Measures to Prevent Criminal Offences in the field of Informatisation and Communications in the Republic of Kazakhstan

Submitted: 13 September 2023
Reviewed: 20 February 2024
Revised: 27 March 2024
Accepted: 24 April 2024

Article submitted to peer blind review

Licensed under a Creative Commons Attribution 4.0 International

Azamat Kambarov[*]
https://orcid.org/0000-0002-6117-1693
Malik Karazhanov[**]
https://orcid.org/0000-0001-7933-6655
Serik Sabitov[***]
https://orcid.org/0000-0003-3327-625X
Yeldos Baigundinov[****]
https://orcid.org/0000-0003-4389-5492
Roman Temirgazin[*****]
https://orcid.org/0000-0001-6967-727X

DOI: https://doi.org/10.26512/lstr.v16i2.50807

Abstract

[Purpose] The relevance of the paper is due to the fact that the introduction of information technology has had an impact on the growth of economic crimes. The purpose of the study is to analyse the effectiveness of existing measures to prevent illegal acts in the field of informatisation and communications.

[Methodology/approach/design] In the course of the study, the concept of cybercrime was covered, the signs and principles of implementation inherent in this category of offences were identified. This provided an opportunity to thoroughly analyse the essence and role of cybercrime in the field of informatisation and communications in the Republic of Kazakhstan. Statistical data on crimes for the period from 2018 to 2022 were examined,

[*] Doctoral Student. Department of Criminal Law Disciplines, Alikhan Bokeikhan University, 11 Mangilik El Str., 11, Semey, Republic of Kazakhstan, 070000. E-mail: azamatkambarov74@gmail.com.

[**] PhD, Dean of the Faculty. Department of Criminal Law Disciplines, Alikhan Bokeikhan University, 11 Mangilik El Str., 11, Semey, Republic of Kazakhstan, 070000. E-mail: malikkarazhanov@outlook.com.

[***] PhD, Head of the Department of Criminal Law Disciplines, Alikhan Bokeikhan University, 11 Mangilik El Str., 11, Semey, Republic of Kazakhstan, 070000. E-mail: serik_sabitov4@proton.me.

[****] PhD, Senior Lecturer. Department of Criminal Law Disciplines, Alikhan Bokeikhan University, 11 Mangilik El Str., 11, Semey, Republic of Kazakhstan, 070000. E-mail: yeldos.baigundinov@hotmail.com.

[*****] PhD, Senior Lecturer. Department of Criminal Law Disciplines, Alikhan Bokeikhan University, 11 Mangilik El Str., 11, Semey, Republic of Kazakhstan, 070000. E-mail: romantemirgazin@protonmail.com.

KAMBAROV A., KARAZHANOV M., SABITOV S., BAIGUNDINOV Y., TEMIRGAZIN R. *Measures to Prevent Criminal Offences in the field of Informatisation and Communications in the Republic of Kazakhstan*. **The Law, State and Telecommunications Review**, v. 16, no. 2, p. 276-294, October 2024.

which allowed analysing the current situation and identifying the main problems in this area. The legal acts regulating the sphere of information technologies and communications in Kazakhstan were also examined.
[Findings] Based on the analysis, recommendations to strengthen the system of countering information crimes were developed. The importance of taking preventive measures to prevent criminal offences in the field of informatisation and communications, especially in the context of rapid technological development, is due to the annual increase in the number of cybercrimes. The practical importance of the results obtained consists in the development of recommendations that will increase the effectiveness of combating criminal offences in the field of informatisation and communications in the Republic of Kazakhstan, improve the level of protection of society from cybercrime and have a positive impact on the national security system of the state.

Keywords: Cybercrime. Globalisation. Digitalisation. Innovation Technologies. Cyberspace.

INTRODUCTION

The escalating prevalence of cybercrime in Kazakhstan underscores the critical need for a thorough analysis of its characteristics and the development of effective remedies. As internal affairs agencies navigate the evolving criminal landscape, characterized by the increasing use of information technology for illicit activities, ensuring information security has emerged as a crucial aspect of preventive work. In light of this pressing issue, this paper aims to provide a detailed analysis of cybercrime in Kazakhstan, examining its dynamics, impacts, and potential solutions.

Recent studies have highlighted the significant rise in cybercrimes targeting various sectors, including government institutions, businesses, and individuals, in Kazakhstan. These crimes range from data breaches and identity theft to financial fraud and cyber espionage, posing serious threats to national security and economic stability. Moreover, the proliferation of digital platforms and the widespread adoption of online services have further expanded the attack surface for cybercriminals, making it imperative for law enforcement agencies to adapt and strengthen their cybersecurity measures (VILKS et al., 2022).

According to K. Nurzhan (2022), cybercrime encompasses a range of illegal activities perpetrated within the digital realm, involving the use of computer systems and networks to target both the systems themselves and the data they contain. According to A.T. Gaisina (2023), cybercrime is a global problem, not limited by borders, and requires the use of criminal law measures, including punitive and preventive aspects, and the scale of crimes worldwide is estimated at tens of millions of criminals causing billions of dollars in damage. The investigation of changes in the number of cybercrimes allows assessing the effectiveness of countering these crimes, drawing conclusions about the state of cybercrime in the country, and determining the future areas of combating it (SOPILKO & RAPATSKA, 2023).

