https://doi.org/10.31489/2025L2/125-133
UDC 343.9
Received: 31 January 2025 | Accepted: 30 March 2025

A.B. Doszhanova[1*], Ye.N. Begaliyev[2]

[1] *Law Enforcement Academy under the General Prosecutor's Office of the Republic of Kazakhstan, Kosshy, Kazakhstan;*
[2] *Supreme Judicial Council of the Republic of Kazakhstan, Astana, Kazakhstan*
(E-mail: aitok82@mail.ru; ernar-begaliev@mail.ru)

[1]*ORCID ID: 0009-0007-3257-6601, Scopus Author ID: 16095*
[2]*ORCID ID: 0000-0001-6659-8576, Scopus Author ID: 16095*

Information and communication technologies of the "Smart City" in the system of identification: forensic aspect

This article examines the application of information and communication technologies (ICT) in forensic practice within the framework of the Smart City concept. Particular attention is paid to the use of intelligent video surveillance systems, machine learning algorithms, cloud computing, and biometric technologies to enhance the accuracy of personal identification and improve the responsiveness of law enforcement agencies. The integration of automated facial recognition systems with state and private sector databases is analyzed, along with their development prospects in light of regulatory and technical considerations. The study explores forensic aspects of ICT implementation in personal identification processes, including the application of artificial intelligence (AI) and big data analytics for identifying wanted individuals, preventing crimes, and increasing the transparency of law enforcement operations. Statistical data are presented to demonstrate the effectiveness of digital technologies in crime detection and public safety enhancement. Additionally, modern video surveillance systems and their functional capabilities in forensic identification are described. The relevance of further modernization and standardization of digital platforms for personal identification, their integration with national databases, and the improvement of personal data protection mechanisms has been substantiated. The prospects for establishing a unified national AI-based video surveillance system are considered, aiming to improve response efficiency, reduce identification errors, and enhance forensic analysis methodologies.

Keywords: information and communication technologies, personal identification, forensic science, Smart City, artificial intelligence, digital security, video surveillance, biometric identification, digital forensics, big data analytics.

Introduction

Over the past decades, the digitalization of society has radically changed the processes of public safety, law enforcement and identity verification. The concept of a "smart city" involves the integration of advanced ICT to improve the quality of life of citizens, ensure law and order and effectively manage the urban environment. The experience of South Korea in integrating data management systems [1] is considered a model in the design and implementation of Smart City infrastructure. In particular, traffic flow data is synchronized in real time with the operations of emergency response services.

A similar integrated approach will be applied to other projects that rely on Internet of Things (IoT) technologies and cloud-based solutions. The overarching goal of these technological synergies is to enhance the quality of life for urban residents and improve the overall efficiency of city infrastructure. The concept of a "smart city" includes many components for creating an intelligent environment and smart management: from smart lighting to smart bus stops [2; 284]. One of the main areas of this concept is the improvement of personal identification systems, which play an important role in forensic practice and crime investigation.

The growth of the population of megacities, the increasing level of urbanization and the expansion of digital technologies require the adaptation of traditional methods of forensic identification to new challenges. Modern solutions based on video analytics, biometrics, artificial intelligence and big data analysis technologies allow law enforcement agencies to more effectively identify suspects, witnesses and victims of crimes. This will reduce the investigation time and help prevent errors.

The relevance of the study is based on the need to develop new methods of forensic identification in the context of intensive digitalization. In Kazakhstan, as in many other countries, digital transformation programs aimed at improving public safety are being actively implemented. In particular, the Smart Nur-

* Corresponding author's e-mail: aitok82@mail.ru

Sultan and Smart Almaty projects have made significant progress in the development of urban intelligent systems. However, issues of legal regulation, personal data protection, reliability of identification algorithms and resistance to cyber threats remain unresolved.

The purpose of this study is a comprehensive analysis of forensic aspects of the use of ICT in personal identification systems. The main hypothesis is that modern digital technologies will contribute to increasing the efficiency of forensic identification, but this requires improving the regulatory framework, implementation methodology and technical adaptation to existing law enforcement systems. The article discusses modern methods of personal identification, their effectiveness, limitations and development prospects in the context of the Smart City concept.

