Advancing Forensic Science in Kazakhstan: The Emergence and Impact of Digital Forensics in Cybercrime Investigation

Submitted: 19 June 2023
Reviewed: 5 July 2023
Revised: 14 November 2023
Accepted: 7 February 2024

Article submitted to peer blind review

Yerkemay Saniyazova[*]
https://orcid.org/0000-0001-9714-8631
Renat Mediyev[**]
https://orcid.org/0009-0000-3142-5309
Elmira Saitova[***]
https://orcid.org/0000-0002-1568-2636
Gulzat Utegenova[****]
https://orcid.org/0009-0004-1279-4271
Aisaulem Kzylkhojayeva[*****]
https://orcid.org/0009-0009-4364-0204

DOI: https://doi.org/10.26512/lstr.v16i2.49190

Abstract

[Purpose] The purpose of the article was to study digital forensics, its role in the Kazakh legal system and the process of investigating cybercrime.

[Methodology] Analysis, synthesis, comparison, deduction, generalization, abstraction, formal legal methods of scientific research were used.

[Findings] A result, it was proved that forensics is an indispensable component of the future development of forensic science in Kazakhstan. It has been established that digital forensics enables speeding up the process of solving cybercrimes, as well as determining their sources and prerequisites. Thus, on the basis of forensics, it is possible not only to identify the problem, but also to form a mechanism for overcoming it in the future. This determines the priority of professional training of forensic experts for future work with digital evidence, traces and their use in the trial. In addition, the areas of activity of law

[*]Department of Criminal Procedure and Forensic Science, Kyrgyz National University named after Jusup Balasagyn, 720033, 547 Frunze Str., Bishkek, Kyrgyz Republic. Email: yerkemaysaniyazova@yahoo.com.
[**]Department of Special Legal Disciplines, Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, 021804, 94 Republic Str., Kosshy, Republic of Kazakhstan. Email: renat.mediyev@proton.me.
[***]Department of Law, Kazakh-Russian International University, 030006, 52 Aiteke bi Str., Aktobe, Republic of Kazakhstan. Email: Elmira_Saitova@outlook.com.
[****]Department of Jurisprudence, Korkyt Ata Kyzylorda University, 120000, 29A Aiteke bi Str., Kyzylorda, Republic of Kazakhstan. Email: Gulzat11utegenova@protonmail.com.
[*****]Department of Jurisprudence, Institute of State and Law of the National Academy of Sciences of the Kyrgyz Republic, 720033, 265A Chui Ave., Bishkek, Kyrgyz Republic. Email: A.Kzylkhojayeva@hotmail.com.

SANIYAZOVA, Y.; MEDIYEV, R.; SAITOVA, E.; UTEGENOVA, G.; KZYLKHOJAVEVA, A. *Advancing Forensic Science in Kazakhstan: The Emergence and Impact of Digital Forensics in Cybercrime Investigation*. **The Law, State and Telecommunications Review**, v. 16, no. 2, p. 48-68, October 2024.

enforcement agencies has been established, in which forensics plays an important role and is mandatory for use.

Keywords: Digital Forensic Methodologies. Kazakhstan Cybercrime Legislation. Forensic Science Evolution. Cybersecurity Legal Implications. Technological Evidence Analysis.

INTRODUCTION

Over time, the needs of law enforcement agencies in the search, identification, and analysis of digital evidence are increasing. This issue is especially relevant in the field of forensic science and its digital development. In the current model of forensic science in Kazakhstan, forensics is at the stage of its inception, which leads to the formation of an independent branch of forensic technology. Its structure includes tools and approaches for the study of digital evidence. Based on this, the issue of effective integration of the provisions of digital forensics (involves the collection, analysis, and preservation of digital evidence obtained from computers, networks, and storage media. This evidence is then used in investigations and legal proceedings) into the current legal system of Kazakhstan becomes relevant. This process does not require an absolute reform of the system itself, while at the same time contributing to the rapid implementation of the doctrinal provisions and practical recommendations of forensics (ALGHAMDIL, 2021; CHORNOUS and LELIUK, 2023).

In the modern legal environment, the content of forensic technology concerns both digital forensics in the context of forensic sciences and investigative approaches adapted to the current Kazakh law enforcement practice. Based on this, there is a need to compare modernised and traditional methods of detecting cybercrime in order to increase the protection of information security (the processes and tools used to prevent unauthorized access, misuse, disclosure, disruption, modification, inspection, recording or destruction of information) as well as prevent cyberattacks. Cybercrime - criminal activity that involves the use of computers, networks, programs, and data (AMATO et al., 2020).

The relevance of the study is due to the fact that the global use of digital tools and media has provoked a transformation in the approaches and subjects of many criminal offenses. This is due to the priority role of information technology in all areas of human life. Accordingly, in modern society, each person owns and uses several digital tools as well as digital services. All this provokes the emergence of a wide range of digital footprints that are important in the course of investigating cybercrime (METELSKYI and KRAVCHUK, 2023; MENTUKH and SHEVCHUK, 2023). The priority for today is not only their identification but also a qualitative study so that they can be used in the course of criminal proceedings. That is why the training of specialists in the field of digital forensics deserves

special attention, since, in accordance with the level of development of the human resource, a certain object, in particular forensic science, is popularised (QADIR and VAROL, 2020).

The use of digital forensics offers several advantages in investigating and prosecuting cybercrimes. Firstly, it allows for the collection and analysis of much larger volumes of evidence, given the digital traces left behind in computer systems, networks, and electronic devices. Additionally, digital forensics enables faster evidence gathering, instead of relying on manual processes. Secondly, the scientific rigour of digital forensic tools and examination protocols helps to validate and authenticate digital evidence, making it more credible in legal proceedings. This also allows crucial evidence to be recovered, even if a suspect has attempted to delete or destroy it. Thirdly, as cybercrimes become more technologically complex, digital forensics provides law enforcement with the capabilities to unpack these crimes and attribute them to specific perpetrators through technical attribution. Finally, the integration of advanced digital forensics techniques, such as network pattern analysis, enables investigators to efficiently link multiple crimes to common suspects. This results in both increased efficiency and stronger evidence for pursuing cybercriminals who can otherwise anonymously commit crimes across jurisdictions.

