**ҚЫЛМЫСТЫҚ ҚҰҚЫҚ ЖӘНЕ ПРОЦЕСС.
КРИМИНОЛОГИЯ. КРИМИНАЛИСТИКА
УГОЛОВНОЕ ПРАВО И ПРОЦЕСС.
КРИМИНОЛОГИЯ. КРИМИНАЛИСТИКА
CRIMINAL LAW AND PROCESS. CRIMINOLOGY. FORENSICS**

IRSTI 10.79.41
UDC 343.98:004.8
https://doi.org/10.51889/2959-6181.2026.84.2.008

Apparova S.Z[1]. , *Bizhanova A.R.[1]**

[1]Abai Kazakh National Pedagogical University
*(e-mail: sabina.apparova@mail.ru, *Aike_74@mail.ru)*

THE USE OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF CRIMES: LEGAL RISKS AND PROSPECTS IN THE REPUBLIC OF KAZAKHSTAN

Abstract

The article examines the legal and practical aspects of the use of artificial intelligence technologies in the investigation of criminal offenses. The relevance of the topic is due to the digitalization of public relations and the increasing complexity of the ways of committing crimes, which requires the introduction of modern technological solutions into the activities of law enforcement agencies. The purpose of the study is to analyze the possibilities of using artificial intelligence in criminal proceedings, identify related legal risks and identify prospects for improving the legislation of the Republic of Kazakhstan.

The paper uses methods of legislative analysis, comparative legal research, systematic and formal legal analysis. The possibilities of using artificial intelligence in processing large amounts of data, analyzing video surveillance materials, identifying digital traces of criminal activity and investigating cybercrimes are being considered. The article examines the foreign experience of introducing intelligent systems into the activities of law enforcement agencies, as well as the current state of legal regulation in the Republic of Kazakhstan.

The results of the study show that the use of artificial intelligence contributes to improving the effectiveness of investigations through automated information analysis, establishing relationships between participants in criminal activity and improving mechanisms to counter cybercrime. At the same time, problems of legal regulation have been identified related to the lack of a clear procedural status of the results of the work of intelligent systems, issues of the admissibility of digital evidence, the distribution of responsibility for algorithmic errors and ensuring the protection of human rights.

It is concluded that at the present stage, the results of the functioning of artificial intelligence systems cannot be considered as independent evidence in criminal cases and should be used exclusively as an auxiliary tool with mandatory human control. The necessity of further improving the legislation of the Republic of Kazakhstan in terms of determining the legal status of digital evidence, introducing mechanisms for independent audit of algorithmic systems and strengthening guarantees for the protection of citizens' rights and freedoms when using artificial intelligence technologies in law enforcement is substantiated.

Key words: artificial intelligence, criminal investigation, digitalization, Legal Regulation, cybercrime, digital evidence, algorithm, personal data.

Аппарова С.З.[1], Бижанова А.Р. [1]
[1]Абай атындағы Қазақ Ұлттық педагогикалық университеті

ҚЫЛМЫСТАРДЫ ТЕРГЕУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНУ: ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ҚҰҚЫҚТЫҚ ТӘУЕКЕЛДЕР МЕН ПЕРСПЕКТИВАЛАР

Аңдатпа

Мақалада қылмыстық құқық бұзушылықтарды тергеу кезінде жасанды интеллект технологияларын қолданудың құқықтық және практикалық аспектілері зерттелген. Тақырыптың өзектілігі қоғамдық қатынастарды цифрландыруға және құқық қорғау органдарының қызметіне заманауи технологиялық шешімдерді енгізуді талап ететін қылмыс жасау тәсілдерінің күрделенуіне байланысты. Зерттеудің мақсаты қылмыстық сот ісін жүргізуде жасанды интеллектті пайдалану мүмкіндіктерін талдау, осыған байланысты құқықтық тәуекелдерді анықтау және Қазақстан Республикасының заңнамасын жетілдіру перспективаларын айқындау болып табылады.

Жұмыста заңнаманы талдау, салыстырмалы-құқықтық зерттеу, жүйелік және ресми-құқықтық талдау әдістері қолданылды. Деректердің үлкен массивтерін өңдеу, бейнебақылау материалдарын талдау, қылмыстық әрекеттің сандық іздерін анықтау және киберқылмыстарды тергеу кезінде жасанды интеллектті қолдану мүмкіндіктері қарастырылады. Құқық қорғау органдарының қызметіне зияткерлік жүйелерді енгізудің шетелдік тәжірибесі, сондай-ақ Қазақстан Республикасындағы құқықтық реттеудің қазіргі жағдайы зерттелді.

