IRSTI 10.81.61
UDC 343.9.018
JEL K14

https://doi.org/10.46914/2959-4197-2026-1-3-173-183

TEMIRBOLAT N.S.,*[1]
c.l.s., senior lecturer.
*e-mail: nuraishamail@gmail.com
ORCID ID: 0000-0002-8447-5753
MEYRKULOVA G.D.,[2]
c.l.s., senior lecturer.
e-mail: adil.96-96@mail.ru
ORCID ID: 0000-0001-7359-0601
[1]KazNU after al-Farabi,
Almaty, Kazakhstan
[2]SKU after M. Auezov,
Shymkent, Kazakhstan

THE ROLE OF DIGITAL FORENSICS IN CRIMINAL INVESTIGATIONS IN THE REPUBLIC OF KAZAKHSTAN

Abstract

The study explores the role of digital forensics in the context of criminal investigations in Kazakhstan, focusing on how digital evidence such as CCTV footage, mobile data, and social media content is collected, analysed, and used. Drawing on policy documents, case studies, and legal frameworks, the research highlights the expanding use of surveillance technologies, artificial intelligence, and big data in both crime prevention and state control. While digital forensics enhances capabilities in tackling cybercrime and fraud, its use in monitoring political dissent raises concerns about civil liberties. The study also identifies major legal, technical, and institutional challenges affecting the reliability and admissibility of digital evidence in court, including vague legislation, inconsistent procedures, and insufficient regulatory oversight. The study contributes both practically and theoretically to discussions on digital forensics practices withing evolving legal systems. It proposes measures to strengthen evidentiary standards, advance legal reform, and enhance institutional capacity, while emphasising the need for increased transparency and ethical governance in digital forensic practices.

Keywords: Digital forensics, Criminalistics, Smart cities, Electronic evidence, Artificial intelligence, Cybercrime.

Introduction

Digital technologies have reshaped how crimes are committed, not only transforming traditional methods but also enabling new forms of crime, such as phishing and cyberattacks [1]. The widespread use of digital devices and the internet in daily life means that nearly every crime now leaves behind some form of digital evidence, which is vital for the criminal justice system. As technology continues to evolve, law enforcement agencies must adapt to new criminal tactics and methods of concealment. This presents major challenges for institutions such as police forces, which have often failed to invest sufficiently in information technology [1].

Digital forensics, as conceptualised by Interpol [2], entails analysing and interpreting data from digital devices, computers, and storage media, with particular emphasis on the stages of identification, acquisition, analysis, and reporting in forensic practice. It plays an essential role in uncovering digital evidence and supporting investigations in an increasingly digital world.

Kazakhstan, a nation characterised by growing digitisation of society, driven by state-led initiatives such as E-government and Digital Kazakhstan [3], has increased both the incidence of digital evidence and the urgency of adapting criminal investigation practices [4]. However, institutional, legal, and technical capacities to handle digital forensics remain underdeveloped and under-researched [5].

Despite the increasing presence of digital evidence in criminal cases, there is limited scholarly attention on how Kazakhstani law enforcement agencies collect, analyse, and utilise such data, and whether current practices meet international forensic standards. Therefore, it is appropriate to outline the aims and the research question which guides this study.

This study seeks to explore how Kazakhstan collects and uses digital evidence (such as CCTV, mobile phone data, and social media) within criminal investigations, and seeks to analyse related challenges in data integrity, privacy, and court admissibility. This line of inquiry is guided by the following research question:

How is digital forensic evidence collected, analysed, and utilised in criminal investigations in Kazakhstan, and what are the key legal, technical, and institutional challenges affecting its reliability and admissibility in court?

This study seeks to analyse the current configuration of digital forensic practices in Kazakhstan by identifying key institutional and procedural constraints and evaluating their consistency with established international standards. In doing so, it advances a more nuanced understanding of the development of digital forensic practices within post-Soviet legal contexts. The literature review that follows examines both the evolution and scope of digital forensics in criminal investigations, as well as the legal and institutional arrangements shaping its application in Kazakhstan. The paper then outlines the methodological approach adopted, which is designed to investigate the institutional structures, technological capacities, and practical challenges that characterise digital forensic work in the country.

The Evolution and Scope of Digital Forensics in Criminalistics

The evolution of digital forensics within criminalistics reflects a dynamic progression from early, rudimentary data recovery efforts to sophisticated, legally rigorous investigative practices that address the complexities of modern digital evidence. A key voice documenting the formative period of digital forensics in criminalistics is Pollitt [6], whose work provides a foundational account of the evolution of digital forensic practices.

Digital forensics has its origins in the early 1980s with the rise of IBM PCs, which attracted computer hobbyists, including individuals from law enforcement. Despite limited support from their agencies, these pioneers recognised the potential of computers in criminal investigations. They independently dedicated time and resources to acquiring expertise in emerging technologies, eventually establishing the first professional body in the field, the International Association of Computer Investigative Specialists. This initiative played a foundational role in shaping the development of contemporary digital forensic practices [6].