Based on the foregoing, the problem of the scientific paper was to study the features of forensics and its advantages in the use of law enforcement officers in the fight against cybercrime. Despite the fact that digital forensics has just begun to spread in Kazakh society, there are a number of scientific papers that reveal its various aspects. C. Karagiannis and K. Vergidis (2021), V.R. Silvarajoo et al. (2021) believe that digital footprints must be traced using digital search and fixation tools in cyberspace, in particular by forensic experts. This conclusion allows establishing that digital materials and evidence should be involved in the process of proof during criminal proceedings in relation to cybercrimes. In turn, I.V. Borysenko et al. (2021) and D. Sun et al. (2021) focused on the characteristics of computer-based forensics as a technique for combating cybercrime. The explored position allows concluding that digital forensics is a separate discipline, and therefore is not closely related to forensic sciences and techniques. E.S. Kemali and S.K. Zhursimbaev (2020), and also E.A. Altaev et al. (2023), described the current level of development of forensics in the Kazakh legal environment. They revealed the high priority of this area and the difficulties in the course of its implementation, links with traditional approaches in forensic science. Such a conclusion is necessary for use in the article directly when describing the Kazakh experience and the priority of attracting tools for working with digital evidence to it.

Currently, Kazakhstan's criminal code lacks specific provisions for classifying and penalising various cybercrimes, which poses significant challenges in

addressing these modern offenses. While general criminal offences like fraud and illegal access to information could potentially cover aspects of cybercrime, the absence of explicit legal guidelines for cyber-specific activities such as data privacy breaches leaves a substantial gap in legal clarity. Notably, there have been efforts to introduce new legislation that aims to incorporate detailed cybercrime provisions into the criminal code (BAZILOVA et al., 2016). However, these proposed changes have not yet been enacted into law. This legislative shortfall presents notable difficulties in prosecuting cybercrimes effectively and applying digital forensics, as the legal system currently does not have a clear framework to rely on for these technologically advanced crimes. The progression of such legislation would be a crucial step in enhancing Kazakhstan's capability to combat and prosecute cybercrimes effectively.

This paper aims to contribute to the understudied topic of digital forensics capabilities in Kazakhstan. It provides a comprehensive overview of the emergence and current state of digital forensics in the country, establishing baseline knowledge where limited literature exists. Additionally, the paper offers an original analysis of how digital forensics integrates with Kazakhstan's existing legal frameworks and forensic science institutions. Thirdly, it identifies the specific limitations and gaps in Kazakhstan's digital forensics ecosystem while proposing concrete policy and technical recommendations for stakeholders. Additionally, the paper highlights the urgent need to develop Kazakh expertise and capacity in advanced digital forensics to combat escalating cybercrime. Finally, this paper provides a foundation for further research on strengthening Kazakhstan's cybersecurity (the practice of safeguarding computer systems, servers, mobile devices, electronics, networks, and data from unauthorized access or attacks) and rule of law by detailing the local context and applications of digital forensics. The lack of scholarship on digital forensics in Kazakhstan makes this paper a timely and locally grounded contribution to the field, providing insights for both researchers and policymakers. Thus, the goal of the scientific paper was formed, which was to study a new vector of forensic science, namely forensics, in the process of investigating cybercrime. The tasks were also formed to:

- Reveal the concept of forensics, to determine its tasks and functions;
- Describe the areas of use of digital forensics;
- Study the current level of cybercrime in Kazakhstan;
- Consider priority areas for the development of forensics in Kazakhstan;
- Establish the role of digital forensics in the fight against cybercrime.

The practical value of the results obtained lies in the fact that it has both doctrinal significances in the context of establishing the essence and functions of digital forensics, and practical in relation to the development of recommendations for its integration into the Kazakh legal environment.

MATERIALS AND METHODS

The method of analysis was used in the paper to divide the general object of study into separate components. In particular, the article analysed such components as computer forensics, digital evidence, cybercrime, and the cybercrime investigation process. On its basis, the structure of the object and the subject of this scientific paper were studied. Also, the analysis method was used to study statistical data regarding the dynamics of the development and spread of cybercrime in Kazakhstan. In addition, this method was used to analyse data on the activity of using forensics by Kazakh law enforcement agencies in the course of investigating such types of illegal actions.

The synthesis method was used in the research to study the essence of forensics in the context of combating cybercrime. This method involved combining the components separated during the analysis into a single whole, specifically the object of the article. Due to the synthesis, there was an improvement in the understanding of the topic of the paper, the relationship between its elements, as well as the disclosure of the characteristic features of digital forensics.

The method of comparison was used in a scientific paper to compare various structures and objects to determine their common and distinctive features, as well as the nature of their interaction. This method formed the basis of the process of researching the fundamental features of forensics and the traditional principles of forensic science in Kazakhstan. The comparison enabled an assessment of the advantages of digital forensics in light of current challenges, particularly the widespread occurrence of cybercrime. Based on this method, the functions and tasks of digital forensics were studied in comparison with traditional approaches.

The deduction method was applied in the article to describe and evaluate the essence of forensics based on knowledge about the general tasks of forensic science. This method was used in the course of expressing the specific properties of digital forensics by understanding the traditional system of forensics in Kazakhstan.

The method of abstraction was applied in this scientific paper to a separate description of forensics as a science and academic discipline. This method is necessary to describe the properties and principles of digital forensics without taking into account the peculiarities of national legislation and other factors. Abstraction contributed to the formation of understanding and the role of forensics in modern

digital society. In addition, on the basis of this method, digital forensics was expressed as a priority method for combating cybercrime.