Зерттеу нәтижелері жасанды интеллектті пайдалану ақпаратты автоматтандырылған талдау, қылмыстық әрекетке қатысушылар арасында байланыс орнату және киберқылмысқа қарсы тетіктерді жетілдіру арқылы тергеу тиімділігін арттыруға ықпал ететінін көрсетеді. Сонымен қатар, зияткерлік жүйелер жұмысының нәтижелерінің нақты іс жүргізу мәртебесінің болмауымен, цифрлық дәлелдемелерге жол беру, алгоритмдік қателіктер үшін жауапкершілікті бөлу және адам құқықтарын қорғауды қамтамасыз ету мәселелерімен байланысты құқықтық реттеу мәселелері анықталды.

Қазіргі кезеңде жасанды интеллект жүйелерінің жұмыс істеу нәтижелері қылмыстық істер бойынша дербес дәлелдемелер ретінде қарастырыла алмайды және тек адам тарапынан міндетті бақылау кезінде көмекші құрал ретінде пайдаланылуы керек деген қорытындыға келді. Цифрлық дәлелдемелердің құқықтық мәртебесін айқындау, алгоритмдік жүйелердің тәуелсіз аудит тетіктерін енгізу және құқық қорғау қызметінде жасанды интеллект технологияларын пайдалану кезінде азаматтардың құқықтары мен бостандықтарын қорғау кепілдіктерін күшейту бөлігінде Қазақстан Республикасының заңнамасын одан әрі жетілдіру қажеттілігі негізделген.

Түйін сөздер: жасанды интеллект, қылмыстық істерді тергеп-тексеру, цифрландыру, құқықтық реттеу, киберқылмыс, цифрлық дәлелдеме, алгоритм, дербес деректер.

С.З. Аппарова [1], А.Р. Бижанова [1]
[1]Казахский Национальный педагогический университет имени Абая

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ: ПРАВОВЫЕ РИСКИ И ПЕРСПЕКТИВЫ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

В статье исследуются правовые и практические аспекты применения технологий искусственного интеллекта при расследовании уголовных правонарушений. Актуальность темы обусловлена цифровизацией общественных отношений и усложнением способов

совершения преступлений, что требует внедрения современных технологических решений в деятельность правоохранительных органов. Целью исследования является анализ возможностей использования искусственного интеллекта в уголовном судопроизводстве, выявление связанных с этим правовых рисков и определение перспектив совершенствования законодательства Республики Казахстан.

В работе использованы методы анализа законодательства, сравнительно-правового исследования, системного и формально-юридического анализа. Рассматриваются возможности применения искусственного интеллекта при обработке больших массивов данных, анализе материалов видеонаблюдения, выявлении цифровых следов преступной деятельности и расследовании киберпреступлений. Исследован зарубежный опыт внедрения интеллектуальных систем в деятельность правоохранительных органов, а также современное состояние правового регулирования в Республике Казахстан.

Результаты исследования показывают, что использование искусственного интеллекта способствует повышению эффективности расследования за счет автоматизированного анализа информации, установления взаимосвязей между участниками преступной деятельности и совершенствования механизмов противодействия киберпреступности. Вместе с тем выявлены проблемы правового регулирования, связанные с отсутствием четкого процессуального статуса результатов работы интеллектуальных систем, вопросами допустимости цифровых доказательств, распределения ответственности за алгоритмические ошибки и обеспечения защиты прав человека.

Сделан вывод о том, что на современном этапе результаты функционирования систем искусственного интеллекта не могут рассматриваться в качестве самостоятельных доказательств по уголовным делам и должны использоваться исключительно как вспомогательный инструмент при обязательном контроле со стороны человека. Обоснована необходимость дальнейшего совершенствования законодательства Республики Казахстан в части определения правового статуса цифровых доказательств, внедрения механизмов независимого аудита алгоритмических систем и усиления гарантий защиты прав и свобод граждан при использовании технологий искусственного интеллекта в правоохранительной деятельности.

Ключевые слова: искусственный интеллект, уголовное расследование, цифровизация, правовое регулирование, киберпреступность, цифровые доказательства, алгоритм, персональные данные.