Thus, the aim of the study is to identify the advantages and disadvantages of using ICT in forensics, determine promising areas for the development of personal identification technologies, and formulate recommendations for their integration into law enforcement activities.

In recent years, Kazakhstan has been actively developing the regulatory framework in the field of digital technologies and personal data protection. The adoption of laws regulating the collection, processing and protection of personal data, as well as the use of electronic documents and electronic digital signatures, demonstrates the state's interest to ensure a balance between technological progress and the protection of citizens' rights.

The purpose of this study is to examine the possibilities and prospects for using Smart City ICT in forensic practice, including personal identification. To achieve this goal, it is planned to analyze existing digital technologies for personal identification, assess their forensic significance, identify regulatory and technical obstacles, and develop proposals for improving the methodology and mechanisms for their implementation in law enforcement practice.

Methods and materials

This study is based on a comprehensive set of scientific methods that enable an in-depth analysis of the use of information and communication technologies (ICT) in the process of personal identification in forensic practice. The following methods were employed: Analysis and synthesis were used to systematize information about modern technologies for personal identification and to determine their forensic significance. Induction and deduction allowed the identification of logical relationships between the development of ICT and their influence on the effectiveness of criminal investigations. The historical-legal method was applied to study the evolution of legal regulation of digital identification both in Kazakhstan and abroad. The comparative legal method was used to analyze the experience of countries such as the EU, USA, and China in implementing smart city technologies for the purpose of personal identification.

The formal-legal method made it possible to assess the compliance of existing legislation with the requirements of digital forensics. Digital forensic methods, such as video analytics, biometric systems, big data analysis, and the use of digital traces, were utilized to evaluate their potential applications in forensic practice. The use of these methods helped to identify the current capabilities and limitations of ICT in forensic identification, as well as to outline directions for further improvement.

The Smart City concept represents an integrated system of urban management based on the convergence of ICT, the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) technologies. The main objectives of implementing these technologies are to improve citizens' quality of life, optimize urban processes, ensure public and traffic safety, and reduce crime rates through intelligent data analysis and automated surveillance systems.

The concept of a "smart city" is a comprehensive system for managing the urban environment based on the integration of ICT, the Internet of Things (IoT), cloud computing and artificial intelligence technologies. The main goals of implementing these technologies are to improve the quality of life of citizens, optimize urban processes, ensure public and road safety, and reduce crime through intelligent data analysis and automated video surveillance systems.

An important element of the digitalization of law enforcement agencies within the framework of the "Smart City" concept is the development of intelligent video surveillance systems, automated identification tools, and crime analysis systems. [3; 45]. In Kazakhstan, video surveillance systems are integrated with the databases of the Ministry of Internal Affairs (MIA), which allows for the prompt identification of individuals, the detection of crimes, and the prevention of offenses.

The automated system for recording violations "Sergek" operates in 13 cities of Kazakhstan (Astana, Almaty, Shymkent, Turkestan, Atyrau, Taraz, Semey, Aktau, Kostanay, Kulsary, Kyzylorda, Kokshetau,

Taldykorgan) and three regions (Zhetysu, Turkestan, Almaty). In the capital of the country, about 6 thousand cameras of this system are installed, which are used to record violations of traffic rules (traffic rules), recognize faces, search for criminals and missing persons, monitor places of mass gathering of citizens, and analyze the characteristics of vehicles using artificial intelligence technologies.

The implementation of the "Sergek" system has had a significant positive impact on the level of public safety and road traffic. For example, in Astana alone, cameras recorded more than 1 million violations in 2024, while 842 thousand incidents were identified in 2023. Thanks to the implementation of this technology, the mortality rate in road accidents decreased by 48 %, the overall crime rate by 67 %, and the number of traffic violations by 72 % [4].