The use of the formal-legal method in the paper was due to the belonging of the topic of the article to the legal circle. Based on this, this method was applied to interpret legal concepts and mechanisms as well as study the provisions of regulations. In the course of revealing the types of cybercrime, the norms of the Criminal Code of the Republic of Kazakhstan (2014) were studied.

The generalisation method was used to identify the benefits of forensics in the context of cybercrime investigation methods. Based on it, recommendations were formed aimed at improving the existing structure of forensic science in Kazakhstan, taking into account digitalization processes. Generalisation was necessary to express the main tasks and functions of forensics, as well as approaches to its implementation directly in Kazakhstan.

RESULTS

The active development of information technologies is reflected in various spheres of public life. Moreover, these processes also reform established mechanisms, such as those for receiving and transmitting confidential information. At present, due to modern approaches based on elements of sociology, psychology, and information technology, the Institute of Social Engineering makes it possible to improve computer security and expand its functionality. Unfortunately, the development of information technology not only positively affects the subjects of society but also negatively. This is expressed in the fact that modern criminals are beginning to commit more criminal offences on the Internet. This is also evidenced by statistical data for the last ten years (Figure1).

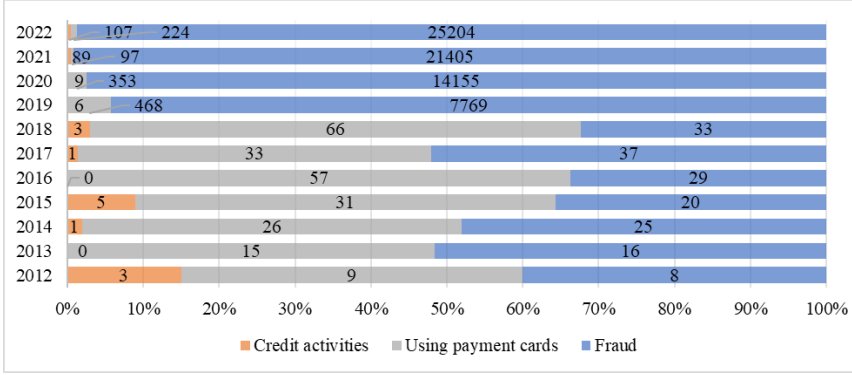

Chart 1 – Number of Registered Cybercrimes in Kazakhstan
Source: How Kazakhstanis are Deceived by Internet Scammers (2022).

Based on the data described, it can be established that the implementation of modern mechanisms in the IT sphere contributes to the formation of new social relations, which in turn are the subject of cybercrime (JARRETT and CHOO, 2021). The basis of cybercrimes, according to the current criminal legislation of Kazakhstan, are socially dangerous acts provided for by Clause 4 of Part 2 of Art. 190 of the Criminal Code of the Republic of Kazakhstan (2014). According to the approaches of criminal law, it is advisable to classify as cybercrime only those criminal offences that are provided for in the above chapter of the Criminal Code. However, within the framework of forensics, this category of illegal acts also includes other offences for which a computer and the Internet are used (for example, Clause 4 of Part 2 of Art. 190 of the Criminal Code of the Republic of Kazakhstan (2014)). This is explained by the fact that the method of committing such an act is associated with the introduction of a person into information systems, which is specifically related to cybersecurity issues. Special attention should be paid to the crime solution rate in the field of information and communications, which, according to statistical data, is unsatisfactory (Figure 2).

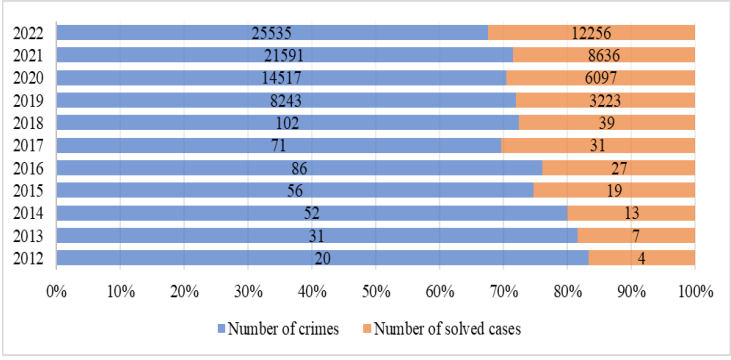

Chart 1 – Ratio of the Number of Crimes and Solved Criminal Cases in the field of Informatisation and Communications
Source: How Kazakhstanis are Deceived by Internet Scammers (2022).

Given the current level of development of society, it can be established that for a person to commit a criminal offence, they will need only a computer. In particular, the theft of money in modern conditions can occur at the expense of software and hardware, telecommunications technologies, the Internet. The concept of cybercrime should be understood as a set of illegal acts carried out in cyberspace through the use of computer systems, computer networks, as well as other tools for accessing cyberspace. The object and essence of this type of criminal offences do not change, but the means and methods are developing, which

expands the number of approaches to committing criminal offenses. As a result, a separate chapter in forensics was formed, which is aimed at studying and preventing cybercrime, namely computer forensics.

Digital forensics in Kazakhstan is vital across various sectors, including law enforcement, corporations, and the military. It's used for investigating cybercrimes like hacking and financial fraud, probing internal corporate breaches, scrutinising insurance fraud, protecting intellectual property rights, and ensuring national cybersecurity. This field is rapidly integrating into Kazakhstan's criminal justice system, with a focus on modernising forensic techniques and training specialists. The proactive adaptation of digital forensics reflects its growing significance in crime detection and prevention, highlighting its role in securing justice and safety in the digital age.