Introduction

At the present stage, digital technologies are rapidly developing worldwide and have a significant impact on all spheres of society. The digitalization of social relations is transforming the content and organization of public administration, the economy, education, healthcare, and law enforcement activities. These changes also affect the law enforcement system, requiring it to adapt to new demands. Whereas in the past most crimes were committed using traditional methods, today many offenses are closely connected with the internet environment, electronic systems, and digital technologies. In this regard, traditional methods of criminal investigation do not always fully meet modern requirements.

In recent years, the use of artificial intelligence technologies in the activities of law enforcement agencies has become widespread in international practice. Artificial intelligence makes it possible to quickly analyze large volumes of data, predict potential criminal risks, process video surveillance materials, identify faces, detect digital evidence, and improve analytical decision-making processes during investigations. Such technologies not only increase the efficiency of investigations but also enable the optimal use of law enforcement resources.

In the Republic of Kazakhstan, the digitalization process is also being implemented step by step. Within the framework of the «Digital Kazakhstan» state program, new information technologies are being introduced into the activities of state bodies, while video surveillance cameras, electronic databases, information-analytical platforms, and elements of digital forensics are increasingly being

used in the law enforcement system[1]. At the same time, the issue of using artificial intelligence tools in the activities of law enforcement agencies has become increasingly relevant. However, comprehensive legal regulation of the use of artificial intelligence in criminal proceedings has not yet been fully established in Kazakhstan. Current legislation does not sufficiently define the procedure for using algorithmic systems in investigative activities, their legal status, the evidentiary value of their results, or issues of liability arising from their use.

In this regard, the study of the legal foundations for the use of artificial intelligence technologies in criminal investigations is of particular scientific and practical importance. On the one hand, artificial intelligence can improve the efficiency of crime detection and investigation; on the other hand, it creates a number of legal risks related to the protection of constitutional rights and freedoms. In particular, violations of the right to privacy, unlawful processing of personal data, algorithmic discrimination, lack of transparency and explainability of automated decisions, as well as the possibility of identification errors, are among the pressing issues requiring legal regulation.

At the same time, issues concerning the admissibility of information obtained through artificial intelligence technologies as evidence, the determination of procedural liability for algorithmic errors, and the establishment of effective mechanisms of judicial oversight remain insufficiently studied. In particular, the use of facial recognition systems and predictive analytics requires the establishment of clear guarantees for the protection of citizens' rights and legitimate interests.

Although the issues related to the use of artificial intelligence in law enforcement activities have been considered in the works of foreign and domestic scholars, most studies focus on technological or general legal aspects. However, within the framework of the criminal procedure system of the Republic of Kazakhstan, the legal foundations, legal risks, and mechanisms for regulating the use of artificial intelligence have not yet been comprehensively examined. This indicates that the scientific development of this issue remains incomplete.

The purpose of the study is to analyze the legal foundations, risks, and prospects of using artificial intelligence technologies in criminal investigations in the Republic of Kazakhstan and to develop proposals for improving their legal regulation.

To achieve this goal, the following objectives were established: to determine the main areas of application of artificial intelligence technologies in criminal proceedings; to study the characteristics of artificial intelligence tools used by law enforcement agencies; to analyze international experience; to assess the current regulatory and legal framework of the Republic of Kazakhstan; to identify legal risks and legislative gaps; and to develop proposals for improving legal guarantees for the protection of human rights in the use of artificial intelligence in law enforcement activities.

International experience demonstrates the importance of introducing the principles of transparency, accountability, independent oversight, judicial control, and ethical regulation when using artificial intelligence in law enforcement agencies. In this regard, there is a need to develop special legislation on artificial intelligence in the Republic of Kazakhstan, including legal norms regulating the use of artificial intelligence in criminal proceedings and the activities of law enforcement agencies. The effective implementation of artificial intelligence in the investigation system is possible only if a balance is maintained between public security interests and the protection of fundamental human rights and freedoms.