In the early days of digital forensics, cases focused on simple tasks like recovering deleted data from individual computers, as storage was limited and often erased. Criminals used dial-up connections to access systems, and a new type of fraud emerged where inexpensive computers were used to hack telephone networks, allowing free calls and anonymity [6].

“Since 2005, the field of digital forensics has grown substantially in parallel with the increasing embedding of digital technologies in everyday life and criminal activity, a trend propelled by the rapid expansion of connected devices, networked systems, and cloud-based infrastructures. As a result, digital evidence became increasingly prevalent in criminal investigations, necessitating more advanced forensic methods and tools to analyse data from a wide range of devices and platforms” [6].

In Dubey, Bhatt, & Negi’s [8] review and analysis of digital forensics tools and challenges, the authors conclude that the tool EnCase, the most widely accepted forensic tool globally, used by 89% of merchandise companies, 91% of banks, 98% of federal agencies, and 80% of universities in the U.S, is the most reliable digital forensic tool, due to its speed in data recovery, password recovery, and email analysis.

According to Resendez, Martinez, & Abraham digital forensics involves the systematic extraction of data from electronic devices using rigorous and legally sound methodologies to make sure the evidence is admissible in a court. This process requires adherence to established forensic protocols, including maintaining a clear chain of custody and thorough documentation. The authors assert that two critical aspects must be considered when handling digital evidence: firstly, the collection process must preserve the original state of the data to avoid contamination; secondly, the procedures employed must align with recognised law enforcement forensic standards to ensure the reliability and legal integrity of the evidence.

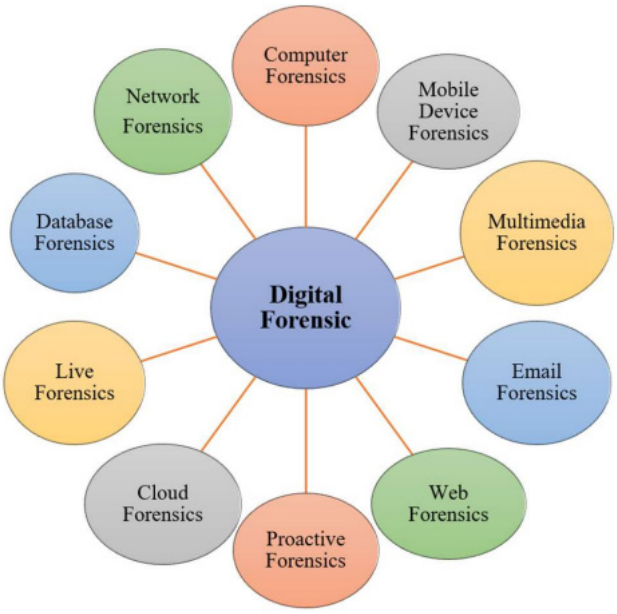

Figure 1 – Classification of Digital Forensics [7]

Note: Compiled by the authors.

The admissibility of digital evidence is of vital importance in modern legal proceedings, as it determines whether crucial electronic data can be lawfully recognised and relied upon in the pursuit of justice across increasingly digital and transnational crimes. Various factors can render digital assets valueless, including hardware obsolescence, inadequacies of outdated computing formats, human error, and malicious software [9].

The presentation of digital forensic evidence in judicial proceedings continues to present significant difficulties, frequently arising from deficiencies such as an inadequately maintained chain of custody, non-compliance with established legal procedures, and compromised integrity of evidential material. Strict adherence to procedural requirements during the collection of evidence at digital crime scenes is therefore critical to ensure its admissibility in court and its effectiveness in supporting prosecution. However, procedural weaknesses in evidence collection, together with failures to preserve the accuracy, authenticity, and completeness of digital data, have resulted in the exclusion of such evidence in a range of legal cases [10].

Antwi-Boasiako & Venter [11] describe a cohesive framework three-phase that amalgamates the technical and legal prerequisites for the acceptance of digital evidence. Initially, the legal foundation for obtaining the evidence must be firmly established, typically through a court order or authorised organisational procedure. Once legality is confirmed, the technical integrity of the evidence is assessed, focusing on factors such as adherence to forensic models, validated tools and expertise, proper chain of custody, and comprehensive documentation. These technical assessments inform judicial decisions regarding both the admissibility and evidential weight of the digital material. This harmonised model also supports standardised practices across jurisdictions, particularly in cross-border cases, thereby promoting consistency and reliability in the handling of digital evidence.

Established standards already offer detailed guidance, collaborative assistance, and exemplary frameworks and procedures for conducting digital forensic investigations and handling electronic evidence. The Convention on Electronic Evidence (2016) functions as an international treaty providing broad guidance on the recognition and admissibility of electronic evidence originating from foreign jurisdictions, while also fostering increased awareness among judges and legal practitioners regarding the principles governing the admissibility of digital evidence [10].