Several notable advancements and initiatives have been made in Kazakhstan to integrate digital forensics within the criminal justice system. Unfortunately, there is limited publicly available information on specific success stories of digital forensics applications in Kazakhstan. However, some noteworthy points on the impact of digital forensics in the country are:

- The forensic science model in Kazakhstan is currently undergoing modernisation, resulting in the creation of a dedicated branch for digital forensics. This branch focuses on the use of tools and methods for studying digital evidence, specifically for investigating cybercrime. The modernisation process emphasises the introduction of scientific development and practical recommendations relevant to cybercrime investigations.

- Digital forensics plays a crucial role in operative investigative activities in Kazakhstan. It is used in the identification of signs of wrongful acts during pre-trial investigations. Experts use digital tools in both covert and overt investigative actions to identify and collect digital evidence. This approach distinguishes digital forensics as a separate industry, focusing on the investigation of criminal offenses involving digital devices, networks, and information.

- In recent years, Kazakhstan's law enforcement has reportedly been able to solve several cases of fraud, illegal access to computer systems, and distribution of malicious software with the help of digital forensic analysis. Though details are scarce, these are being cited as examples of the importance of digital forensics.

- In 2021, Kazakhstan's Ministry of Internal Affairs launched the Centre for Computer Forensics and Investigation of Cyber Attacks (TSARKA).

This dedicated facility applies advanced digital forensic tools to investigate cybercrimes. Its establishment demonstrates the priority given to digital forensics capabilities (Khusanov, 2022).

- Kazakhstan is also expanding training partnerships with international agencies like Europol to increase its digital forensics knowledge and adoption. Workshops conducted have focused on cyber-investigative techniques.

- Growing cybercrime statistics and low-resolution rates in the past have driven Kazakhstan to strengthen its digital forensics capacities. The number of solved cases is seen as a metric of success.

- Digital forensics plays a crucial role in operative investigative activities in Kazakhstan. It is used in the identification of signs of wrongful acts during pre-trial investigations. Experts use digital tools in both covert and overt investigative actions to identify and collect digital evidence. This approach distinguishes digital forensics as a separate industry, focusing on the investigation of criminal offences involving digital devices, networks, and information.

- Positive outcomes in investigations utilising digital forensics have helped highlight resource gaps for legislators and policy makers. This has led to increased budget allocations for advancing forensic tools and training personnel.

These advancements and initiatives demonstrate Kazakhstan's proactive approach to integrating digital forensics into the criminal justice system. The focus is on both technological development and professional training. Digital forensics has been successful in facilitating prosecutions, reinforcing its reputation as a 'force multiplier' for Kazakhstan's law enforcement. This has led to greater institutional support and systematic adoption, despite the confidentiality of specific details of landmark cases. Although the country still has a long way to go, early successes have encouraged further investment in this crucial capability.

Forensics, also called digital forensics, is an applied science that studies the peculiarities of the analysis and investigation of cybercrime (KAVRESTAD, 2020). Its subject is the methods of obtaining and examining evidence. Forensics is responsible for the reasonable collection and analysis of materials in information systems, as well as communication flows, database management systems, or the systems for storing information in a certain order. Based on the above concept, it is advisable to divide computer forensics into two categories: digital and

network. The first is implemented in the process of meeting the needs of law enforcement agencies, for example, in the course of providing reliable evidence necessary for the solution of cybercrimes. Network forensics originated and spread in the course of preventing and countering hacker threats; therefore, it is associated with the architecture of information security. The latter includes risk analysis, detection of interference in the information structure, prevention of modification, and organisation of covert investigative actions on information.

The forensic expert works with evidence and data in the form of computer information, both regular and incidental. Such materials can easily be deformed or destroyed. Identification of digital evidence tampering is possible both by the content of the materials and by traces in other places belonging to the category of information. It should be noted that digital evidence can be explored and studied only at the expense of hardware and software that are complex in structure. This factor makes it difficult to demonstrate evidence and maintain its original invariability during storage. In order to determine the advantages of forensics in forensic science and its role in the process of solving cybercrime, its main tasks and functions should be determined. Digital forensics contributes to the development of tactics for operative investigative activities as well as investigative actions related to computer information. Also, this science is responsible for the creation of methods, approaches, and tools designed to collect and evaluate cybercrime evidence. Forensics carries out the establishment of forensic signs of illegal acts related to computer data and materials. As for the scope of digital forensics, its principles are important for the investigation of cybercrime. In addition, this science is used in the collection and evaluation of evidence, for example, in cases of infringement of intellectual property rights, i.e., the object of these rights appears in the form of computer information. Forensics is an important part of insurance investigations carried out by insurance companies, for example, in relation to breaches of contract. This is especially true when the object of insurance is an information system. Forensics can be used in the field of internal corporate investigations of security breaches directly related to information systems. It can also be implemented when taking measures to prevent the leakage of data containing confidential information.

Separately, it should be noted that digital forensics is used by the military in the course of performing intelligence tasks to identify, eliminate, or restore computer materials. An example is the impact on the information systems of the enemy and the protection of own systems. Since forensics is a science, there are methods on the basis of which its implementation is possible. These include observation, measurement, description, comparison, experiment, modelling, explanation, analysis, synthesis, and forecasting. The listed methods can be used separately or in combination in the course of digital forensics. Some features of the

application of forensic methods, such as observation, should be noted. This is explained by the fact that the main object of research in this science is computer data, which in principle cannot be observed by a person specifically. Therefore, in the course of solving cybercrime, this method is used in a peculiar way, taking into account changes in computer information. In addition to the general scientific research methods described above, forensics is also characterised by some special ones. The latter include the formation and implementation of specialised forensic information systems; modifying them for the purpose of using them for own purposes. Also, digital forensics techniques are used in the installation or evaluation of evidence in public search engines (such as Google) and special purpose search engines that are used by law enforcement agencies. The specificity of forensics in the context of cybercrime investigation lies in the possibility of developing a virtual subject and carrying out operative activities, undercover work. The advantage of this approach in forensic science is the possibility of high-quality collection and systematisation of the hash functions of known files, for example, to separate them from documents containing original personal data or, vice versa, modified information. Forensics implementation methods allow archiving unlimited content of media for research and use in the course of an investigation.