Materials and Methods

The research materials included regulatory legal acts of the Republic of Kazakhstan, international documents, scientific publications, and analytical materials on the use of artificial intelligence in law

[1] *Resolution of the Government of the Republic of Kazakhstan No. 827 of 12 December 2017 "On Approval of the State Programme 'Digital Kazakhstan'" (as amended on 1 October 2020) was repealed by Resolution of the Government of the Republic of Kazakhstan No. 311 of 17 May 2022. Available at: https://prg.kz/document/?doc_id=39315220&pos=5;111 (accessed: 14.04.2026).*

enforcement agencies. The study applied methods of legal analysis, comparative legal method, system analysis, and methods of generalizing international experience in the use of artificial intelligence technologies in criminal investigations. In addition, the existing legal risks and prospects of introducing artificial intelligence into the criminal procedure system of the Republic of Kazakhstan were examined.

Results and discussion

One of the pros of AI- ability to analyse information of huge numbers in a short amount of time. This technology is able to do actions accurately similar to what people's thinking and analysing abilities could. Nowadays, while looking deeper into crimes they use the telephone calls, messages, bank operations, camera footage, and all the other digital information as a meaningful verdict. There is just no way that one could analyse the tons of evidence like these. So the AI can easily figure out the link between all the verdicts and approximately makes interrogation way easier.

It is believed that many digital traces are left in the course of criminal activities. It might include bank transactions, calls, geolocation data, social media activity and all the actions taken place by internet. AI systems recycle all this information automatically, suspect's circle of contacts and gives an opportunity to get the movements and actions of his. Not only does it help with finding suspected one, but also finds a similarity between crime actions and gives a

Scheme that's gonna be a lot more of a help.

Digital forensics has become one of the key areas of modern criminal investigations, as a significant portion of evidence is obtained from electronic information carriers, including video recordings, emails, messenger communications, banking transaction data, internet traffic records, computers, and smartphones. Artificial intelligence technologies significantly facilitate the collection, processing, and analysis of such digital evidence. AI-powered forensic tools are capable of recovering deleted files, examining electronic communications, identifying links between devices, and automatically detecting suspicious activities. Considering that modern electronic devices may contain thousands of files, photographs, messages, and other forms of digital information, the use of AI substantially accelerates investigative procedures and improves the effectiveness of evidence examination.

As a regard, the need of inputting new technologies in the digital forensics is rising. AI is also widely used in CCTV cameras.This types of cameras have been put in the cities and look after public places all day. However, it's impossible to review all the details on your own. In these cases computer sight technologies help to recognise a face, movements and suspicious behaviour of one.

In addition, artificial intelligence is widely used as an effective tool for ensuring public safety, identifying wanted persons, monitoring road traffic, and rapidly detecting emergency situations. However, the use of such technologies must comply with the principle of respect for citizens' privacy. Excessive digital surveillance may negatively affect democratic values and fundamental rights. Therefore, maintaining a balance between security and individual freedom remains essential [1].

In recent years, the number of offenses committed through the Internet has increased significantly. Judicial practice increasingly encounters cases involving online fraud, phishing, hacking attacks, and the theft of banking data. In the detection and investigation of such crimes, artificial intelligence systems automatically analyze suspicious activities within network infrastructures.

In the field of cybersecurity, artificial intelligence assists in identifying malicious software, monitoring suspicious transactions, and preventing online fraud. For example, in banking systems, AI technologies analyze customers' routine behavioral patterns and automatically detect unusual transactions, generating alerts about potential threats. Given the growing number of cybercrimes in Kazakhstan, the importance of these technologies continues to increase.

Alongside numerous advantages, the use of artificial intelligence in criminal investigations also gives rise to significant legal risks. First and foremost, the protection of personal data remains a critical issue. AI systems collect and process vast amounts of information. If such data are used unlawfully or disclosed to third parties, the rights and legitimate interests of citizens may be violated.

Another important concern relates to algorithmic errors. In certain situations, artificial intelligence may generate inaccurate results and incorrectly identify an individual as a suspect. Such errors can have serious implications for the protection of human rights. Furthermore, many AI systems operate according to the «black box» principle, meaning that the decision-making process of the algorithm is not fully transparent or understandable. This lack of transparency may raise concerns regarding the fairness, accountability, and legitimacy of criminal investigations.

Researchers studying the application of artificial intelligence note that it can be unpredictable (it may produce a result different from the expected one [2, p.1360], which may be readable but not explainable from the perspective of existing judicial practice), unreliable, and its actions may lack transparency for human understanding [3, p.1370]. In addition, it may be biased [4, p.2-3]. The decision-making process of artificial intelligence may be based on the number of sources it considers necessary, meaning that it independently selects important documents (for example, out of 100 documents on a topic, it may choose only 2 while ignoring all the others). This is because the decision-making model is based on a specific digital code, and some data cannot be compressed by artificial intelligence without loss [4, p.5].