Results

The study found that the use of information and communication technologies (ICT) in personal identification systems significantly enhances the effectiveness of forensic practice. The key findings are as follows:

Identification of core personal identification technologies

The analysis revealed that the most widely used technologies in forensic practice include biometric systems (facial recognition, fingerprint scanning, iris recognition), video analytics, and digital trace analysis. The application of artificial intelligence in processing data from video surveillance systems improves the accuracy and speed of suspect identification.

Evaluation of legal aspects and existing barriers

The study identified gaps in the legal regulation of ICT use in forensics, particularly regarding the protection of personal data and the legality of collecting and storing biometric information. International experience (EU, USA, China) demonstrates the need to balance effective crime investigation with the protection of human rights.

Problems and limitations of technologies

Although facial recognition algorithms show high efficiency in controlled environments, their accuracy can decline due to lighting changes, camera angles, or the use of disguises. The analysis of digital traces requires significant computational power and effective methods for filtering false positives. Additional security measures are needed to counter cyber threats, including the potential manipulation of biometric data.

Practical implementation of technologies in Kazakhstan

Smart City projects in Kazakhstan (Smart Nur-Sultan, Smart Almaty) provide successful examples of integrating ICT into public safety systems. The use of facial recognition-enabled video surveillance systems has yielded positive results in crime prevention and offender identification. Thus, the findings confirm that smart city technologies hold great potential for forensic identification. However, their implementation requires improvements in legal regulation, increased algorithm reliability, and the mitigation of associated risks.

The implementation of the National Video Surveillance System project, designed to last until 2030, began in Astana and Almaty in 2025. Within the framework of this project, it is planned to install 10 thousand modern video surveillance cameras, deploy 502 hardware and software systems on the street and road network, integrate 8 thousand cameras at strategically important facilities (including those vulnerable to terrorism), and create a single situation center.

Artificial intelligence technologies will be used to manage urban transport, analyze big data, and improve forensic monitoring, which will significantly improve public and road safety. The technology has already demonstrated high efficiency: 46 wanted criminals have been detained in Astana using this system, and about 30 people have been identified in Almaty. The Ministry of Internal Affairs continues to implement the strategy to expand the intelligent video surveillance system and integrate it into a single digital law enforcement network throughout the country.

Discussion

The application of information and communication technologies (ICT) in forensic personal identification represents a crucial stage in the development of modern forensic science. The integration of smart city technologies — including surveillance systems, biometric identification, digital trace analysis, and big data processing — creates new opportunities for crime detection and ensuring public safety. However, alongside their effectiveness, these technologies raise several legal, ethical, and practical concerns.

Comparative Analysis

Comparing the results of this study with existing research in the field makes it possible to identify key trends and challenges. International experience demonstrates a wide use of ICT for personal identification. For example, in China, the United Kingdom, and the United States, facial recognition-enabled surveillance systems are used effectively in public spaces with high population density to identify suspects. However, researchers highlight risks related to the quality of source data, the adaptability of algorithms to different ethnic and age groups, and the possibility of biometric data forgery.

In Kazakhstan, a trend toward digitalization in the law enforcement system is evident. Programs such as Smart Nur-Sultan and Smart Almaty represent visible efforts to integrate ICT into urban governance. However, their application within the forensic domain remains underdeveloped.

Critical Evaluation of Technological Effectiveness

Although modern methods of identification offer high levels of accuracy, their practical implementation depends on several factors:

Data quality and accessibility: The reliability of surveillance and biometric identification largely depends on the quality of the input images and the conditions under which they are captured.

Data processing speed: The growing volume of data requires rapid analysis and powerful computational capacity from law enforcement agencies.

False data and cybersecurity threats: While modern technologies enhance identification processes, they also make it possible to forge biometric traits. This raises the risk of database breaches, personal data leaks, and manipulation of digital evidence.

Therefore, improving the effectiveness of ICT in forensics requires not only the enhancement of algorithms, but also stronger cybersecurity measures, greater transparency in data processing procedures, and tighter control over their application.