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are key global standard-setting institutions that produce internationally recognised guidelines, including those relevant to digital forensics, with the aim of enhancing consistency,

reliability, and quality in investigative practice. Within this framework, ISO/IEC 27043 provides a comprehensive model for conducting digital investigations, covering the full lifecycle from preparation through to post-incident activities, and emphasising standardised procedures to support repeatability and consistency. ISO/IEC 27037, in turn, offers guidance on incident handling, with a particular focus on preserving the integrity and authenticity of digital evidence [12]. ISO/IEC 27041 addresses the suitability and appropriateness of methods related to evidence handling, storage, and investigative procedures, ensuring that they are aligned with defined objectives [13]. Complementing these, ISO/IEC 27042 provides guidance on the effective application of analytical tools and techniques for examining digital evidence, building on the principles established in ISO/IEC 27037 [14].

Collectively, these standards establish a structured basis for digital forensic work, supporting investigative processes that are both methodologically robust and legally defensible. In practice, they help professionals navigate the complexities of evidence handling and analysis, especially in dynamic or high-stakes environments. Understanding and applying these guidelines is crucial not only for technical accuracy but also for maintaining the credibility of findings in legal or organisational contexts.

Next, it is important to critically examine the institutional and legal frameworks governing digital forensics in Kazakhstan, with particular attention to domestic legislation, forensic procedures, and the legal admissibility of digital evidence, alongside an assessment of how major policy initiatives and international evaluations have shaped the sector's development and reform trajectory. Forensic science in Kazakhstan is still in its early developmental phase, gradually evolving into a distinct field of forensic technology [15], yet there is a growing legal framework pertaining to digital forensics. The following instruments collectively underscore Kazakhstan's scant but growing legal framework for digital forensics.

In 2023, the Government [16] formally adopted a new strategic framework aimed at guiding the country's digital change, the development of its information and communication technology segment, and the strengthening of cybersecurity through to 2029. This updated policy replaces a previous strategy introduced in 2021 and is intended to align with the broader national planning system. Under this framework, central government bodies and relevant organisations are tasked with implementing the strategy and reporting on its progress in accordance with established state planning procedures. Oversight and coordination of these efforts have been assigned to the Ministry of Digital Development, Innovation and Aerospace Industry. The decree, which took effect upon signature, signals the government's reinforced commitment to developing a technologically advanced and secure digital environment.

Although Kazakhstan's Resolution No. 269 does not explicitly address digital forensics, it lays critical groundwork that supports its advancement. The strategy outlines the development of national systems for biometric identification, video surveillance, and intelligent monitoring, particularly within the framework of "Smart City" initiatives. These technologies are integral to digital forensic processes, enabling the collection, preservation, and analysis of electronic evidence in both criminal and civil contexts. Although digital forensics is not a central focus of the concept, the infrastructure it promotes, along with its cybersecurity provisions and regulatory reforms, creates a solid basis for the development and expansion of contemporary forensic capabilities.

The document "On approval of the Rules for the organisation and production of forensic examinations and research in forensic examination bodies" from the Minister of Justice of Kazakhstan, dated April 27, 2017, No. 484, establishes the rules for organising and conducting forensic examinations in forensic agencies across the country. Although it does not specifically detail digital forensics, the regulations apply broadly to all forensic examinations, encompassing the processing and analysis of digital evidence, which plays a crucial role in contemporary forensic work [17].

As of publication of this study, Kazakhstan has not yet ratified the Budapest Convention on Cybercrime, the leading international treaty on cybercrime and electronic evidence that guides countries in creating cybercrime laws and promotes global cooperation. The treaty covers criminal acts like illegal access, data interference, fraud, and child exploitation, and grants powers for investigation and evidence collection [18].

Despite not formally joining, since 2017, Kazakhstan has collaborated with the Council of Europe to assess its legal and institutional frameworks on cybercrime and electronic evidence, leading to a

formal request for accession in November 2022. On 19 April 2023, Kazakhstan was invited to join the Convention on Cybercrime as an Observer to the Cybercrime Convention Committee, gaining access to enhanced capacity-building support. The Council of Europe, through the Octopus Project, will continue assisting Kazakhstan in finalising its accession and reinforcing its capabilities to address cybercrime and e-evidence issues [19].

Materials and methods

For this study on the role of digital forensics in modern Kazakhs criminal investigations, a qualitative case study methodology will be employed. According to Yin [20, p. 15], the case study approach is particularly suitable when investigating a modern phenomenon situated within its real-life context, particularly in situations where the distinction between the phenomenon and its surrounding context is not clearly defined.

This approach allows for an in-depth exploration of how digital evidence, such as CCTV footage, mobile data, and social media records, is collected, analysed, and utilised within Kazakhstan's criminal justice system. Primary data will be collected through document analysis of relevant legal codes, court rulings, procedural manuals, and policy reports related to digital forensics in Kazakhstan, where possible and accessible.

Thematic analysis will be used to identify key patterns and issues, particularly those related to data integrity, privacy, and evidentiary admissibility in court. If accessible, a limited quantitative component may be incorporated by analysing available statistics on the prevalence of digital evidence in investigations and its impact on legal outcomes.

