, улица Ленинские горы, д. 1, 4-й учебный корпус, 11999, Москва, Российская Федерация



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (https://creativecommons.org/licenses/by-nc/4.0/).