One of the important issues related to the implementation of artificial intelligence in criminal investigations is the question of legal responsibility. In practice, situations may arise where an automated system makes an incorrect analytical conclusion, identifies the wrong individual, or generates inaccurate recommendations for investigators. In such cases, determining responsibility becomes extremely complicated. It remains unclear whether responsibility should be assigned to the software developer, the law enforcement officer using the system, or the state institution that implemented the technology.

Therefore, the development of legal norms regulating liability for damages caused by artificial intelligence systems is becoming increasingly necessary. Another important issue concerns the admissibility of digital evidence obtained through artificial intelligence technologies. Modern criminal proceedings require that evidence be collected, verified, and evaluated in accordance with procedural law.

However, AI systems often process information using complex algorithms that may not be fully understandable even to technical specialists. As a result, courts may face difficulties when determining whether such evidence is reliable and legally admissible. This creates the need for procedural standards regulating the collection and use of AI-generated evidence in criminal cases. Furthermore, artificial intelligence systems heavily depend on the quality of data used during their training process. If the data contains incomplete, outdated, or discriminatory information, the algorithm may produce biased outcomes.

This issue is particularly dangerous in the sphere of criminal justice because any discriminatory decision may violate the principle of equality before the law. For example, predictive policing systems may focus more attention on certain social groups or geographical areas based on historical crime statistics. Consequently, the use of such systems without proper supervision may contribute to social inequality and undermine public trust in law enforcement agencies.

In this regard, it is important to develop digital culture and legal literacy in society. Citizens need to know how their data is used and what potential risks may exist. In addition, law enforcement agencies must work with the public in an open and transparent manner. If citizens do not understand how artificial intelligence is used, this may lead to a decrease in trust in the state.

Today, many countries widely use artificial intelligence technologies in their law enforcement systems. In particular, the experience of the United States, China, and European countries attracts special attention [5].

The jurisdictions of the People’s Republic of China (PRC) and the European Union (EU) strive for leadership in the field of artificial intelligence technologies; however, their approaches to the development and implementation of regulatory acts differ significantly. The EU places emphasis on strict regulation and the protection of human rights, which contributes to the formation of ethical standards in various fields, including defense, but also causes criticism due to possible restrictions on

innovative activity. A key element of this strategy became the Artificial Intelligence Act adopted in 2024, which establishes a legal framework for the safe use of AI and the protection of citizens' rights. In contrast, China applies a centralized approach aimed at stimulating innovation and ensuring rapid decision-making. Such an approach allows the country to remain at the forefront of AI legal regulation by implementing effective mechanisms such as the «Regulation on the Management of Algorithms» and the «Personal Information Protection Law». Nevertheless, there is a risk that the emphasis on the rapid implementation of technologies may lead to insufficient protection of citizens' rights [6].

Cyber security also remains one of the central challenges associated with the use of artificial intelligence in criminal investigations. AI systems operate through digital infrastructure and process significant amounts of sensitive information, including personal data, criminal records, and surveillance materials. If these systems are attacked by cybercriminals, confidential information may be stolen, altered, or manipulated. Such incidents may not only disrupt criminal investigations but also threaten national security. Therefore, the implementation of strong cyber security mechanisms and regular technical audits is essential for ensuring the safe operation of AI technologies in law enforcement bodies. Public control and transparency are also important conditions for the lawful use of artificial intelligence. Citizens should clearly understand the purposes for which AI systems are being introduced, how their personal information is processed, and what safeguards exist against abuse.

Transparent legal procedures may help prevent unlawful surveillance and strengthen confidence in state institutions. In democratic societies, the use of artificial intelligence in law enforcement should always remain subject to judicial oversight and independent monitoring mechanisms. Criminal activities committed through digital technologies frequently cross national borders, making it difficult for a single country to investigate such crimes independently. For this reason, states need to cooperate by exchanging information, harmonizing legal standards, and developing common approaches toward AI regulation. International organizations such as the United Nations, the Council of Europe, and the OECD are already actively discussing ethical and legal principles concerning artificial intelligence technologies [7].

International practice demonstrates that artificial intelligence technologies are increasingly integrated into criminal investigation and forensic activities. One of the most significant areas of application is the analysis of large volumes of structured and unstructured data. AI systems are capable of processing information obtained from various sources, identifying hidden correlations, and generating analytical insights that may support investigative decision-making. Such capabilities substantially reduce the time required for information processing and improve the efficiency of criminal investigations.

Another important area concerns the use of computer vision technologies. Modern facial recognition systems and image analysis algorithms assist law enforcement agencies in identifying suspects, analyzing surveillance footage, detecting relevant objects, and enhancing the quality of digital images obtained during investigative activities. These technologies contribute to more effective examination of visual evidence and facilitate the identification of persons involved in criminal offenses.

Artificial intelligence is also increasingly applied in predictive analytical systems. By processing historical crime data and statistical indicators, AI tools can identify geographical areas or circumstances associated with an elevated risk of criminal activity. Such analytical instruments may assist law enforcement agencies in the allocation of resources and the implementation of preventive measures. Similar approaches are reflected in Kazakhstan's ongoing digital transformation initiatives within the law enforcement sector [8].

The growing complexity of cybercrime has further expanded the role of artificial intelligence in criminal investigations. AI-based solutions are used to detect suspicious network activities, analyze blockchain transactions, identify potential cyber threats, and support investigations involving digital assets and cryptocurrency-related offenses [9].

In addition, digital forensic software equipped with AI capabilities assists specialists in recovering deleted information, processing encrypted data, and verifying the integrity and authenticity of digital evidence.

Despite the significant advantages of artificial intelligence technologies, their implementation requires appropriate legal safeguards. In many jurisdictions, the principle of human oversight remains fundamental. Under this approach, artificial intelligence serves as an auxiliary analytical instrument, while legally significant decisions continue to be made by authorized officials who bear procedural responsibility for their actions. Furthermore, the operation of AI systems is generally subject to legal requirements concerning personal data protection, transparency, accountability, and the prevention of discriminatory outcomes resulting from algorithmic decision-making. The scientific aspects of this process in jurisprudence are discussed in detail in materials on the use of artificial intelligence in criminology [10].

Artificial intelligence technologies may also contribute to improving the efficiency of forensic examinations. For example, AI systems are capable of comparing fingerprints, analyzing DNA materials, identifying forged documents, and reconstructing digital events with a high level of precision. Such technologies reduce the workload of experts and accelerate investigative procedures. However, despite these advantages, forensic experts must continue to independently verify the conclusions generated by automated systems in order to avoid technical mistakes and ensure procedural fairness. Another promising direction is the use of artificial intelligence for combating financial and economic crimes. AI systems are able to detect suspicious banking transactions, identify illegal financial schemes, and analyze large volumes of accounting data much faster than traditional methods. Considering the increasing complexity of financial crimes in the digital economy, such technologies may significantly strengthen the effectiveness of anti-corruption and anti-money laundering measures.

Given the transnational nature of cybercrime, international cooperation remains essential for the effective regulation of artificial intelligence and the investigation of digitally enabled offences. Digital technologies are not limited by national borders, and offences committed through the Internet may affect several jurisdictions simultaneously. Consequently, international organizations are paying increasing attention to issues related to AI governance, cybersecurity, personal data protection, and the safeguarding of fundamental human rights. The development of common international standards for the use of artificial intelligence may further strengthen cross-border cooperation and contribute to global digital security.

It is also important for Kazakhstan to study international experience. This is because taking global experience into account makes it possible to improve the country’s legal system and adapt law enforcement activities to modern requirements.

With regard to the current legislation of the Republic of Kazakhstan, there is currently no special law regulating the use of artificial intelligence technologies in law enforcement activities. Nevertheless, legal relations in this sphere are indirectly regulated by several normative legal acts. In particular, the Constitution of the Republic of Kazakhstan guarantees the protection of human rights and freedoms, the inviolability of private life, and the protection of personal data. In addition, the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» establishes the procedure for the collection, storage, and processing of personal information.

The norms of the Criminal Procedure Code define the procedures for collecting, examining, and evaluating evidence. However, the current legislation does not clearly define the legal status of information obtained through artificial intelligence systems, the conditions for using such information as evidence, or the procedures for verifying the reliability of algorithmic processing results. This creates a certain degree of legal uncertainty in law enforcement practice.