Results and discussion

Digital forensics is becoming increasingly important in Kazakhstan's law enforcement, corporate security, and national defence. It supports investigations into cybercrime, fraud, and violations of intellectual property while helping to strengthen national cybersecurity [15]. Recent efforts include the establishment of a dedicated digital forensics branch and the launch in 2021 of the Centre for Computer Forensics and Investigation of Cyber Attacks (TSARKA). These initiatives demonstrate the government's commitment to modernising forensic technology and providing specialised t raining [15]. Although publicly available details on individual cases remain limited, digital forensic methods have been utilised in investigations involving fraud, unauthorised access to systems, and malware-related offences. In addition, collaboration with international bodies such as Europol has supported the development of local professional capacity and expertise [15].

Rising cybercrime and historically low resolution rates have prompted greater investment in digital forensics, now seen as vital to pre-trial investigations and evidence gathering. Early successes have secured stronger institutional backing, positioning digital forensics as a key asset in Kazakhstan's criminal justice system [15].

The "Smart Cities" initiative, part of the national Digital Kazakhstan programme, seeks to improve urban quality of life and enhance public security through the integration of advanced technologies. In 2018, Kazakhstan launched the Smart Astana and Smart Almaty projects, along with pilot schemes across 17 regions to test specific smart city components [21]. These initiatives integrate a range of digital technologies that likewise enhance forensic capabilities, including intelligent video surveillance systems, machine learning applications, cloud-based computing, and biometric identification tools such as facial and fingerprint recognition.

As part of the Smart Aqkol pilot initiative, advanced surveillance and data analysis technologies have been implemented to strengthen urban safety and operational oversight. Approximately seventy closed circuit television cameras have been strategically positioned at key locations, including city entry points, schools and various public spaces, with the aim of enhancing security and public order. A dedicated Situation Centre functions as the central data processing hub, collecting and analysing information from these surveillance systems. By employing artificial intelligence-based analytics, the centre enables real time monitoring and facilitates more in-depth assessments of urban activity. Furthermore, the integration of the Smart Aqkol system with external databases, including those in

education, healthcare, and taxation, enables more integrated forms of digital forensic analysis and data-informed decision-making, thereby enhancing understanding of urban processes and strengthening governance practices [21].

As part of Almaty's broader transport modernisation, the city introduced advanced systems to enhance monitoring and enforcement, Sergek. Automated Sergek systems now tracks buses in real time through GPS and onboard cameras, while a dedicated mechanism allows for fines to be issued based on passenger complaints. In addition, a comprehensive photo and video recording system was implemented to detect and document traffic violations, currently overseeing more than seven hundred traffic lanes. These digital measures collectively strengthen oversight, improve service accountability and support data driven enforcement within the city's transport network [21].

The "Sergek" is currently deployed across 13 cities in Kazakhstan. In the capital city alone, around 6,000 surveillance cameras form part of this system, enabling the monitoring of traffic offences, the application of facial recognition technologies, the tracking of suspected offenders and missing persons, the supervision of crowded public spaces, and the analysis of vehicle attributes through artificial intelligence [22].

In addition, the National Video Surveillance System, scheduled for implementation through to 2030, was launched in 2025 in Astana and Almaty. This initiative includes plans to deploy 10,000 high-tech CCTV cameras and to integrate a further 8,000 existing cameras positioned at strategically significant sites, including areas identified as potential terrorism risks. Additionally, 502 hardware and software systems will be deployed across the urban road network, alongside the creation of a unified situation centre [22].

Artificial intelligence technologies are expected to strengthen forensic monitoring and large-scale data analysis, thereby substantially improving public safety outcomes. The system has already demonstrated notable effectiveness, facilitating the arrest of 46 wanted persons in Astana and enabling the identification of approximately 30 individuals in Almaty. The Ministry of Internal Affairs is continuing its efforts to further develop this intelligent surveillance infrastructure and to integrate it fully into a nationwide digital law enforcement framework [22].

In Kazakhstan, digital forensic evidence is collected, analysed, and utilised primarily as a tool for state surveillance and control, particularly in cases involving political dissent. According to Amnesty International [23], during 2015 and 2016, the Kazakhstani authorities intensified restrictions on freedom of expression and peaceful assembly, with a particular focus on social media and messaging applications. These platforms, which were used to express dissent, share information, and organise protests, became key targets for monitoring. Authorities collected digital content such as posts and messages, likely through surveillance and cooperation with service providers. This information was then analysed to identify individuals involved in organising or promoting demonstrations. In cases such as those of human rights defenders Maks Bokaev and Talgat Ayan, digital communications were used as evidence to impose administrative penalties and pursue criminal prosecutions. This indicates that digital forensic evidence in Kazakhstan is not only gathered and analysed systematically but is also instrumentalised in criminal investigations, particularly against those opposing government policies.

In Kazakhstan, social media posts and messages are increasingly used as important digital forensic evidence in criminal investigations, especially in politically motivated cases. For example, a satirical blogger faces up to seven years in prison for allegedly inciting interethnic discord, with his Instagram content, a satire involving a Russian TV presenter and a critical song, forming the core of the charges [24]. This case shows how Kazakhstani authorities collect and analyse digital content from social media platforms to build criminal cases. The digital evidence is then used not only to prosecute individuals but also to suppress dissent and restrict civil society, demonstrating the important role digital forensics plays in the government's approach to controlling political expression.