Legal and Ethical Aspects

The widespread adoption of digital identification systems requires a fundamental revision of the legal framework. In Kazakhstan, legislative acts concerning the protection of personal data and the use of biometric technologies are not yet fully aligned with the current challenges of digital forensics. Key legal concerns include:

Defining the procedures for the collection, storage, and processing of biometric data;

Establishing limits on state intrusion into individuals' private lives;

Ensuring transparency in the application of surveillance and facial recognition technologies.

From an ethical perspective, it is crucial to maintain a balance between public safety and the protection of individual rights. In China, for instance, the excessive use of surveillance has sparked concerns about a mass monitoring system, whereas EU countries apply strict regulations under the General Data Protection Regulation (GDPR). For Kazakhstan, it is essential not only to develop mechanisms for the effective use of identification technologies, but also to create systems that do not infringe on citizens' rights. This includes the implementation of independent monitoring and the development of clear usage protocols.

Key smart city technologies used in forensics:

– AI-powered video surveillance — cameras with facial recognition and automatic behavior analysis; [5; 5].

– biometric identification — fingerprints, iris, voice characteristics;

– Big data analysis systems — monitoring digital traces, including mobile devices and social networks;

– Automated video surveillance systems for public places — monitoring crowds, identifying suspicious actions.

Research has shown that the use of ICT in law enforcement significantly increases the efficiency of identification of individuals, reduces the likelihood of identification errors and increases the speed of response. However, there are certain challenges, such as the protection of personal data, the accuracy of identification algorithms and their adaptation to the conditions of a particular country.

For further development of the "Smart City" concept in forensics, it is necessary to improve the regulatory framework, introduce mechanisms for monitoring compliance with citizens' rights, and standardize the methodology for introducing ICT into the personal identification system.

The main laws regulating the ICT sector and personal data protection in Kazakhstan are:

– The Law of the Republic of Kazakhstan "On Personal Data and Their Protection" (№ 94-V dated May 21, 2013) regulates the issues of collection, processing and protection of personal data of citizens;

– The Law of the Republic of Kazakhstan "On Informatization" (№ 418-V dated November 24, 2015) regulates public relations in the field of informatization, including the creation, development and use of informatization objects;

– The Law of the Republic of Kazakhstan "On Electronic Documents and Electronic Digital Signatures" (January 7, 2003, № 370-II) establishes the legal basis for the use of electronic documents and electronic digital signatures.

These legislative acts form the basis for regulating digital technologies and protecting personal data in the country. However, despite the existing legal framework, a single standard for integrating biometric data into law enforcement information systems has not yet been developed, which indicates the need for further improvement of legal regulation.

It is necessary to comprehensively modernize legal instruments for regulating digital technologies, develop a unified standard for integrating public and private databases, and implement cybersecurity measures to protect information from unauthorized access.

International experience in regulating digital identification technologies demonstrates various approaches to ensuring a balance between the effectiveness of law enforcement and the protection of citizens' rights.

European Union: Since 2018, the General Data Protection Regulation (GDPR) has imposed strict requirements on the processing of personal and biometric data. This regulation requires citizens to obtain explicit consent for the collection and processing of their data and provides for the "right to be forgotten". The use of automated facial recognition systems in public places is prohibited, except in cases of threat to national security.

The USA: There is no federal regulation of biometric data, but some states use local laws. The California Consumer Privacy Act (CCPA) requires transparency when collecting personal data, while the Illinois Biometric Information Privacy Act (BIPA) requires companies to obtain consent before collecting people's biometric data and that the information not be disclosed to third parties without authorization.

Chinese People's Republic. The country widely uses a facial recognition system integrated with the national social credit system. Biometric technologies are actively used to identify citizens in public places, on transport, in the banking sector and in law enforcement agencies. Compared to the EU and the US, Chinese legislation does not impose significant restrictions on the protection of personal data, which allows the state to widely use personal identification technologies.

An analysis of international experience shows that Kazakhstan needs to develop its own regulatory model that takes into account national security requirements and principles of personal data protection. The optimal solution may be to adapt the best international practices, including the European approach to protecting biometric information and the American local regulatory system.