One of the most common approaches to using digital forensics is to simulate Internet network services to study the behaviour of suspicious software. The development of forensics in forensic science is impossible without the involvement of highly qualified specialists. Field experts play an important role in identifying and evaluating information security offences (SUNDE and DROR, 2021). Examples of the latter include hacking websites, stealing confidential information contained on digital media, as well as encrypting such data. As a result of identifying these processes, forensic experts perform a set of tasks using forensics. These include establishing a way to implement hacking, the development of an attack algorithm, attack sequence simulation, collection and systematisation of attack traces, and the reduction or restoration of the damage caused. In addition, forensics experts need to develop and implement the necessary measures to protect information in the appropriate environment in order to increase the level of information security in the industry that has suffered losses. However, the described list of activities of cybercrime investigation experts using the basics of forensics is not exhaustive. This is explained by the fact that their tasks also include the development of an expert opinion on the offense committed regarding interference in the information security of various objects and areas. As a result, forensic science is developing in general, which contributes to an increase in the cybercrime solution rate. In Kazakh forensic science, computer forensics is a relatively new vector. Despite this, it is characterised by rapid development, which

contributes to the implementation of a thorough collection and evaluation of electronic evidence by law enforcement agencies. As a result of the use of forensic tools by forensics experts, not only a qualitative assessment of the amount and nature of the damage caused by an electronic attack occurs but also the restoration of lost data (AUBARIKOVA et al., 2022). This contributes to the acceleration of the process of identifying an offender, as well as evidence indicating the guilt of this person in the committed wrongful act. Based on the foregoing, it can be established that the modern Kazakh model of investigating criminal offences is characterised by the use of tools and approaches of digital forensics. Especially relevant is the use of forensic science during operative investigative activities, as well as the identification of signs of a wrongful act even at the stage of pre-trial investigation. Thus, digital tools are used by experts in the preparation and conduct of covert and overt investigative actions aimed at identifying and collecting digital evidence (WU et al., 2020).

At the same time, it is important to clearly distinguish between the digitalization of forensics and digital forensics. Since the first concept reveals a natural method of introducing digital tools into various areas of forensic technology and forensic examination (the scientific process of analysing and interpreting digital evidence to understand a crime and link suspects. It follows standardized procedures) (DU et al., 2020; CHUKAIEVA and MATULIENĖ, 2023). In turn, digital forensics in Kazakhstan is currently a separate industry that aims at studying digital devices, networks, and information directly in the course of the investigation of criminal offences, in particular cybercrimes. Given this, it should be noted that the existing model of forensic science in Kazakhstan is undergoing modernization, which is expressed in the gradual formation of a separate branch of forensic technology, which involves the use of tools and methods for the study of digital evidence. Currently, digital forensics is being integrated into the Kazakh system of forensics, which in turn does not require an absolute reform of the system itself. To a greater extent, this process is aimed at the introduction of scientific development and practical recommendations for the investigation of cybercrime. At the same time, it is advisable to attribute some of the principles of forensics to forensic tactics, namely, the processes of extracting information from electronic communication networks and information systems, as well as to methods, for example, for certain methods of investigating cybercrimes. Despite this, the basis of digital forensics is still technical and forensic in nature.

Attribution to the Kazakh digital forensics of technical issues for the investigation of criminal acts committed in cyberspace using digital intelligence methods is possible in the context of the formation of a separate branch of forensic technology. For example, there are other types of forensic technology that affect both forensic tactics and the methodology for investigating specific types of

crimes. In particular, the principles of forensic ballistics are implemented in the methodology for investigating wrongful acts committed with the use of firearms. Based on the above example, it can be established that the forensic evaluation of digital evidence, including electronic media, computer data, and digital materials, is experiencing particular development in forensic science in Kazakhstan while influencing the list of forensic tactics and methods of law enforcement agencies.

The practice of organising and conducting examinations based on forensics is widespread in Kazakhstan (Forensic Kazakhstan, 2022). Its end result is an opinion, in which the expert notes the subject of the research, the methods and tools that were used during this procedure. Since the examination will be carried out by special subjects with the necessary level of skills and experience, it should be noted that its results can be transferred to arbitration and ordinary courts. In this case, the expert opinion is evidence and is presented in the form of a written document. Thus, the presentation of an independent examination in a lawsuit may prompt the court to order a forensic examination. Based on the foregoing, it can be established that forensics originated and is developing in Kazakhstan to investigate computer and digital crimes. It is expedient to refer to the current structure: digital forensics, network forensics, forensic information analysis, hardware, and technical support.

To fully integrate digital forensics into criminal investigations and prosecutions in Kazakhstan, it is recommended that several legal reforms be implemented. Firstly, the criminal code and procedural laws should be updated to align with the realities of cybercrime and digital evidence, providing clear statutes on offenses and evidence collection and use. Secondly, to ensure the admissibility of digital evidence and its probative value, it is necessary to modernise evidentiary laws and establish guidelines, modelled on other jurisdictions. Additionally, it is crucial to implement comprehensive protocols for the proper seizure, storage, and analysis of digital evidence in law enforcement, following best practices. Furthermore, judges, lawyers, and investigators involved in cases must receive improved training on digital forensics fundamentals.