In summary, digital forensic evidence in Kazakhstan is collected through an expanding network of surveillance technologies, analysed using artificial intelligence and big data systems, and utilised in a wide range of criminal investigations. Although it is increasingly used to address cybercrime, fraud, and breaches of public safety, its application also extends to the surveillance of political dissent and the enforcement of state authority. The incorporation of smart city systems, nationwide surveillance programmes, and international cooperation has enhanced both the technical capabilities and institutional capacity for digital forensics. At the same time, this dual-use character, serving

both security objectives and mechanisms of control, underscores the complex and at times contested position of digital evidence within Kazakhstan's criminal justice framework.

Despite the growing relevance of digital evidence in criminal investigations and legal proceedings, Kazakhstan's legal framework lacks detailed procedural standards specifically governing the admissibility of such evidence in court. Digital evidence is generally treated under the same evidentiary standards as physical or testimonial evidence, but this can result in inconsistent interpretations by judges and law enforcement due to the absence of dedicated legislation or judicial guidelines. Issues such as data authenticity, chain of custody, and the forensic soundness of collection methods are not comprehensively addressed in the current procedural code. This regulatory gap poses challenges for the consistent and reliable use of digital evidence, particularly in complex cybercrime cases where evidentiary integrity is paramount.

"In 2020, K.S. Lakbaev et al. examined the utilisation of digital forensic expertise within Kazakhstan's legal framework. The study emphasises the role of expert examinations, defined as impartial analyses carried out by specialists possessing relevant education and professional experience, which serve to establish facts related to specific legal proceedings" [25]. These examinations are commissioned by both state and private entities and are integral to civil, arbitration, and criminal cases. The findings produced through such expert analyses hold evidentiary value in court and typically incur a minimum fee of 200,000 tenge, primarily utilised by individuals and corporate clients [25]. The research identifies approximately thirty distinct types of expert examinations, contingent upon the commissioning organisation, with the process culminating in a formal expert report. This investigation contributes to a broader understanding of the evolving landscape of digital forensics in Kazakhstan, illustrating its practical application through expert examination practices.

The broader availability of internet resources has led to the emergence of new, specific types of offences that are not adequately addressed by the criminal legislation of the Republic of Kazakhstan. An essential step in combating crimes that undermine information security is the formulation of a comprehensive and precise conceptual framework within criminal law relating to the information sphere, accompanied by further elucidation and clarification of the relevant terms [26].

The development of legal concepts in this evolving field must rest on a comprehensive understanding of the technical features of contemporary information processing technologies as well as the character of digital information itself, whether it is kept on computer media, inserted in information systems, or conveyed through networks of communication. This is essential, as such information constitutes an entirely new category within criminal law [27].

According to the current criminal legislation of Kazakhstan, the foundation of cybercrime is established by socially harmful acts specified in Clause 4 of Part 2 of Article 190 of the 2014 Criminal Code. From the standpoint of criminal law, it is recommended to define as cybercrime only those offences explicitly enumerated within this section. Nevertheless, within forensic practice, the concept is interpreted more broadly to include other unlawful acts that involve the use of computers and the Internet (also falling under Clause 4 of Part 2 of Article 190). This broader categorisation is justified by the fact that such offences typically involve unauthorised access to information systems, thus directly linking them to cybersecurity concerns. It is also noteworthy that, as evidenced by statistical data, the clearance rate for crimes committed in the field of information and communications remains unsatisfactory [15].

To further develop the Smart City concept in a forensic context, it is necessary to reinforce the regulatory framework, establish safeguards for the protection of citizens' rights, and ensure the standardised integration of information and communication technologies (ICT) within personal identification systems [22].

The main legislative acts regulating information and communication technologies and the protection of personal data in Kazakhstan comprise the following:

- The Law "On Personal Data and Their Protection" (No. 94-V, 21 May 2013), which regulates the collection, processing, and protection of individuals' personal data.
- The Law "On Informatisation" (No. 418-V, 24 November 2015), which regulates activities related to the development and use of information systems.
- The Law "On Electronic Documents and Electronic Digital Signatures" (No. 370-II, 7 January 2003), which serves as the legal foundation for exploiting electronic documents and digital signatures [22].

Although these legislative instruments provide the legal foundation for digital technologies and the protection of personal data, there is still no single unified standard governing the integration of biometric data into law enforcement systems. This highlights the need to modernise and enhance the legal framework further, including developing a standard approach for incorporating biometric information into public safety and forensic databases [22].