Analysis and empirical research

Comparative Analysis of the Implementation of Smart City Technologies in Different Countries

1. People's Republic of China. China is a world leader in the use of personal identification technologies in law enforcement. As part of the national project "Sharp Eye", more than 600 million video surveillance cameras equipped with facial recognition and analytical functions applied to behavioral data have been installed. Artificial intelligence makes it possible to predict crimes, detect offenses and quickly identify suspects. However, the widespread use of digital surveillance raises issues of privacy of personal data and government oversight.

2. The United States of America. In the United States, personal identification technologies are widely used, but they are accompanied by strict legal regulations. In some states (for example, California), the use of facial recognition technologies by the police is prohibited due to the high probability of errors. In addition, the Federal Bureau of Investigation (FBI) actively uses the Next Generation Identification (NGI) system, which stores more than 165 million biometric data. This will help improve the efficiency of law enforcement investigative activities.

3. European Union. EU countries are seeking to find a balance between the efficiency of digital technologies and the protection of personal data. In 2022, the European Parliament proposed a draft law on AI that would impose strict requirements on the use of artificial intelligence in personal identification processes. Automatic real-time facial recognition is prohibited in public places and is only permitted in cases of a threat to national security.

4. Republic of Kazakhstan. Digitalization of law enforcement agencies in Kazakhstan is developing rapidly. The Smart City projects in Astana and Almaty involve the integration of intelligent video surveillance

and data analysis systems into the infrastructure of the Ministry of Internal Affairs [6]. However, the country has not yet adopted a single regulatory legal act governing the use of biometric identification. This indicates the need to develop a legislative framework that determines the procedure for using personal identification technologies.

Improving legal regulation

– The modern world is rapidly changing under the influence of digital technologies [7; 150]. To effectively use identification technologies in law enforcement agencies, it is necessary to implement the following measures:

– develop a unified law on the use of biometric data, which should clearly regulate the procedure for collecting, storing and processing information;

– introduce state control mechanisms in identification systems, which will prevent violations and illegal use;

– develop standards for the ethical use of information and communication technologies (ICT) in forensics, which should ensure a balance between the effectiveness of the investigation and the protection of citizens' rights.

Adaptation of foreign experience in Kazakhstan

For the successful implementation of "smart city" technologies in the personal identification system, Kazakhstan needs to take into account international experience:

– Study of China's experience in the large-scale use of video surveillance systems in compliance with the principles of personal data protection;

– Application of the European Union's experience in regulating biometric identification and implementing standards of transparency in the use of technologies;

– Analysis of the model for integrating American biometric databases with law enforcement agencies.

The Impact of Digital Transformation on the Future of Forensic Practice

As technology advances, forensic science faces new challenges:

– training specialists in digital forensics and big data analysis;

– developing methods to combat cybercrime aimed at hacking identification systems;

– implementing a national digital security program that includes measures to protect personal data and prevent illegal use of technology.

Thus, within the framework of the Smart City concept, the development of ICT is becoming an important tool in forensics. However, for their effective use, a comprehensive approach is needed, including improving the regulatory framework, introducing advanced technologies and increasing the digital literacy of industry specialists.

Conclusions

Modern information and communication technologies, thanks to their integration into the concept of the "Smart City", play an important role in the field of forensics, providing new ways of a personal identification. The development of intelligent video surveillance systems, biometric identification, digital fingerprinting and big data analysis has significantly increased the accuracy and speed of identification processes [8]. However, the implementation of these technologies is accompanied by a number of problems, such as data security, adaptation of algorithms, as well as their legal and ethical application.

An analysis of international experience shows that different countries use different models for regulating personal identification technologies. While the European Union has limited the use of facial recognition systems in public places, China, on the contrary, is actively developing centralized surveillance platforms, and the United States uses local regulatory measures at the level of individual states in this area. Kazakhstan needs to develop a balanced regulatory system that takes into account advanced international experience and national specifics.

In addition, the development of artificial intelligence and machine learning technologies opens up new prospects for forensics. Modern algorithms allow us to reduce the number of errors in face recognition, increase the accuracy of identification and expand the capabilities of digital trace analysis. However, the effective use of these technologies requires constant updating of cybersecurity methods, which in turn requires the development of a comprehensive information security strategy.

Information and communication technologies (ICT) are fundamentally transforming methods of personal identification in forensic practice. The methods and technological solutions examined in this study

demonstrate that the use of ICT enhances both the accuracy and speed of identification, reduces the influence of human error, and minimizes the likelihood of mistakes. However, large-scale implementation is accompanied by legal, technical, and ethical challenges.

Key Findings:

ICT as a tool for forensic identification — video analytics, biometric systems, digital traces, and artificial intelligence algorithms have become integral components of modern law enforcement. These technologies support not only rapid crime investigations but also proactive crime prevention.

Legal, technical, and ethical constraints — legislation in Kazakhstan and other countries must adapt to the new realities of digital forensics. The protection of personal data, the legality of biometric data collection and use, and the risks of misuse by public and private entities remain critical concerns.

Prospective directions for development — enhancing multifactor identification systems, updating the regulatory framework, strengthening cybersecurity, and integrating data from multiple sources will contribute to the effective application of ICT in forensics.

Practical Significance of the Research:

For law enforcement agencies — to improve identification methods, accelerate investigation processes, and increase crime detection rates.

For technology developers — to create more accurate, reliable, and secure identification systems.

For legislators and legal experts — to develop a sound legal framework that ensures the lawful use of ICT in forensic practice.

For the academic community — to further develop new theoretical and methodological approaches in digital forensics.

Final Evaluation

The integration of smart city technologies into forensic identification systems offers significant potential, but requires a comprehensive approach to address technical, legal, and ethical issues. In the future, it will be necessary not only to improve recognition algorithms but also to ensure the transparency of their application and the protection of citizens' personal data.

Thus, the digitalization of forensic science is not only a technological but also a social process. The synergy of technological innovation, legal regulation, and ethical standards can foster a balanced identification system — one that ensures public safety while safeguarding individual rights.

Ethical aspects of the use of information and communication technologies also remain an important area for further development. The use of digital technologies should be carried out in accordance with the principles of non-discrimination, transparency and respect for the rights of citizens [9]. Government agencies, the scientific community and technology companies need to collaborate to develop standards [10] that ensure a balance between effective law enforcement and the protection of personal data.

Based on the conducted research, the following main areas of further development can be identified:

1. Technical improvements — development of machine learning algorithms, increasing the accuracy of face recognition, improving cybersecurity systems.

2. Methodological solutions — unification of forensic identification methods, adaptation of international experience, expansion of digital data analysis tools.

3. Practical implementation — implementation of pilot projects, advanced training of specialists, development of interdepartmental cooperation in the field of personal identification.

In the context of digitalization, the future of forensics depends on the successful integration of Smart City technologies into the activities of law enforcement agencies. Only a comprehensive approach that includes technological, legal and methodological aspects will make it possible to achieve significant progress in ensuring public safety.

Thus, ICT within the framework of the Smart City concept is a powerful tool for future forensics. Their effective use requires a comprehensive approach, including legal regulation, technical improvements, data protection and compliance with ethical standards. Only if these conditions are met will it be possible to create a reliable and fair identification system that will contribute to strengthening law and order and public safety.

Acknowledgements

This article was published using funds from the project (funding source: Scientific Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan BR 28511965).

References

1 Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269. «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы». — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P2300000269

2 Смарт-город: стратегия, технологии и эффективность / под ред. В.Д. Соловьева. — М.: Инфра-М, 2021. — 284 с.

3 Кривоносов А.В. Современные технологии установления личности в криминалистике / А.В. Кривоносов // Вестник криминалистики. — 2022. — № 4. — С. 45–58.

4 Проект Smart Nur-Sultan. — [Электронный ресурс]. — Режим доступа: https://astana.gov.kz.