In recent years, several data breaches have occurred in Kazakhstan, compromising sensitive information of individuals and organizations. For example, in 2019, a major data breach affected a Kazakhstani telecommunications company, resulting in the unauthorized access to customer data, including personal and financial information.

Instances of financial fraud, such as online banking scams and credit card fraud, have been reported in Kazakhstan. Cybercriminals often use phishing emails or fraudulent websites to trick individuals into disclosing their banking credentials, leading to unauthorized transactions and financial losses.

Ransomware attacks, where cybercriminals encrypt data and demand payment for its release, have targeted businesses and government agencies in Kazakhstan. In 2020, several hospitals and healthcare institutions in Kazakhstan fell victim to ransomware attacks, disrupting critical healthcare services and causing significant financial losses.

B.B. Doszhanov (2023) notes that depending on which object is being attacked, several groups of cybercrimes can be distinguished: computer crimes in the field of entrepreneurship, which are associated using digital technologies to commit illegal acts against this sphere, crimes against personal rights and privacy, which are aimed at violating the rights and confidentiality of personal data, crimes against public and state interests that are aimed at malicious interference in the work of state and public systems. In turn, B. Cherniakhovskyi (2020) and M.S. Zarkenov (2021) state that based on the way computers or computer systems are used, three classifications of cybercrimes can be distinguished: acts in which computers themselves are the object of a crime, such as theft of information, unauthorised access to systems, destruction, or damage to files and devices, and other similar actions; actions in which computers are used as instruments of crime for example, theft of electronic means and other crimes committed using electronic systems; crimes in which computers play the role of instruments of intellectual actions. This allows concluding that due to the development of digitalisation processes, the number of ways of committing illegal acts is growing.

As A.K. Nurpeisova (2020) mentions, in October 2017, an Action plan for the implementation of the Cybersecurity Concept was adopted, which provided for the improvement and consolidation of legislative norms in the field of information security. Besides, A.B. Seidanov et al. (2021) note that the concept of “cyber insurance” was introduced into the industry law, which provides for compensation for material damage caused to organisations as a result of computer incidents, and moral damage to individuals in the event of data leakage. The country has also appointed an authorised body for the protection of personal data – the Information Security Committee of the Ministry of Digital Development, Innovation, and Aerospace Industry of Kazakhstan (MDDIAI RK) (LAW OF THE REPUBLIC…, 2010).

As can be noted from the above, the policy of the Republic of Kazakhstan on the prevention of this category of offences is effectively developing, but the number of crimes increases annually. In this regard, the purpose of the study is to analyse the essence of cybercrime and identify the most effective measures to combat them.

MATERIALS AND METHODS

This study was conducted using various types of analysis method. The method of functional analysis helped cover the concept of cybercrime by identifying its characteristic features, characteristics, and principles of implementation. By analyzing the functions and behaviors associated with cybercriminal activities, researchers could gain insights into the nature and scope of cybercrime. The method of logical analysis allowed isolating its constituent elements from the concept of cybercrime and determining their relationship. It also helped to highlight the actions and techniques that are used by cybercriminals and how they can affect the security of information systems. The method of logical analysis allowed identifying common characteristics and features of cybercrimes, namely, characterising the purpose, subjects, objects, and the means and methods used. Statistical analysis was utilized to assess the prevalence and trends of cybercrime based on the facts of registration of crimes in the field of informatization and communications. This method provided quantitative insights into the frequency and distribution of cybercrimes over a specific period, enabling researchers to identify patterns and prioritize areas for intervention and prevention

The formal legal method involved the analysis of relevant legislation to understand the legal framework surrounding cybercrime. By examining laws related to the prevention of offenses, informatization, communications, and cyber security in Kazakhstan, researchers could identify legal provisions, concepts, and their interrelationships, thus providing a foundation for legal analysis and interpretation. In turn, the following laws were examined: Law of the Republic of Kazakhstan No. 271-IV "On the Prevention of offences" (2010), Law of the Republic of Kazakhstan No. 418-V "On Informatisation" (2015), Law of the Republic of Kazakhstan No. 567-II "On Communications" (2004), On approval of the Cyber Security Concept ("Cyber Shield of Kazakhstan") (2017), Criminal Code of the Republic of Kazakhstan (2023). The method of legal hermeneutics allowed for a systematic analysis of legal texts to determine their purpose, main provisions, and interpretation. By applying legal hermeneutics to the laws of

Kazakhstan, researchers could establish the purpose of the law and ensure its consistency with legal principles, contributing to a deeper understanding of the legal framework governing cybercrime. The application of the method of legal hermeneutics helped to establish the purpose of the law and its compliance with the principles of the legal system, a conclusion was made on the interpretation and application of laws in specific cases. The dogmatic method, which is based on a systematic and logical analysis of the laws, helped to break down the laws into their constituent elements, determine their relationship and meaning. The application of the dogmatic method allowed establishing a logical sequence and connection between various norms and rules for a better understanding of the law and its consistency within the legal system. Due to the use of the dogmatic method, it was possible to draw conclusions about the interpretation and application of laws in practice.

The method of deduction in the context of the examination of cybercrime allowed proceeding from general principles and laws to deduce specific provisions regarding cybercrime. Based on existing definitions, concepts, and legislation, general principles, features, and characteristics were formulated, and specific consequences regarding cybercrime were derived. In turn, the induction method allowed identifying general patterns and conclusions based on specific facts and observations. In the context of the investigation of cybercrime, the use of the induction method allowed analysing specific cases and, based on them, drawing conclusions about the general characteristics and elements of cybercrime. In addition, the induction method allowed characterising the elements inherent in cybercrime based on the general concept. The use of deduction and induction methods allowed systematising information about cybercrime and its elements, identifying common patterns. The synthesis method facilitated the integration of information identified during the analysis into a cohesive whole. By combining insights from various analytical approaches, researchers could assess the effectiveness of measures to prevent cybercrime and develop comprehensive strategies for addressing this category of crime.

RESULTS

Legal Framework for Preventing Cybercrime in Kazakhstan

All types of criminal offences in the field of informatisation and communication can be prevented in various ways. It is necessary to use various preventive measures to achieve this goal. In this case, preventive measures are understood as activities aimed at identifying and eliminating the causes that give rise to offences, and the conditions that contribute to their commission. At the moment, Kazakhstan does not use any special methods to counteract offences in the field of informatisation and communications; in the world, various measures are used to combat cybercrime, including legal, organisational, and technical methods (TEMIRALIEV and OMAROV, 2019). The main instruments of legal measures aimed at preventing offences are legislative norms. They define responsibility for the commission of offences, improve criminal and other legislation, and also include the conclusion and execution of international treaties in this area.

Kazakhstan has adopted a number of laws aimed at preventing criminal offences in the field of informatisation and communications. Issues related to prevention are regulated by Law of the Republic of Kazakhstan No. 271-IV "On the Prevention of Offenses" (2010). This Law establishes the basic principles of the legal, economic, social, and organisational nature of the activities of the authorities and the public. That is, its main purpose is to determine methods and techniques for countering crimes. There are also special laws, such as Law of the Republic of Kazakhstan No. 418-V "On Informatisation" (2015), which regulates public relations in the field of informatisation on the territory of Kazakhstan between various entities in the creation, development, and operation of information facilities. There is also the Law of the Republic of Kazakhstan No. 567-II "On Communications" (2004), which establishes the foundations of legal activities in the field of communications and defines the powers, rights and obligations of various categories of subjects of legal relations. In addition, information security issues in the field of informatisation and communications are regulated by other legal norms. Thus, a number of norms were adopted for the implementation of the Law of the Republic of Kazakhstan No. 418-V "On Informatisation" (2015). These legislative acts provide an opportunity to regulate the sphere of informatisation and communication in the most extensive way and include a list of norms that establish various features for countering and preventing crimes. For example, the Government implemented the Law On approval of the Cyber Security Concept ("Cyber Shield of Kazakhstan") (2017). This concept establishes the basic principles of national policy in the field of protection of electronic resources, information systems, and telecommunication networks, ensuring the safe use of various technologies. Within the framework of this concept, it is proposed to introduce the concept of "cyber hygiene" into the legal field.

The Criminal Code of the Republic of Kazakhstan also has a separate chapter No. VII "Criminal offences in the field of information and communication" (2023), which consists of 9 articles. Some of these articles include "Unlawful access to information, to an information system, or telecommunications network" (Article 205) and "Unlawful acquisition of information" (Article 208). It is worth considering the number of registered cybercrimes in the Unified Register of Pre-Trial Investigations (URPI) in the period 2018-2022 (Table 1).

Article	**Registered in the URPI**					**Total**
	2018	**2019**	**2020**	**2021**	**2022**	
Paragraph 4 part 2 of Article 190 of the Criminal Code of the Republic of Kazakhstan (Fraud committed by deceiving or abusing the trust of an information system user)	517	7769	14220	21405	22880	66791
Article 205 of the Criminal Code of the Republic of Kazakhstan (Unauthorised access to information, to an information system, or a telecommunications network)	28	59	71	46	80	284
Article 206 of the Criminal Code of the Republic of Kazakhstan (Unlawful destruction or modification of information)	13	6	12	9	12	52
Article 207 of the Criminal Code of the Republic of Kazakhstan (Disruption of the information system or telecommunications networks)	5	6	4	0	2	17
Article 208 of the Criminal Code of the Republic of Kazakhstan (Illegal acquisition of information)	11	16	8	9	12	56
Article 209 of the Criminal Code of the Republic of Kazakhstan (Coercion to transfer information)	1	0	0	0	0	1
Article 210 of the Criminal Code of the Republic of Kazakhstan (Creation, use or distribution of malicious computer programmes and software products)	4	4	4	4	2	18
Article 211 of the Criminal Code of the Republic of Kazakhstan (Illegal distribution of restricted electronic information resources)	7	8	8	5	8	36
Article 212 of the Criminal Code of the Republic of Kazakhstan (Provision of services for the placement of Internet resources pursuing illegal purposes)	1	2	0	0	1	4
Article 213 of the Criminal Code of the Republic of Kazakhstan	2	7	2	1	0	12

(Illegal modification of the identification code of a cellular subscriber device, subscriber identification device, and the creation, use, and distribution of programmes to change the identification code of a subscriber device)						
Total	589	7877	14325	21479	22997	67271

Table 1 – Number of Registered Cybercrimes in 2018-2022

Source: Legal Statistics (2022).

The data provided allows concluding that the largest number of crimes arise in cases that are related to Internet fraud. Nevertheless, substantially fewer facts of offences are registered annually, which are provided for by Chapter 7 of the Criminal Code of the Republic of Kazakhstan in comparison with Internet fraud (Figure 1).

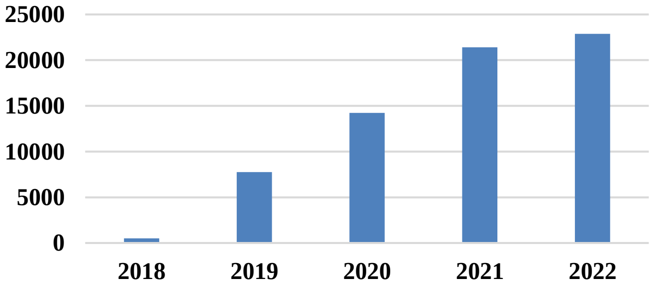

Chart 1 – Registration of the fact of Internet fraud in 2018-2022

Source: Legal Statistics (2022).

Based on the information obtained, the increase in registration of the fact of Internet fraud from 2018 to 2022 increased 43 times (Legal Statistics, 2022). This allows concluding that it is necessary to apply more effective measures to prevent these acts. Notably, the use of only legal measures is not always enough for effective preventive work. It is necessary to consider organisational measures aimed at preventing the emergence of threats to information security. Such measures include the approval of documents regulating the functioning of the information and communication infrastructure, the development of an information security policy, the use of information security risk assessment techniques, and the introduction of rules for the identification, classification and labelling of information assets. An important aspect is to ensure the continuous operation of assets related to information processing and inventory and certification of computer equipment, telecommunications equipment, and software. Internal audit of information security, the use of cryptographic protection of information, access control to electronic resources, the correct use of the Internet and e-mail on mobile devices and media, the organisation of authentication procedures, anti-virus control, and physical protection of information resources – all these measures are also part of the organisational strategy (KAMBAROV, 2015). In addition, an important aspect is the personnel policy, which includes confidentiality conditions in employment contracts both during the working period and for a certain period after its end. Current educational programmes that consider the latest developments and technological innovations are used to train personnel in the rules and means of information protection.

Limitations of Cyber Hygiene and Preventive Measures

In accordance with the Law On approval of the Cyber Security Concept ("Cyber Shield of Kazakhstan") (2017), to achieve the task of raising awareness about cyber threats, developing human potential in the information and communication technology industry, and creating sustainable protection against malicious software and technical impact, it is proposed to form stable ideas about "cyber hygiene" in society. In the conditions of rapid digital progress, it is necessary to adhere to certain principles of safe work in the field of information technology. The term "cyber hygiene" refers to compliance with the basic rules of digital security when interacting in the information and communication environment, which has become quite an important and integral aspect in the life of the public. Notably, it would be very expedient to introduce into the Concept provisions on the greater prevalence of cyber hygiene in society to minimise the risk of crimes among citizens (METELSKYI and KRAVCHUK, 2023).

The rules of cyber hygiene include the following recommendations: the use of licensed software and the installation of all updates in a timely manner; refusal to install software from unknown manufacturers and from unverified download sources, and encryption of user data; prevention of opening or clicking on links in electronic format letters that are received from unknown persons; establishment of passwords of an exceptionally complex and differentiated plan on all resources used, that is, social networks and mail to ensure that a password leak on one resource does not make a profile on other resources vulnerable; refusal to transfer passwords to third parties and send PIN codes from bank cards; deletion of unused profiles on Internet resources; avoidance of visiting unknown sites containing content that contradicts the norms of morality and legislation;

usage of antivirus programmes that block known vulnerabilities; deletion of detailed information, namely place of residence, legal name, date of birth about oneself and loved ones on social networks or hiding such information if it is already available.

Thus, the rules of cyber hygiene are necessary to be followed on a daily basis. In addition to organisational measures, technical measures also play a substantial role of a preventive nature. Notably, they are designed to protect information systems and communication networks from unwanted influences, prevent the leakage of confidential information, and the use of technical devices such as lasers, radio equipment, visual surveillance and communications. The application of these methods is conducted through the use of various developments, devices, equipment, software, and hardware of the technical plan. They can be divided into two main groups, namely hardware and software.

Hardware methods are used to implement the protection of hardware and computer communications equipment from undesirable physical influences from external forces, and to block and minimise the risk of leakage of confidential information and other data. Various technical devices are used for the effective implementation of these methods. For example, there are devices and structures that prevent unauthorised access to protected information. Uninterruptible power supplies are also used, providing protection against sudden voltage fluctuations and guaranteeing power supply in emergency situations. Shielding devices are used to protect equipment, wired communication lines, and protected premises. Various means are used to ensure authorised physical access of users to the protected premises, such as locks, access control systems, personal identification devices, and devices for identifying and fixing the terminals and users used in attempts of unauthorised access to the information-communication infrastructure. In addition, security and fire alarm systems, port protection of computer equipment, and visual monitoring of the internal and external perimeter are used.

Software protection methods play an important role in ensuring the security of information. They are aimed at direct data protection and include a variety of information encryption techniques, the use of passwords, and anti-virus control tools. Data encryption methods allow protecting information by converting it into an encrypted form that can only be understood by authorised users using the appropriate key. This ensures confidentiality and protection against unauthorised access to information.

Cybersecurity Initiatives and Challenges in CIS Countries

Today there are many examples of digital transformation of the countries of the Commonwealth of Independent States (CIS). Comprehensive measures are being taken in Uzbekistan for the active development of the digital economy and the widespread use of modern information and communication technologies in all sectors and spheres, especially in public administration, education, healthcare, and agriculture (ULIUTINA, 2023). As part of this, the implementation of more than 220 priority projects aimed at improving the e-government system, further developing the domestic software and information technology market, creating IT parks in all regions of the country, and providing this area with qualified personnel was launched. In this regard, a comprehensive programme "Digital Tashkent" was approved, including the launch of a geoportal integrated with more than 40 information systems, the creation of an information system for managing public transport and communal infrastructure, the digitalisation of the social sphere with the subsequent dissemination of this experience to other regions; digital transformation programmes and the strategy "Digital Uzbekistan – 2030" developed by the Ministry for the Development of Information Technologies and Communications were also approved (DOSZHANOV, 2023). Special attention is paid to cybersecurity issues to ensure high-quality and timely fulfilment of the tasks set. During 2020, more than 27 million cases of malicious and suspicious network activity originating from the Internet address space were detected, which posed a threat to the security and stable operation of information systems and resources (ZARKENOV, 2021).

Within the framework of the Kyrgyz Republic, a Cybersecurity Strategy was developed and approved only in 2019, with plans to create basic conditions for ensuring security in the country in the period from 2019 to 2023 (NURPEISOVA, 2020). As a result, it is also planned to introduce responsibility for cybercrimes, including cross-border computer crimes, and the development of methods for detecting, collecting, and providing evidence using information-communication technologies (ICT). The technical base is the most vulnerable element in Kyrgyzstan since the country lacks basic cybersecurity components, and there is also insufficient resistance to network attacks. There are no Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT) groups in Kyrgyzstan. The lack of specialists in the field of cyberterrorism, cyber espionage, and threats of a combined nature indicates an insufficient level of development of the technical base.

At the moment, there is no ideal system that would cover all the ways and methods to counteract offences. Based on this, only an integrated approach, which will include legal, organisational, and technical measures, will provide an opportunity to reduce socially dangerous actions. Kazakhstan is undergoing a process of digitalisation and globalisation, solving issues of computer support for government agencies and organisations, but there is still a shortage of qualified personnel. However, the rapid pace of integration of the state into the global space of the information plan, the provision of available funds and their integration into the daily lives of citizens, and the annual increase in the number of illegal acts in this area allow concluding that this problem may become more acute. Proceeding from this, to effectively combat information offences and cybercrimes, the following measures can be taken: improving technologies that facilitate the detection of cybercrimes on the network and conducting their investigation, maximising the use of blockchain technology to counter cyber threats, the development and implementation of artificial intelligence in the field of cybercrime investigation, tightening responsibility for cybercrime, active counteraction to cyberterrorism in all its forms and manifestations.

Thus, the creation of conditions for improving the effectiveness of measures to prevent crimes and offences in the field of informatisation and communications is necessary since they are aimed at neutralising and minimising the negative consequences of criminal activity and preventing the occurrence of such threats. In connection with the above, it is advisable to supplement the current legislation with norms that will provide an opportunity to minimise the risk of illegal acts of this category, the development of information technologies in law enforcement agencies to identify new ways and methods of committing crimes and their elimination.

DISCUSSION

The processes of globalisation, including the globalisation of information technologies, provide unlimited opportunities to influence the individual and society. As S. Nurhayati et al. state, one of the negative consequences of the development of information technologies is the emergence and spread of a new type of crime – high-tech crime when computers and information networks become the object of criminal actions and the means or method of their commission (NURHAYATI et al., 2021). The problem of cybercrime has become relevant in the era of the information society, when computers and telecommunications systems have penetrated into all spheres of life of people and states, and the global Internet is one of the fastest-growing telecommunications technologies.

At the moment, there is a variety of terms used to denote crimes committed in computer and telecommunications systems, such as computer crimes, high-tech crimes, cybercrimes, computer security crimes, computer crimes in the field of information. A number of approaches to understanding the phenomenon under consideration were analysed by G. Siregar and S. Sinaga (2021), who note that cybercrime in a broad sense includes any illegal actions committed using or related to computing devices, including crimes such as illegal storage, offering, or dissemination of information using computer technology. K. Kikerpill (2020) believes that cybercrime is related to offences committed in various information networks. On the other hand, S. Back and J. LaPrade (2019) consider cybercrimes as socially dangerous actions committed using computer technology in relation to information processed and used on the Internet. However, this concept does not reveal the concept of cybercrime fully and in detail, but only considers its narrow area.

B. Dupont (2019) states that international law does not distinguish between the terms “cybercrime” and “computer crime”, preferring the first term. The Cybercrime Convention, adopted by the Council of Europe, classifies cybercrime and defines the term “cybercrime” rather than “computer crime”. Based on this, it should be concluded that the concept of “cybercrime” reveals more broadly the corpus delicti using various digital technologies. Nowadays, the term “cybercrime” is often used together with the term “computer crime”, and these terms are often used synonymously. C.S. Biswal and S.K. Pani (2021) mention that the term “computer crime” is given the greatest preference in the literature. In accordance with this position, it can be concluded that most studies are conducted at the forensic or procedural level. In addition, the Criminal Code of the Republic of Kazakhstan provides for liability for offences related to information and information systems. The lack of a unified approach to the definition of this concept is probably due to the lack of consistency in studies devoted to the examination of cybercrime and the theoretical aspects of such offences (SHEVCHUK, 2020).

Notably, these terms are very close to each other, but they are not synonyms. Thus, the term “cybercrime” is broader than “computer crime” and more accurately reflects the essence of crime in the information space. W. Akhuai et al. (2022) defined the prefix “cyber” as part of complex words related to information technology, the Internet, and virtual reality. Cybercrime includes crimes related to both the use of computers, information technology, and global networks. A. Moneva (2020) states that the term “computer crime” refers only to crimes committed against computers or computer data. The global information space and the mega-information environment are immaterial and irreducible to the physical environment in which they exist. Computer crime, in turn, covers crimes that violate the safe functioning of computers, computer networks, and the data processed by them. Thus, computer crime is a subtype of cybercrime.

It is necessary to consider the factors that influence the increase in the number of cybercrimes. Thus, C. San Miguel et al. (2020) noted that the global computerisation of all fields of society does not increase, but, on the contrary, reduces the level of their security, the acceleration of scientific-technological progress increases the likelihood of criminals using completely peaceful technologies as attack tools. It is worth agreeing with this position and adding that the possibility of “double” use of these technologies was not only unintended but also unpredicted by their creators. Terrorism is increasingly acquiring the features of information technologies. This is due to the fact that modern information and telecommunication systems are increasingly being used for communication and intelligence. Cyberterrorism is becoming one of the most common crimes. The main part of terrorist acts is aimed at causing material damage, threatening people's lives and health, and information and psychological shock, which affects large masses of people and creates a favourable environment for achieving terrorist goals. The state of cybercrime in the country allows identifying several current trends. A. Jordan (2020) mentions that the main share of cases of unauthorised access to computer information, which currently account for 19% of the total number of recorded computer crimes, and the creation of malicious software – 8%, are related to the theft of funds and minor crimes committed from hooligan motives.

Another problem is the low level of computer literacy among the population and legal entities (KURYLO et al., 2023). Hackers, abusing the lack of knowledge about basic information security, manipulate personal and commercial information of individuals and legal entities, which becomes a tool for the extortion of funds. State bodies are not actively conducting preventive work to prevent crimes in the field of informatisation and communications. There is also insufficient coverage of the most common methods of hacking the security of computers, smartphones, and other devices, and the promotion of elementary methods of ensuring information security. Depending on the target of the attack, the following categories of cybercrimes are distinguished: computer crimes in the field of entrepreneurship, computer crimes against personal rights, and violations of privacy, and computer crimes against public and state interests.

M. Kumari (2019) states that in 2007-2008, the International Telecommunication Union developed several types of classifications of cybercrime, considering new types of crimes that have appeared in recent years. Thus, the "Model Law" of the International Telecommunication Union has proposed a classification that includes cyberterrorism as one of the subspecies of other crimes, such as "unauthorised access" to commit terrorist acts. Statistics show that 12 thousand people are exposed to cyber-attacks every second in the world, and the damage from cybercrime exceeds 100 billion dollars a year (JORDAN, 2020). In the Resolution of the Government of the Republic of Kazakhstan No. 407 dated June 30, 2017, the importance of ensuring cybersecurity in the context of digitalisation of the economy was emphasised. The Government noted that the effective implementation of digitalisation is possible only when ensuring the security of sectors that are associated with using information-communication technologies (CRIMINAL CODE OF THE…, 2023). One of the stages of digitalisation is the introduction of "electronic proceeding”, which includes components such as electronic appeals of citizens, a unified register of subjects and objects of inspections.

However, crimes in the field of informatisation and communications, especially those related to unlawful access to information, unlawful destruction, or modification of information and the creation of malicious computer programmes, are still present. Over the past three years, there has been a decrease in the number of registered crimes. However, experts believe that this is only a small part of the crimes actually committed in this area since most cases remain unregistered due to the lack of reaction from the victims of crimes and the hidden nature of crimes committed using computer technologies (KANYBEKOVA, et al., 2023). Thus, the legislation of the Republic of Kazakhstan in the field of cyberspace is at the initial stage of development. This is due to the fact that the widespread use of information technologies and the increase in related offences have occurred relatively recently. An active national policy in the field of informatisation and communications, improvement of current legislation, development of information-communication technologies used by state bodies and increasing cyber hygiene among citizens will provide an opportunity to prevent and minimise the risk of cybercrime.

While this study offers valuable insights into the legislative framework, preventive measures, and registered cybercrimes in Kazakhstan, it is important to acknowledge its limitations. The study relies on data from legal statistics and existing legislation. There may be limitations in the availability, accuracy, and completeness of the data, which could affect the comprehensiveness of the analysis. The study primarily focuses on cybercrime-related legislation, preventive measures, and registered cybercrimes in Kazakhstan. However, cybercrime is a complex and evolving phenomenon influenced by various socio-economic, technological, and geopolitical factors. The analysis may not cover all aspects of cybercrime comprehensively. The findings and conclusions drawn from the analysis are based on specific legal frameworks and empirical data from Kazakhstan. It may not be appropriate to generalize the findings to other countries or regions with different legal systems, socio-cultural contexts, and levels of technological advancement. While various analytical methods were employed in the study, including functional analysis, logical analysis, statistical analysis, and legal analysis, there may be inherent limitations in each method, such as subjectivity, bias, and interpretation errors. Addressing these limitations requires future research efforts that incorporate diverse methodologies, expand the scope of analysis, consider comparative perspectives, and engage with relevant stakeholders to develop comprehensive strategies for combating cybercrime effectively.

CONCLUSIONS

Throughout the research, it was established that cybercrimes involve unlawful actions perpetrated using advanced communication technologies to undermine the legal interests of citizens, society, and the state. An examination of Kazakhstan's regulatory framework was undertaken to assess responsibilities and preventive measures against such crimes. This analysis aimed to identify primary methods and strategies for crime prevention and evaluate their efficacy. Subsequently, a statistical analysis was conducted on crimes related to informatization and communications, documented in the URPI database from 2018 to 2022. It was observed that instances of Internet fraud surged by a factor of 43 during this period, resulting in a total of 67,721 registered crimes.

One of the ways to prevent illegal acts is cyber hygiene. It covers a wide range of measures and rules aimed at ensuring network security and personal data protection. Compliance with these rules reduces the risk of becoming a victim of cybercriminals. Teaching people the basics of using and security on the web, spreading information about typical fraudulent schemes and threats, and developing recommendations for safe use of the Internet will help reduce the number of successful attacks. Cooperation between government organisations, the private sector, and the public is an integral part of the fight against cybercrime. Together, they can develop effective policies and programmes, share information about new threats, and participate in public education on cyber hygiene. The improvement of the current legislation and active national policy will provide an opportunity to minimise the risk of the occurrence of cybercrimes and counteract them. Subsequent studies will be aimed at analysing the fight against cybercrime in foreign countries.

REFERENCES

AKHUAI, W., NUGRAHA, A. A., LUKITANINGTYAS, Y. K. R. D., RIDHO, A., WULANSARI, H., & AL ROMADHONA, R. A. (2022). Social capital of Pancasila education in smart education with social media in cybercrime prevention in the Industrial Revolution Era 4.0. *Jurnal Panjar: Pengabdian Bidang Pembelajaran*, *4*(2), 283-442.

BACK, S., & LAPRADE, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 1-4.

BISWAL, CH. S., & PANI, S. K. (2021). Cyber-crime prevention methodology. In: *Intelligent Data Analytics for Terror Threat Prediction:*

Architectures, Methodologies, Techniques and Applications (pp. 291-312). New York: Scrivener Publishing LLC.

CHERNIAKHOVSKYI, B. (2020). Modern possibilities of forensic examinations in the investigation of unauthorized interference in the work of computers, automated systems, computer networks or telecommunication networks. *Law Journal of the National Academy of Internal Affairs*, *10*(2), 81-89.

CRIMINAL CODE OF THE REPUBLIC OF KAZAKHSTAN. (2023). Available at: https://online.zakon.kz/Document/?doc_id=31575252

DOSZHANOV, B. B. (2023). Objective signs of criminal offenses in the sphere of informatization and communication. *Bulletin of Abai Kazakh National Pedagogical University. Series "Jurisprudence"*, *72*(2), 53-64.

DUPONT, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, *42*(5), 500-515.

GAISINA, A. T. (2023). Problem issues of counteraction to criminal offenses in the sphere of informatization and communications. In: *VII Annual Scientific and Practical Conference of Undergraduates and Doctoral Students "Current Issues Improvements Legislation and Law Enforcement Practice"* (pp. 276-280). Astana: Academy of Justice at the Supreme Court of the Republic of Kazakhstan.

JORDAN, A. (2020). *Cybercrime prevention principles for internet service providers*. Geneva: World Economic Forum.

KAMBAROV, A. K. (2022). The main ways of committing criminal offenses in the field of informatization and communication. In: *Criminal Proceedings: Procedural Theory and Forensic Practice* (pp. 85-87). Semey: Alikhan Bokeykhan University.

KANYBEKOVA, B., ARSTANBEKOV, M., KAKESHOV, B., ERDOLATOV, Ch., & ARTYKBAEV, I. (2023). Criminological aspects of the behaviour of victims of cyberattacks: case analysis of hacking state organisations ensuring national security. *Pakistan Journal of Criminology*, *15*(4), 175-192.

KIKERPILL, K. (2020). The individual's role in cybercrime prevention: Internal spheres of protection and our ability to safeguard them. *Kybernetes*, *50*(4), 1015-1026.

KUMARI, M. (2019). Application of machine learning and deep learning in cybercrime prevention – A study. In: *National Conference on Research Trends in Big Data and Intelligent Computing* (pp. 1-4). Bangalore: Indian Academy Degree College.

KURYLO, V., KARAMAN, O., BADER, S., POCHINKOVA, M., & STEPANENKO, V. (2023). Critical thinking as an information security factor in the modern world. *Social and Legal Studios, 6*(3), 67-74.

LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 271-IV "On the Prevention of Offenses". (2010). Available at: https://online.zakon.kz/Document/?doc_id=30657323

LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 418-V "On Informatization". (2015). Available at: https://online.zakon.kz/Document/?doc_id=33885902

LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 567-II "On Communications". (2004). Available at: https://online.zakon.kz/Document/?doc_id=1049207

LEGAL STATISTICS. (2022). Available at: https://qamqor.gov.kz/crimestat/statistics

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

MONEVA, A. (2020). *Cyber places, crime patterns, and cybercrime prevention: An environmental criminology and crime analysis approach through data science*. Elche: Miguel Hernandez University.

NURHAYATI, S., MUSA, S., BORIBOON, G., NURAENI, R., & PUTRI, S. (2021). Community learning center efforts to improve information literacy in the community for cybercrime prevention during a pandemic. *Journal of Nonformal Education, 7*(1), 32-38.

NURPEISOVA, A. K. (2020). Information security and protection of information according to the criminal legislation of the Republic of Kazakhstan. In: *Contemporary Problems of State and Law* (pp. 235-242). Novosibirsk: Siberian University of Consumer Cooperation.

NURZHAN, K. (2022). Criminal offenses in the sphere of informatization and communications in the Republic of Kazakhstan. In: *International Scientific and Practical Conference "Advancing in Research, Practice and Education"* (pp. 253-256). Florence: International Science Group.

ON APPROVAL OF THE CYBER SECURITY CONCEPT ("Cyber Shield of Kazakhstan"). (2017). Available at: https://adilet.zan.kz/rus/docs/P1700000407

SAN MIGUEL, C., MORALES, K., & YNALVEZ, M. A. (2020). Online victimization, social media utilization, and cyber crime prevention measures. *Asia-Pacific Social Science Review, 20*(4), 123-135.

SEIDANOV, A. B., TEMIRGAZIN, R. KH., & UTEBAEV, E. K. (2021). Analysis of the elements of the methodology of investigation of crimes under the criminal code of the republic. In: *Criminal Proceedings:*

Procedural Theory and Criminalistics Practice Kazakhstan (pp. 65-68). Simferopol-Alushta: IT “ARIAL”.

SHEVCHUK, V. M. (2020). Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine, 27*(2), 170-183.

SIREGAR, G., & SINAGA, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction*, *5*(2), 211-227.

SOPILKO, I., & RAPATSKA, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs, 28*(1), 44-54.

TEMIRALIEV, T. S., & OMAROV, Y. A. (2019). Problems of Counteraction to crimes committed with the application of information systems and the ways to solve such issues. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, *55*(1), 94-99.

ULIUTINA, O. (2023). Information and communication technologies legislation for self-government bodies. *Law. Human. Environment*, *14*(4), 66-78.

VILKS, A., KIPANE, A., KUDEIKINA, I., PALKOVA, K., & GRASIS, J. (2022). Criminological aspects of current cyber security. *Revista de Direito, Estado e Telecomunicacoes*, *14*(2), 94-108.

ZARKENOV, M. S. (2021). Topical issues of the subjective side of some offenses in the field of informatization and communication. *Bulletin of the Academy of Law Enforcement Agencies Under the General Prosecutor’s Office of the Republic of Kazakhstan*, *20*(2), 38-47.

ZARKENOV, M. S., & ZHEMPISOV, N. SH. (2021). Criminal liability in the field of illegal mining of digital assets. *Bulletin of the Academy of Law Enforcement Agencies under the General Prosecutor’s Office of the Republic of Kazakhstan*, *2*, 48-55.

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