Kazakhstan is currently experiencing a significant shortage of skilled professionals in the field of digital forensics, emphasising the urgent need for capacity building in this specialised area. This gap is particularly evident due to the lack of specialised digital forensics training programs in universities and vocational institutions. To address this issue, strategic partnerships between the government and international forensics organisations are necessary to introduce advanced training and certification programs in Kazakhstan. Incentives, such as scholarships and defined career paths, could motivate students and professionals to pursue digital forensics expertise. It is essential to establish comprehensive digital

forensics curricula at Kazakh universities, covering both technical skills and legal/ethical aspects. In addition, continuous professional development is essential to keep up with technological advancements. Ministries should offer internal training for law enforcement and legal professionals. It is also recommended to establish professional associations for digital forensics practitioners in Kazakhstan to promote a collaborative exchange of knowledge and standards.

Therefore, in order to advance forensics in Kazakhstan and enhance forensic science, it is necessary to reform the training of specialists in this field. This can be achieved by incorporating digital forensics as a fundamental and mandatory academic discipline in higher education institutions under the Ministry of Internal Affairs of the Republic of Kazakhstan. As a result, students are expected to acquire not only new knowledge and skills but also the ability to promptly and effectively solve cybercrime. This will enable the development of tools for obtaining, processing, and analysing digital evidence by specialists.

DISCUSSION

Since forensics is a new direction in Kazakh criminalistics, it accordingly arouses particular interest in itself from scientists. The positions of researchers are not unanimous since they contain both similar and distinctive features. This allows revealing the role and essence of forensics in forensic science, in particular, in the process of investigating cybercrime.

For example, G.M. Jones and S.G. Winster (2022) and also N. Moustafa (2022) studied the historical origins of digital forensics in foreign practice. They argue that the birth of this science took place in the early 1970s, namely, during the spread of information databases. The rapid development of forensics occurred precisely in 1985, which was caused by the intensification of the development and introduction of computers in various spheres of public life. Already at that time, computer technology specialists were given access to internal systems and equipment through special codes (DANYLKOVYCH et al., 2023). Therefore, researchers believe that by that time, it became clear that digital technologies would be actively used by criminals. In response to this, the branch of digital forensics began to develop in order to counter the challenges to society that concerned the emergence and development of computer crime. The researchers note that since then, a number of effective technical and forensic tools have been formed, aimed not only at detecting, but also investigating cybercrime. This conclusion has common features with the results obtained in the course of this research. This is expressed in the description of the connection between the emergence of digital forensics and the use of cyberspace by criminals to commit criminal offences.

A similar opinion is shared by F. Casino et al. (2022) and J.P. Yaacoub et al. (2022), who interpreted the concept of "forensics". In their opinion, it is an

integral part of the forensic sciences and represents a system of scientific methods for storing, collecting, verifying, identifying, analysing, interpreting, documenting, and presenting digital evidence taken from digital sources. The ultimate goal of its use is to investigate illegal events in cyberspace. At the same time, the researchers note that forensics has an inherent multidisciplinary and interdisciplinary nature. This allows effectively implementing its elements in other activities of law enforcement agencies. As for the connection with forensic sciences, namely the dependence of the technical aspects of the study of digital evidence and the organisational and legal aspects of the solution of cybercrime, the researchers believe that it is not perfect. This is due to the fact that there are significant disagreements between technical specialists and legal practitioners that affect the understanding of digital forensics methods. The researchers noted that the technical procedures in forensics have a complex structure, which necessitates the training of highly qualified specialists. Based on this, in order to successfully harmonise digital forensics with the traditional principles of forensic science, it is advisable to develop theoretical ideas regarding the place and functions of their methods. The researchers argue that forensics in forensic sciences, as well as in practice of law enforcement, is an indispensable element for investigating cybercrime. Based on the position described, it should be noted that it has common features with the conclusions drawn in this article. In particular, there seems to be evidence of the role of forensics, its content and place in forensic science. Moreover, the same conclusion is reached regarding the mandatory use of digital forensics tools in the modern fight against cybercrime.

In turn, B.H. Toleubekova and T.B. Khvedelidze (2022) studied the content of digital forensics in the context of the academic discipline. In their opinion, the development of legal science is impossible without the formation of a separate discipline within higher educational institutions. This is due to the fact that forensics involves the use of special tools and technologies that require certain professional skills (BOCHELIUK et al., 2022). The researchers argue that "digital forensics" as a separate form should be used and evaluated solely on the basis of knowledge about the system of academic disciplines. Given the subject of forensic science as an independent applied legal academic discipline, it should be noted that it develops on the basis of general and special knowledge about digital technologies (CHERNIAVSKYI et al., 2023). This can be expressed in the form of traditional constituent elements such as forensic technology, tactics, and methodology. The researchers found that the implementation of forensics is possible only by a specialist who has knowledge not only in the legal dimension but also in IT. With regard to the cross-disciplinary content of digital forensics, she believes that it covers both the standard elements of the subject matter of the science of forensics and specific issues regarding the integration of forensics into the traditional

system of forensic science. This approach is consistent with the position discussed in this paper. This is due to the fact that forensics can become an effective method of solving cybercrime only if specialists in this field are trained and their skills are used.

K.S. Lakbaev et al. (2020) analysed the experience of Kazakhstan and the dynamics of the use of forensics in it. They paid special attention to the examination, which is a separate procedure during which the circumstances related to a particular case are identified and investigated. The researchers noted that the peculiarity of such a procedure is that it is performed by persons who have special skills in the field of digital forensics, and most importantly, are disinterested persons regarding a particular case and examination in general. In Kazakhstan, examinations can be organised by both state and non-state agencies. At the same time, the researchers note that a number of qualification requirements are put forward for experts. For example, the availability of special education and work experience. The results obtained during it can have an important evidence base, for example, to confirm the position of a party in court. The cost of this digital forensics service amounts to at least 200 thousand tenge. Researchers note that both citizens and legal entities use it for the most part. The appointment of an expert examination is carried out by a court ruling during the hearing of a civil, arbitration, or criminal case. As for the types of examinations, there are almost 30 of them, in accordance with the organisations that conduct them. The procedure is completed by the issuance of a special opinion by an expert. The results discussed are intertwined with the conclusions obtained within the framework of this scientific paper. This is expressed in the unity of approaches that describe the trends in the development of forensics in Kazakhstan, using the example of expert examinations.