5 Face Recognition Technologies: A Primer. Congressional Research Service Report R46541. — United States, 2020. — P. 5–12.

6 Государственная программа «Цифровой Казахстан». — [Электронный ресурс]. — Режим доступа: https://digitalkz.kz/

7 Garvie C. The Perpetual Line-Up. / C. Garvie, A. Bedoya, J. Frankle. — Georgetown Law Center, 2016. — 150 p.

8 NIST Face Recognition Vendor Test (FRVT). — [Электронный ресурс]. — Режим доступа: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

9 Закон РК от 21.05.2013 № 94-V «О персональных данных и их защите». — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z1300000094

10 Verkada camera breach. — Bloomberg, 2021. — [Электронный ресурс]. — Режим доступа: https://www.bloomberg.com/news/articles/2021-03-09/hackers-breach-surveillance-startup-verkada

А.Б. Досжанова, Е.Н. Бегалиев

Жеке басын анықтау жүйесіндегі «Ақылды қала» ақпараттық-коммуникациялық технологиялары: криминалистикалық аспект

Мақалада «Ақылды қала» (Smart City) тұжырымдамасы аясында ақпараттық-коммуникациялық технологияларды (АКТ) криминалистикалық практикада қолдану мүмкіндіктері талданған. Әсіресе, бейнебақылаудың интеллектуалды жүйелерін, машиналық оқыту алгоритмдерін, бұлттық есептеулерді және биометриялық технологияларды құқық қорғау органдарының жедел әрекет етуі мен жеке басты дәл анықтауын жақсарту мақсатында пайдалану мәселелері қарастырылған. Мемлекеттік және жеке ұйымдардың дерекқорларымен интеграцияланған автоматтандырылған бет-әлпетті тану жүйелерінің мүмкіндіктері мен оларды нормативтік-құқықтық және техникалық аспектілерді ескере отырып дамыту перспективалары зерттелген. Мақалада криминалистикадағы АКТ-ны қолдану ерекшеліктері қарастырылған, оның ішінде жасанды интеллект (ЖИ) пен үлкен деректерді талдау арқылы іздеудегі тұлғаларды анықтау, қылмыстардың алдын алу және құқық қорғау органдары жұмысының ашықтығын арттыру мәселелері зерделенген. Цифрлық технологиялардың қылмысты ашудағы және қоғамдық қауіпсіздікті қамтамасыз етудегі тиімділігін дәлелдейтін статистикалық мәліметтер келтірілген. Криминалистикалық сәйкестендіру барысында қазіргі заманғы бейнебақылау жүйелері мен олардың функционалдық мүмкіндіктері сипатталған. Жеке басты анықтаудың цифрлық платформаларын әрі қарай жаңғырту және стандарттау, оларды ұлттық дерекқорлармен интеграциялау және жеке деректерді қорғау механизмдерін жетілдіру қажеттілігі негізделген. ЖИ негізінде ұлттық бейнебақылау жүйесін құру перспективалары қарастырылған, бұл құқық қорғау органдарының жедел әрекет етуін күшейтіп, сәйкестендірудегі қателіктерді азайтуға және криминалистикалық талдау әдістерін жетілдіруге мүмкіндік береді.

Кілт сөздер: ақпараттық-коммуникациялық технологиялар, жеке басты анықтау, криминалистика, «Ақылды қала», жасанды интеллект, цифрлық қауіпсіздік, бейнебақылау, биометриялық сәйкестендіру, цифрлық криминалистика, үлкен деректерді талдау.