In our opinion, information generated by artificial intelligence should not be regarded as independent evidence but rather as an additional informational tool subject to evaluation by investigators and courts. This is because the operating principles of algorithms are not always

transparent, and the possibility of independently verifying the accuracy of their conclusions may be limited.

One of the main risks associated with the use of artificial intelligence systems is the possibility of algorithmic errors. Such errors may lead to incorrect identification of individuals, inaccurate predictions, or false conclusions. In the context of criminal proceedings, such mistakes may cause significant harm to the rights and legitimate interests of citizens.

Kazakhstan's legislation does not contain specific rules establishing liability for erroneous actions of artificial intelligence systems. Therefore, determining the subject of liability remains a complex issue. In our opinion, since artificial intelligence cannot be regarded as a full legal subject, responsibility for the results of its operation should be imposed on the state body or specific officials who introduced and used the system. In addition, high-risk algorithms should be subject to mandatory independent audits and continuous monitoring.

Although the introduction of artificial intelligence technologies into the activities of law enforcement agencies contributes to ensuring public security, the protection of citizens' constitutional rights must remain a priority. In particular, when using facial recognition systems and predictive analytics tools, special importance should be attached to observing the principle of the inviolability of private life.

In the author's opinion, it is necessary to establish special legal foundations for the use of artificial intelligence technologies in the activities of law enforcement agencies in the Republic of Kazakhstan. Such a regulatory system should be based on at least four fundamental principles: transparency of algorithms, mandatory human oversight, independent audit, and effective judicial protection of citizens' rights. In addition, it would be appropriate to adopt special legal norms clarifying the evidentiary status of information obtained with the assistance of artificial intelligence and establishing procedures for its use in court.

Thus, although artificial intelligence makes it possible to improve the efficiency of criminal investigations, its application must be accompanied by legal safeguards, state supervision, and reliable mechanisms for the protection of human rights. Only under such conditions will it be possible to ensure the safe and effective implementation of artificial intelligence technologies in the law enforcement system.

Conclusion

In summary, the findings of this research indicate that artificial intelligence is becoming an increasingly important component of modern criminal investigations. The ability of AI-based systems to process extensive datasets, identify patterns within digital information, detect relevant connections between events, and support the examination of electronic evidence creates new opportunities for improving investigative practices. These capabilities are particularly valuable in addressing cybercrime and other offenses involving large volumes of digital data.

Despite the gradual integration of artificial intelligence into law enforcement activities in Kazakhstan, the legal status of AI-generated results, the admissibility of digital evidence, and liability for algorithmic errors remain insufficiently regulated.

The analysis conducted in this study suggests that information obtained through artificial intelligence should not currently be treated as independent evidence in criminal proceedings. Rather, it should serve as an auxiliary source of analytical support whose results require verification through established procedural mechanisms.

Particular attention should also be paid to the risks associated with algorithmic inaccuracies. Errors in data processing, biased training datasets, or technical limitations of AI models may affect the reliability of investigative conclusions and, in certain circumstances, may lead to unjustified interference with individual rights. For this reason, the legal responsibilities of developers, system operators, and public officials involved in the deployment of such technologies should be clearly defined.

Based on the results obtained, it appears necessary to further develop the legal regulation of artificial intelligence within the criminal justice system of Kazakhstan. This includes establishing clear procedural rules for the use of AI technologies, defining standards for the assessment of digital evidence, introducing independent oversight and auditing mechanisms, and strengthening safeguards aimed at protecting fundamental rights and freedoms. Such measures would contribute to greater transparency, accountability, and public trust in the use of AI-assisted investigative tools.

Ultimately, the effectiveness of artificial intelligence in criminal investigations will depend not only on technological advancement but also on the existence of an appropriate legal and ethical framework. In our opinion, artificial intelligence should be regarded as a supporting instrument that enhances investigative capabilities rather than as a substitute for human judgment. Achieving an appropriate balance between technological innovation, procedural fairness, and the protection of human rights will be essential for the responsible integration of artificial intelligence into the criminal justice system.

Authors' Contributions

Apparova S.Z. conducted research on the legal aspects of the use of artificial intelligence in criminal proceedings, including the analysis of international experience, legal risks, digital evidence, and human rights protection issues.

Bizhanova A.R. developed the concept and structure of the study, participated in formulating the conclusions and recommendations, and contributed to the preparation and scientific editing of the article.

References:

1 *Daubassova Sh.S., Alaeva G.T., Dzhumabayeva K.A. AI and criminal surveillance in Kazakhstan // Eurasian Scientific Journal of Law. – 2024. – № 4(9). – P. 19–29.*

2 *Selbst A.D. Negligence and AI's Human Users // Boston University Law Review. – 2020. – Vol. 100. – P. 1315–1377.*

3 *Dufour J.M. Some Impossibility Theorems in Econometrics with Applications to Structural and Dynamic Models // Econometrica. – 1997. – Vol. 65. – № 6. – P. 1365–1387.*

4 *Yampolskiy R.V. Unexplainability and Incomprehensibility of Artificial Intelligence // Journal of Artificial Intelligence and Consciousness. – 2019. – Vol. 7. – № 2. – P. 1–15.*

5 *28 стран, включая США и Китай, подписали совместную декларацию об угрозах искусственного интеллекта. Чего опасаются больше всего? [Электронный ресурс]. – URL: https://www.currenttime.tv/a/ssha-kitay-deklaratsiyu-ugrozah-iskusstvennogo-intellekta/32667849.html (дата обращения: 16.06.2026).*

6 *Khassanay A., Tifine P. Through the Lens of the Law: How China and the European Union Are Shaping the Future of Artificial Intelligence // Вестник КазНПУ имени Абая. Серия «Юриспруденция». – 2024. – № 4(78). – С. 43–53.*

7 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 16.06.2026).*

8 *Казахстан представил международному сообществу аналитический обзор «Artificial Intelligence and Digital Transformation of Law Enforcement: The Experience of the Prosecutor General's Office of Kazakhstan» [Электронный ресурс]. – URL: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1205888?lang=ru (дата обращения: 16.06.2026).*

9 *Даниленко Ю.А. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2023. – Т. 9 (75). – № 4. – С. 232–240.*

10 Лыков Э.Н. Использование искусственного интеллекта в криминалистике [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-kriminalistike (дата обращения: 16.06.2026).

References:

1 Daubassova Sh.S., Alaeva G.T., Dzhumabayeva K.A. AI and Criminal Surveillance in Kazakhstan. Eurasian Scientific Journal of Law, 2024, No. 4(9), pp. 19-29.

2 Selbst A.D. Negligence and AI's Human Users. Boston University Law Review, 2020, Vol. 100, pp. 1315-1377.

3 Dufour J.M. Some Impossibility Theorems in Econometrics with Applications to Structural and Dynamic Models. Econometrica, 1997, Vol. 65, No. 6, pp. 1365-1387.

4 Yampolskiy R.V. Unexplainability and Incomprehensibility of Artificial Intelligence. Journal of Artificial Intelligence and Consciousness, 2019, Vol. 7, No. 2, pp. 1-15.

5 28 stran, vklyuchaya SShA i Kitai, podpisali sovmestnuyu deklaratsiyu ob ugrozakh iskusstvennogo intellekta. Chego opasayutsya bol'she vsego? Available at: https://www.currenttime.tv/a/ssha-kitay-deklaratsiyu-ugrozah-iskusstvennogo-intellekta/32667849.html (accessed 16 June 2026).

6 Khassanay A., Tifine P. Through the Lens of the Law: How China and the European Union Are Shaping the Future of Artificial Intelligence. Bulletin of KazNPU named after Abai. Series «Jurisprudence», 2024, No. 4(78), pp. 43–53.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 16 June 2026).

8 Kazakhstan predstavil mezhdunarodnomu soobshchestvu analiticheskii obzor «Artificial Intelligence and Digital Transformation of Law Enforcement: The Experience of the Prosecutor General's Office of Kazakhstan». Available at: https://www.gov.kz/memleket/entities/prokuror/press/news/details/1205888?lang=ru (accessed 16 June 2026).

9 Danilenko Yu.A. Ispol'zovanie iskusstvennogo intellekta v prestupnykh tselyakh: ugolovno-pravovaya kharakteristika. Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Yuridicheskie nauki, 2023, Vol. 9 (75), No. 4, pp. 232–240.

10 Lykov E.N. Ispol'zovanie iskusstvennogo intellekta v kriminalistike. Available at: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-kriminalistike (accessed 16 June 2026).