Kazakhstan's digital forensic and cybercrime response capabilities have drawn limited international attention, though recent engagement with the Council of Europe indicates growing interest in legal harmonisation. In April 2023, the country was officially invited to accede to the Budapest Convention on Cybercrime, reflecting its intent to strengthen cooperation in electronic evidence and cross border investigations [28]. However, Kazakhstan remains a nonparty to the Convention, which restricts its full participation in international legal frameworks for cybercrime and digital evidence handling. A 2024 evaluation conducted under the Council of Europe's Octopus Project noted positive institutional developments. For instance, while the establishment of national contact points and interagency cooperation mechanisms was recognised, shortcomings were identified in procedural legislation, institutional capacity development, and compliance with international standards [19]. These findings highlight the need for further legal reform and institutional investment to ensure Kazakhstan's digital forensic framework meets globally accepted norms.

The reliability and admissibility of digital evidence in Kazakhstan are significantly affected by legal, technical, and institutional challenges. The absence of specific procedural standards, coupled with vague legal definitions and limited judicial guidance, creates uncertainty in court proceedings. Technical issues such as inconsistent data handling practices and lack of forensic validation further compromise evidentiary integrity. Institutionally, the underdeveloped regulatory framework and lack of standardisation in areas like biometric data integration hinder effective implementation. Addressing these gaps is essential to ensure digital evidence can be used reliably and fairly in Kazakhstan's legal system.

Conclusion

This study intended to explore how digital evidence is collected, analysed, and used in Kazakhstan's criminal investigations. We found that Kazakhstan increasingly uses digital forensics, powered by surveillance technologies, artificial intelligence, and big data, for crime investigation and public safety. While this has strengthened the capacity to combat cybercrime and fraud, it is also used to monitor political dissent, raising concerns over civil liberties and state control. Smart city programmes and international partnerships have strengthened technical capacities; however, the dual-purpose application of digital forensics highlights its complex and at times contested position within Kazakhstan's legal system.

In addition, the study has identified a range of legal, technical, and institutional constraints that influence both the reliability and the admissibility of digital evidence. These include vague legislation, inconsistent procedures, weak evidentiary standards, and limited oversight on biometric data integration. Without reform, these weaknesses may undermine the fairness and legitimacy of legal proceedings involving digital evidence.

This study underscores the increasing dependence on digital forensic methods within Kazakhstan's criminal investigations, while also examining how smart surveillance infrastructures are deployed in ways that serve both public security objectives and mechanisms of political governance. By tracing the evolution of digital forensic technologies and their incorporation into policing and state administration systems, the study develops practical recommendations aimed at strengthening evidentiary integrity, improving standardisation, and enhancing transparency across law enforcement and judicial institutions.

The study contributes to the broader theoretical discourse on digital criminalistics in post-Soviet legal systems, offering a nuanced understanding of how digital evidence functions within hybrid regimes where technological modernisation coexists with authoritarian governance. It expands the conceptualisation of digital forensics as both a technical practice and a political instrument, contributing to debates on digital authoritarianism, techno-governance, and the rule of law in transitional states.

This study faced limitations in accessing comprehensive primary data, particularly regarding internal procedures, specific case examples, and statistical records of digital evidence use in Kazakhstani

courts. The research relies heavily on secondary sources and public documentation, which may not fully capture on-the-ground practices or informal mechanisms. Additionally, the absence of interviews with legal or forensic professionals limited the depth of institutional insight.

REFERENCES

1 Walcott S., Muir R. Unleashing the value of digital forensics (Commissioned by the Transforming Forensics Programme), London: The Police Foundation, 2021. URL: https://www.police-foundation.org.uk/wp-content/uploads/2010/10/value_of_digital_forensics.pdf (accessed: 28.03.2026)

2 INTERPOL. Global guidelines for digital forensics laboratories, Lyon: INTERPOL Global Complex for Innovation. 2019. URL: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf (accessed: 28.03.2026)

3 Petrenko E.S., Shevyakova A.L. Features and perspectives of digitization in Kazakhstan, Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT. 2019, pp. 889–899. DOI: 10.1007/978-3-030-13397-9_91 (accessed: 28.03.2026)

4 Stickings M., Nosal J. Blunting the cutting edge of crime: OSCE helps combat cybercrime in Central Asia [Blog post], Vienna: OSCE – Organization for Security and Co-operation in Europe. 2024. URL: https://www.osce.org/blog/574757 (accessed: 28.03.2026)

5 6Wresearch. Kazakhstan digital forensics market (2024–2030) [Market research report], 6Wresearch. 2024. URL:: https://www.6wresearch.com/industry-report/kazakhstan-digital-forensics-market (accessed: 28.03.2026)

6 Pollitt M. A history of digital forensics, Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4–6, 2010, Revised Selected Papers 6. 2010, pp. 3–15. DOI:10.1007/978-3-642-15506-2_1

7 Selim A., Ali İ. The role of digital forensic analysis in modern investigations // Journal of Emerging Computer Technologies. 2024, vol. 4, no. 1, pp. 1–5. DOI: 10.57020/ject.1445625

8 Dubey H., Bhatt S., Negi L. Digital forensics techniques and trends: a review // International Arab Journal of Information Technology. 2023, vol. 20, no. 4, pp. 644–654. DOI: 10.34028/iajit/20/4/11

9 Granja F.M., Rafael G.D.R. The preservation of digital evidence and its admissibility in the court // International Journal of Electronic Security and Digital Forensics. 2017, vol. 9, no. 1, pp. 1–18. DOI: 10.1504/IJESDF.2017.081749

10 Yeboah-Ofori A., Brown A.D. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence // Journal of Forensic, Legal & Investigative Sciences. 2020, vol. 6, no. 1, pp. 1–8. DOI: 10.24966/FLIS-733X/100045

11 Antwi-Boasiako A., Venter H. A model for digital evidence admissibility assessment, Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 30–February 1, 2017, Revised Selected Papers 13. 2017, pp. 23–38. DOI: 10.1007/978-3-319-67208-3_2

12 ISO/IEC. ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, Geneva: International Organization for Standardization. 2012. URL: https://www.iso.org/standard/44381.html (accessed: 28.03.2026)

13 ISO/IEC. ISO/IEC 27041:2015 – Information technology – Security techniques – Guidelines on assuring suitability and adequacy of incident investigative method, Geneva: International Organization for Standardization. 2015. URL: https://www.iso.org/standard/44445.html (accessed: 28.03.2026)

14 ISO/IEC. ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence, Geneva: International Organization for Standardization. 2015. URL: https://www.iso.org/standard/44446.html

15 Saniyazova Y., Mediyev R., Saitova E., Utegenova G., Kzylkhojayeva A. Advancing forensic science in Kazakhstan: the emergence and impact of digital forensics in cybercrime investigation, Law, State & Telecommunications Review / Revista de Direito, Estado e Telecomunicações. 2024, vol. 16, no. 2, pp. 48–68. DOI: 10.26512/lstr.v16i2.49190

16 Government of the Republic of Kazakhstan. On the approval of the Concept of digital transformation, development of the information and communication technology industry, and cybersecurity for 2023–2029 (Resolution No. 269). Әділет. 2023. URL: https://adilet.zan.kz/rus/docs/P2300000269 (accessed: 28.03.2026)

17 Minister of Justice of the Republic of Kazakhstan. Order No. 484 on approval of the Rules for the organization and conduct of forensic examinations and research in forensic examination agencies. 2017. URL: https://adilet.zan.kz/rus/docs/V1700015180 (accessed: 28.03.2026)

18 Council of Europe. Joining the Convention on Cybercrime: Benefits (Version 1). 2025, URL: https://rm.coe.int/cyber-buda-benefits-2025-1-april-en/1680b51696 (accessed: 28.03.2026)

19 Council of Europe. Octopus Project: Authorities of Kazakhstan coordinate on the next steps to complete accession to the Convention on Cybercrime. 2024. URL: https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime (accessed: 28.03.2026)

20 Yin R.K. Case study research and applications: design and methods, 6th ed., Thousand Oaks, CA: Sage. 2018, 352 p. URL: https://collegepublishing.sagepub.com/products/case-study-research-and-applications-6-250150 (accessed: 28.03.2026)

21 Turgel I., Bozhko L., Ulyanova E., Khabdullin A. Implementation of the smart city technology for environmental protection management of cities: the experience of Russia and Kazakhstan // Environmental and Climate Technologies. 2019, vol. 23, no. 2, pp. 148–165. DOI: 10.2478/rtuect-2019-0061

22 Doszhanova A.B., Begaliyev Y.N. Information and communication technologies of the "Smart City" in the system of identification: forensic aspect // Bulletin of the Karaganda University "Law Series". 2025, vol. 30, no. 2(118), pp. 125–133, DOI: 10.31489/2025L2/125-133

23 Amnesty International. Think before you post: Closing down social media space in Kazakhstan (EUR 57/5644/2017). 2017. URL: https://www.amnesty.org/en/documents/eur57/5644/2017/en/ (accessed: 28.03.2026)

24 Amnesty International. Kazakhstan: Authorities must drop politically motivated charges against satirical blogger, Amnesty International. 2025. URL: https://www.amnesty.org/en/latest/news/2025/02/kazakhstan-authorities-must-drop-politically-motivated-charges-against-satirical-blogger/ (accessed: 28.03.2026)

25 Lakbayev K.S., Rysmagambetova G.M., Umetov A.U., Sysoyev A.K. The crimes in the field of high technology: concept, problems and methods of counteraction in Kazakhstan // International Journal of Electronic Security and Digital Forensics. 2020, vol. 12, no. 4, pp. 412–423. DOI: 10.1504/IJESDF.2020.110651

26 Adanbekova Z.N., Omarova A.B., Yermukhametova S. R., Khudaiberdina G.A., Tynybekov S.T. Features of the conclusion of a civil transaction on the internet // International Journal of Electronic Security and Digital Forensics. 2022, vol. 14, no. 1, pp. 19–36. DOI: 10.1504/IJESDF.2022.120035

27 Beisbekova G.K., Konussova V.T., Ismagulov K.E., Saktaganova I.S., Mukasheva A.A. Problems of concretization of legal norms in Kazakhstan // Journal of Advanced Research in Law and Economics. 2019, vol. 10, no. 1(39), pp. 52–57. DOI: 10.14505//jarle.v10.1(39).07

28 Council of Europe. Kazakhstan invited to accede to the Budapest Convention on Cybercrime, Council of Europe. 2023. URL: https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/id/216084174 (accessed: 28.03.2026)

ТЕМІРБОЛАТ Н.С.,[*1]
з.ғ.к., аға оқытушы.
[*]e-mail: nuraishamail@gmail.com
ORCID ID: 0000-0002-8447-5753
МЕЙРКУЛОВА Г.Д.,[2]
з.ғ.к., аға оқытушы.
e-mail: adil.96-96@mail.ru
ORCID ID: 0000-0001-7359-0601
[1]әл-Фараби атындағы ҚазҰУ,
Алматы қ., Қазақстан
[2]М. Әуезов атындағы ОҚУ,
Шымкент қ., Қазақстан

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ІСТЕРДІ ТЕРГЕУДЕГІ ЦИФРЛЫҚ КРИМИНАЛИСТИКАНЫҢ РӨЛІ

Аңдатпа

Бұл зерттеу Қазақстандағы қылмыстық істерді тергеуде цифрлық криминалистиканың рөлін қарастырады. Негізгі назар бейнебақылау жазбалары, мобильді деректер мен әлеуметтік желілер мазмұны сияқты цифрлық дәлелдемелердің жиналуына, талдануына және қолданылуына аударылады. Саясаттық құжаттар, істер мысалдары және құқықтық негіздерге сүйене отырып, зерттеу қадағалау технологияларының, жасанды интеллект пен үлкен деректердің қылмыстың алдын алуда да, сонымен қатар мемлекеттік бақылауда да кеңінен қолданылуын көрсетеді. Цифрлық криминалистика киберқылмыс пен алаяқтықпен күресу мүмкіндіктерін арттырғанымен, оны саяси көзқарастарды бақылауда пайдалану азаматтық бостандықтарға қатысты алаңдаушылық туғызады. Сондай-ақ зерттеу сотта цифрлық дәлелдемелердің сенімділігі мен

қабылдануына әсер ететін негізгі құқықтық, техникалық және институционалдық мәселелерді айқындайды. Олардың қатарында заңнаманың бұлыңғырлығы, рәсімдердің бірізді болмауы және реттеушілік бақылаудың жеткіліксіздігі бар. Бұл мақала өтпелі құқықтық жүйелердегі цифрлық криминалистикаға қатысты пікірталастарға әрі практикалық, әрі теориялық үлес қосады. Дәлелдемелік стандарттарды жетілдіру, құқықтық реформалар жүргізу және институционалдық әлеуетті арттыру бойынша ұсыныстар берілген. Сонымен бірге цифрлық криминалистикалық тәжірибелердің ашықтығын және этикалық бақылауды күшейту қажеттілігі атап өтіледі.

Тірек сөздер: цифрлық криминалистика, криминалистика, ақылды қалалар, электрондық дәлелдемелер, жасанды интеллект, киберқылмыс.

ТЕМІРБОЛАТ Н.С.,[*1]
к.ю.н., ст. преподаватель.
[*]e-mail: nuraishamail@gmail.com
ORCID ID: 0000-0002-8447-5753
МЕЙРКУЛОВА Г.Д.,[2]
к.ю.н., ст. преподаватель.
e-mail: adil.96-96@mail.ru
ORCID ID: 0000-0001-7359-0601
[1]КазНУ им. аль-Фараби,
г. Алматы, Казахстан
[2]ЮКУ им. М. Ауезова,
г. Шымкент, Казахстан

РОЛЬ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В УГОЛОВНЫХ РАССЛЕДОВАНИЯХ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

В исследовании рассматривается роль цифровой криминалистики в уголовных расследованиях Казахстана, с акцентом на то, как собираются, анализируются и используются цифровые доказательства, такие как записи с камер видеонаблюдения, данные мобильных устройств и контент социальных сетей. На основе анализа нормативных документов, примеров из практики и правовых рамок подчеркивается расширяющееся применение технологий наблюдения, искусственного интеллекта и больших данных как в предотвращении преступлений, так и в обеспечении государственного контроля. Хотя цифровая криминалистика повышает возможности борьбы с киберпреступностью и мошенничеством, ее использование для мониторинга политического инакомыслия вызывает обеспокоенность в отношении гражданских свобод. В исследовании также выявлены основные правовые, технические и институциональные проблемы, влияющие на достоверность и допустимость цифровых доказательств в суде, включая расплывчатость законодательства, непоследовательность процедур и недостаточный регуляторный контроль. Работа вносит как практический, так и теоретический вклад в обсуждение цифровой криминалистики в переходных правовых системах. В качестве рекомендаций предлагается совершенствование стандартов доказательств, проведение правовой реформы и укрепление институционального потенциала, а также повышение прозрачности и этического контроля в области цифровой криминалистики.

Ключевые слова: цифровая криминалистика, криминалистика, умные города, электронные доказательства, искусственный интеллект, киберпреступность.

Article submission date: 15.04.2026