А.Б. Досжанова, Е.Н. Бегалиев

Информационно-коммуникационные технологии «Умного города» в системе установления личности: криминалистический аспект

В статье анализируются возможности применения информационно-коммуникационных технологий (ИКТ) в криминалистической практике в рамках концепции «Умного города» (Smart City). Особое внимание уделяется использованию интеллектуальных систем видеомониторинга, алгоритмов машинного обучения, облачных вычислений и биометрических технологий для повышения точности идентификации личности и оперативности реагирования правоохранительных органов. Исследуется

интеграция автоматизированных систем распознавания лиц с базами данных государственных и частных организаций, а также перспективы их развития с учетом нормативно-правовых и технических аспектов. Рассматриваются криминалистические аспекты применения ИКТ в процессе установления личности, включая использование искусственного интеллекта (ИИ) и анализа больших данных для выявления разыскиваемых лиц, предотвращения преступлений и повышения прозрачности работы правоохранительных структур. Приведены статистические данные, подтверждающие эффективность цифровых технологий в раскрытии преступлений и обеспечении общественной безопасности. Описаны современные системы видеонаблюдения и их функциональные возможности в процессе криминалистической идентификации. Обоснована необходимость дальнейшей модернизации и стандартизации цифровых платформ идентификации, включая их интеграцию с национальными базами данных и развитием механизмов защиты персональной информации. Рассмотрены перспективы создания единой национальной системы видеомониторинга на основе ИИ, которая обеспечит повышение оперативности реагирования, снижение ошибок идентификации и усовершенствование методов криминалистического анализа.

Ключевые слова: информационно-коммуникационные технологии, установление личности, криминалистика, «Умный город», искусственный интеллект, цифровая безопасность, видеомониторинг, биометрическая идентификация, цифровая криминалистика, анализ больших данных.

References

1 Postanovlenie Pravitelstva Respubliki Kazakhstan ot 28 marta 2023 goda № 269 «Ob utverzhdenii Kontseptsii tsifrovoi transformatsii, razvitiia otrasli informatsionno-kommunikatsionnykh tekhnologii i kiberbezopasnosti na 2023–2029 gody» [Resolution of the Government of the Republic of Kazakhstan dated March 28, 2023 No. 269. "On approval of the Concept of digital transformation, development of the information and communication technology industry and cybersecurity for 2023–2029"]. (2023, 28 March). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/P2300000269 [in Russian].

2 Soloveva, V.D. (Eds.). (2021). *Smart-gorod: strategiia, tekhnologii i effektivnost. [Smart City: Strategy, Technology and Efficiency]*. Moscow: Infra-M [in Russian].

3 Krivonosov, A.V. (2022). Sovremennye tekhnologii ustanovleniia lichnosti v kriminalistike [Modern technologies of identification in forensic science]. *Vestnik kriminalistiki — Bulletin of Criminalistics*, 4, 45–58 [in Russian].

4 Proekt Smart Nur-Sultan [Smart Nur-Sultan project]. *astana.gov.kz.* Retrieved from https://astana.gov.kz [in Russian].

5 (2020). *Face Recognition Technologies: A Primer. Congressional Research Service Report R46541*. United States.

6 Gosudarstvennaia programma «Tsifrovoi Kazakhstan» [State program "Digital Kazakhstan"]. *digitalkz.kz.* Retrieved from https://digitalkz.kz/ [in Russian].

7 (2016). Garvie, C., Bedoya, A., & Frankle, J. *The Perpetual Line-Up*. Georgetown Law Center.

8 NIST Face Recognition Vendor Test (FRVT). *www.nist.gov.* Retrieved from https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

9 Zakon RK ot 21.05.2013 № 94-V «O personalnykh dannykh i ikh zashchite» [Law of the Republic of Kazakhstan dated 21.05.2013 No. 94-V "On personal data and their protection"]. (2013, 21 May). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z1300000094 [in Russian].

10 (2021). Verkada camera breach. Bloomberg. *bloomberg.com.* Retrieved from https://www.bloomberg.com/news/articles/2021-03-09/hackers-breach-surveillance-startup-verkada

Information about the authors

Doszhanova Aitolkyn Bugybaikyzy — PhD Student at the Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Kosshy, Kazakhstan; e-mail: aitok82@mail.ru

Begaliyev Yernar Nurlanovich — Doctor of Law, Professor, Member of the Supreme Judicial Council of the Republic of Kazakhstan, Astana, Kazakhstan; e-mail: ernar-begaliev@mail.ru