A. Khusanov (2022) also explored the experience of Kazakhstan in the field of digital forensics. As an example, he cited the launch of the TSARKA (Centre for Analysis and Investigation of Cyber Attacks) of the Centre for Computer Forensics. He believes that such an approach is a priority since it allows not only to influence forensic science in the state but also the employment of young professionals in this field. The main purpose of this Centre is to provide services for the investigation of cyberattacks based on forensics. According to the researcher, in order to successfully investigate cybercrime, it is necessary to use international standards aimed at responding to and preventing the negative consequences of such incidents. As for specialists, he notes that they should be highly qualified forensic experts with additional international certificates in the mastering of digital tools. It is also necessary to have a certificate of preparation in the Scientific Research Institute of Forensic Examinations, Specialty of Forensic Examination of the Ministry of Justice of the Republic of Kazakhstan. The researcher

paid attention to the tools, on the basis of which the implementation of forensics takes place. He noted that these include mobile devices, computer hardware, software, as well as information and corporate systems such as CRM systems. The described position corresponds to that explored in this research. What is common is the description of the role of specialists and forensics in the course of investigating cybercrime.

When discussing the current state of digital forensics in Kazakhstan, it becomes evident that the legal framework has not kept pace with the rising prevalence of cybercrime and the growing reliance on digital evidence. Presently, there exists no comprehensive legislation that effectively regulates the collection, analysis, and utilisation of digital evidence within investigations and court proceedings (ADANBEKOVA et al., 2022). This lack of clear legal guidance creates uncertainty regarding the admissibility and evidentiary value of digital evidence.

In the context of Kazakhstan's criminal legislation, cybercrime offences are primarily delineated in Chapter 7 of the Criminal Code of the Republic of Kazakhstan (2014), encompassing Articles 205-213. These articles address various cybercrimes, such as unauthorised access to information systems, illegal modification or destruction of information, and violations related to computer systems and data. However, despite the existence of these provisions, law enforcement agencies frequently lack established procedures and protocols for properly handling digital evidence, thus undermining its integrity and increasing the risk of tampering or contamination. Furthermore, an additional challenge arises from the potential lack of technical expertise among judges and prosecutors when evaluating digital evidence, which contrasts with their proficiency in assessing traditional physical evidence. This disparity in knowledge and skills further complicates the effective use of digital evidence within the legal system.

Based on the discussion, it can be established that, despite significant differences in the approaches of scientists, they all describe a single goal. It consists in the introduction of forensics into the forensic system and directly into the process of investigating cybercrime. This indicates the priority of this approach and the need for its implementation in Kazakhstan.

CONCLUSIONS

As a result of the research, it was possible to establish that forensics enables improving the current institute of forensic science in Kazakhstan through the use of digital technologies directly in the detection and work with digital evidence and traces. It has been established that with the development of information technologies, there is an expansion of tools and approaches to committing cybercrimes. That is why digital forensics is becoming especially popular, aimed at solving problematic aspects in the field of cybercrime.

Within this research, forensics was considered in the context of applied science, which deals with solving crimes related to computer data and security by evaluating digital evidence. It was also found that digital forensics involves the search and identification of important information in the course of investigating cybercrime. It has been proven that forensics in modern society plays an important role in the activities of law enforcement agencies. The current level of cybercrime in Kazakhstan, as well as the dynamics of using forensic approaches in the course of their investigation, are considered as part of the scientific paper. It was possible to establish the problems that exist in the forensic system of Kazakhstan, namely regarding the solving of criminal offences in the field of information and communications.

Thus, the functions and areas in which the use of digital forensics is mandatory, taking into account the characteristics of modern society, were revealed. It has been established that forensics in Kazakhstan is at the stage of its inception, and its future development is quite promising. For the future development of legal mechanisms and ensuring the protection of the rights of citizens, in particular with regard to information stored on digital media, it is appropriate to introduce a separate professional direction among students in the field of forensic science. This is due to the dynamic spread of digitalization in all spheres of state activities, which suggests that the volume of cybercrime will increase and its nature will change. For this purpose, in subsequent scientific papers, it is necessary to consider the procedure for training forensic experts to reveal the features of their acquisition of competence and professional skills.

REFERENCES

ADANBEKOVA, Z., OMAROVA, A. B., YERMUKHAMETOVA, S., ASSANOVA, S., & TYNYBEKOV, S. (2022). Features of an Electronic Transaction as Evidence in Court. *Revista de Direito, Estado e Telecomunicacoes*, 14(1), 98-112.

ALGHAMDIL, M. I. (2021). *Cybersecurity threats with new perspectives.* London: Intech Open.

ALTAEV, E. A., UMIRZHANOV, T. W., & KANATBAEV, T. K. (2023). Prospects for the development of forensic science in the Republic of Kazakhstan. *Economy, Management, Law: Current Issues and Vectors of Development,* 10, 21-25.

AMATO, F., CASTINGLIONE, A., COZZOLINO, G., & NARDUCCI, F. (2020). A semantic-based methodology for digital forensics analysis. *Journal of Parallel and Distributed Computing*, 138, 172-177.

AUBAKIROVA, A. A., ILDEBAYEV, R. E., BEGALIYEV, Y. N., TUMANSHIYEV, R. K., & ALIMANOVA, E. A. (2022). Forensic investigation

of forged educational documents. *International Journal of Electronic Security and Digital Forensics*, 14(3), 274-288.

BAZILOVA, A. A., MALIKOVA, S. B., OMAROVA, A. B., ATAKHANOVA, G. M., & DAUBASSOV, S. S. (2016). Disadvantages in differentiation and exceeding limits of necessary defense according to the legislation of the republic of kazakhstan. *Journal of Advanced Research in Law and Economics*, 7(4), 752-758.

BOCHELIUK, V. Y., SPYTSKA, L. V., SHAPOSHNYKOVA, I. V., TURUBAROVA, A. V., & PANOV, M. S. (2022). Five stages of professional personality development: Comparative analysis. *Polish Psychological Bulletin*, 53(2), 88-93.

BORYSENKO, I. V., BULULUKOV, O. Y., PCHOLKIN, V. D., BARANCHYK, V. V., & PRYHODKO, V. O. (2021). The modern development of new promising fields in forensic examinations. *Journal of Forensic Science and Medicine*, 7(4), 137-144.

CASINO, F., DASAKLIS, T. K., SPATHOULAS, G., ANAGNOSTOPOULOS, M., GHOSAL, A., BOROCZ, I., & PATSAKIS, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 64-93.

CHERNIAVSKYI, S., VOZNIUK, A., & HRIBOV, M. (2023). Legality of traditional techniques, means and modern technologies of visual surveillance. *Scientific Journal of the National Academy of Internal Affairs*, 28(1), 9-21. https://doi.org/10.56215/naia-herald/1.2023.09

CHORNOUS, YU., & LELIUK, T. (2023). Organization of forensic examinations in criminal proceedings as a condition for the effectiveness of the investigation of criminal offences. *Law Journal of the National Academy of Internal Affairs*, 13(2), 50-62. https://doi.org/10.56215/naia-chasopis/2.2023.50

CHUKAIEVA, A., & MATULIENĖ, S. (2023). Possibilities of applying artificial intelligence in the work of law enforcement agencies. *Scientific Journal of the National Academy of Internal Affairs*, 28(3), 28-37. https://doi.org/10.56215/naia-herald/3.2023.28

Criminal Code of the Republic of Kazakhstan. (2014). https://adilet.zan.kz/rus/docs/K1400000226

DANYLKOVYCH, A., SANGINOVA, O., & SHAKHNOVSKY, A. (2023). Computer simulation and optimization of the composition of the hydrophobising mixture. *Bulletin of Cherkasy State Technological University*, (2), 100-110. https://doi.org/10.24025/2306-4412.2.2023.277295

Du, X., HARGREAVES, C., SHEPPARD, J., ANDA, F., SAYAKKARA, A., LE-KHAC, N. A., & SCANLON, M. (2020). SoK: Exploring the state

of the art and the future potential of artificial intelligence in digital forensic investigation. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10). New York: Association for Computing Machinery.

Forensic Kazakhstan. 2022. https://forensic.kz

How Kazakhstanis are deceived by Internet scammers. (2022). https://kapital.kz/gosudarstvo/102872/kak-kazakhstantsev-ob-manyvayut-internet-moshenniki.html

JARRETT, A., & CHOO, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science*, 3(6), e1418.

JONES, G. M., & WINSTER, S. G. (2022). An insight into digital forensics: History, frameworks, types and tools. In: *Cyber Security and Digital Forensics* (pp. 105-125). Beverly: Scrivener Publishing.

KARAGIANNIS, C., & VERGIDIK, K. (2021). Digital evidence and cloud forensics*:* Contemporary legal challenges and the power of disposal. *Information*, 12(5), 181.

KAVRESTAD, J. (2020). *Fundamentals of digital forensics.* Abington: Springer International Publishing.

KEMALI, E. S., & ZHURSIMBAEV, S. K. (2020). Some problems of criminalistics in the light of today. *Scientific and Legal Journal of the Institute of Legislation of the Republic of Kazakhstan*, 1(59), 1-7.

KHUSANOV, A. (2022). Prospects for the development of the forensic service. *Society and Innovation*, 3(2), 31-39.

LAKBAYEV, K. S., RYSMAGAMBRTOVA, G. M., UMETOV, A. U., & SYSOYEV, A. K. (2020). The crimes in the field of high technology: Concept, problems and methods of counteraction in Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 12(4), 412-423.

MENTUKH, N., & SHEVCHUK, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.

METELSKYI, I., & KRAVCHUK, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.

MOUSTAFA, N. (2022). *Digital forensics in the era of artificial intelligence*. Abington: CRC Press.

QADIAR, A. M., & VAROL, A. (2020). The role of machine learning in digital forensics. In*: Proceedings of the (2020) 8th International Symposium on Digital Forensics and Security (ISDFS*) (pp. 1-5). Beirut: IEEE.

SILVARAJOO, V. R., LIM, S. Y., & DAUD, P. (2021). Digital evidence case management tool for collaborative digital forensics investigation. In:

Proceedings of the (2021) 3rd International Cyber Resilience Conference (CRC) (pp. 1-4). Langkawi Island: IEEE.

SUN, D., ZHANG, X., CHOO, K. K. R., Hu, L., & WANG, F. (2021). *NLP*-based digital forensic investigation platform for online communications. *Computers & Security*, 104, 102210.

SUNDE, N., & DROR, I. E. (2021). A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. *Forensic Science International: Digital Investigation*, 37, 301175.

TOLEUBEKOVA, B. H., & KHVEDELIDZE, T. B. (2022). Features of implementation of the concept of anti-corruption policy of the Republic of Kazakhstan for (2022-2026) by higher education institutions under the conditions of introducing digital technologies. *Bulletin of Abai Kazakh National Pedagogical University*, 67(1), 26-33.

Wu, T., BREITINGER, F., & O'SHAUGHNESSY, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34, 300999.

YAACOUB, J. P. A., NOURA, H. N., SALMAN, O., & CHEHAB, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, 19, 100544.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET