Topical Issues in the Fight Against Criminal Offences in the Field of Informatisation and Communications

Submitted: 22 August 2022
Reviewed: 29 August 2022
Revised: 17 September 2022
Accepted: 6 October 2022

Article submitted to blind peer review

Azamat Kambarov*
https://orcid.org/0000-0002-6117-1693
Malik Karazhanov**
https://orcid.org/0000-0001-7933-6655
Assylbek Smagulov***
https://orcid.org/0000-0003-3110-2088
Serikkazy Kumisbekov****
https://orcid.org/0000-0001-9089-2273

DOI: https://doi.org/10.26512/lstr.v15i1.44728

Abstract

[Purpose] To investigate the main provisions of modern legal science regarding criminal offences in the field of informatisation and communications.

[Methodology/Approach/Design] The study used general scientific and special legal methods, in particular, analysis, generalisation, statistical, and comparative legal. Classification and modelling methods were actively used during the study.

[Findings] The main result of this study was the analysis of statistical data on committed criminal offences in the field of informatisation and communications, identification of general trends, and the development of the original classification of offences in the field under study. The authors conducted a comparative analysis of the experience of other countries in preventing and combating crimes in the field of informatisation and communications, developing practical recommendations for solving urgent problems of combating this category of crimes in Kazakhstan.

[Practical Implications] The results of the study, consisting in the developed model of international cooperation in combating criminal offences in the field of informatisation and

* Doctoral Student at the Department of Criminal Law Disciplines, Alikhan Bokeikhan University. Address: Alikhan Bokeikhan University, 070000, 11 Mangilik El Str., Semey, Republic of Kazakhstan. E-mail: kambarova019@gmail.com.

** PhD in Law, Associate Professor at the Department of Criminal Law Disciplines, Alikhan Bokeikhan University. Address: Alikhan Bokeikhan University, 070000, 11 Mangilik El Str., Semey, Republic of Kazakhstan. E-mail: mal.karazhanov@aol.com.

*** Full Doctor in Law, Professor at the Department of Law, Kazakh-Russian International University. Address: Kazakh-Russian International University, 030006, 52 Aiteke bi Str., Aktobe, Republic of Kazakhstan. E-mail: ass-smagulov@gmail.com.

**** PhD in Philosophy, Associate Professor at the Department of General Legal Disciplines, Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Barimbek Beisenov. Address: Karaganda Academy, 100009, 124 Yermekov Str., Karaganda, Republic of Kazakhstan. E-mail: kumisbekov-ser@yahoo.com.

communications, can be used by the competent authorities in the field of criminal proceedings in Kazakhstan.
[Originality/Value] Special attention in the paper was paid to offences in the field of informatisation and communications from the standpoint of violation of human rights and freedoms, especially the right to information.

Keywords: Cybercrime. Information Development. Criminal Proceedings. International Cooperation.

INTRODUCTION

With the development of information and communication technologies, the number of studies on cybercrime has grown exponentially over the past few decades (BOSSLER and BERENBLUM, 2019; NURDAULET et al., 2018). The intensification of scientific research in this area can also be explained from the standpoint that at this stage of the development of human civilisation, there is an active introduction of information and communication technologies into the political, social, and economic life of society.

The above trend has both an obvious positive effect against the background of globalisation, and negative consequences in the form of new offences, for example, those related to illegal access to information and its dissemination, fraud committed with the help of the latest digital technologies, cyberterrorism, etc. In addition, the outbreak of the Covid-19 pandemic, which occurred recently, and far-reaching measures to block and reduce its consequences have a direct and indirect impact on complex social spheres, including opportunities for committing crimes offline and on the Internet (BUIL-GIL et al., 2020; JOMARTOVA et al., 2021). The Covid-19 pandemic has radically changed life (HAWDON et al., 2020), showing all countries of the world how vulnerable a person can be not only to a deadly disease, but also to other threats, including those posed by digitalisation technologies (SULEIMENOV et al., 2022).

For example, O. M. Dzhanadilov and M. G. Azhibayev (2019) investigated the issues of countering crime in the field of information circulation and communication in the light of the current criminal legislation of Kazakhstan. The researchers also proposed recommendations for solving problems aimed at developing scientifically sound proposals for improving the legislation and practice of criminal prosecution bodies of Kazakhstan during pre-trial investigation to combat criminal offences in information and communication networks. R. S. Graham and S. K. Smith (2019b) examined the investigation of cybercrimes and theories of cyber-victimisation. Special attention in these studies was also paid to four categories of cybercrime, which, according to the authors, are the most dangerous for society: cybercrime, cyber pornography, cyber

violence, and cyber fraud. The results of the study by T. K. Yerjanov et al. (2018) indicate new types of cybercrime – cyberterrorism and identity theft for the purpose of committing crimes – that could be included in the Convention on Cybercrime. S. Zabikh (2020) investigated the international experience in the legal provision of information security and the possibility of its application in the Republic of Kazakhstan, in particular, the researcher notes that the security of the information space entails the protection of the rights and interests of man and citizen, society and the state in the information sphere from real and potential threats.

The study analysed the national acts of Kazakhstan and international legal acts in the field of prevention and combating crimes committed in the field of informatisation and communications. The analysis of statistical data on offences in this area was also necessary for the study. The basis of this study was also the theoretical works of researchers on the study of various aspects of offences in the field of informatisation and communications, and the papers of those researchers who studied the impact of information and communication technologies on the life of society and the legal sphere of the state, the consequences of digitalisation of society in the context of globalisation.

Undoubtedly, the considered studies have great practical value for representatives of the competent criminal justice authorities, both in the Republic of Kazakhstan and in other post-Soviet states. However, as noted by K. Mačák (2017), international law fails to cope with modern problems caused by rapid technological development, which may have such consequences in the future as the decline of interstate cyberspace management or the recalibration of legal approaches to its regulation. For this reason, further study on the issue of cybercrime, its types and methods of combating it, is relevant.

Accordingly, the purpose of the study was to analyse the existing national legislation of Kazakhstan and international legal acts for compliance with their current realities in combating offences that arise in the field of informatisation and communications, research, comparison of existing terminology and qualification of these crimes, development of its original classification based on the analysis.

MATERIALS AND METHODS

Accordingly, the study used the method of analysis to examine the theoretical foundations of the occurrence, development trends, and features of this type of offence, a statistical method to analyse and summarise statistical data, and a comparative legal method to investigate the legal regulation of offences in the field of informatisation and communications in other countries, to detect its similar and distinctive features with national legislation in this area and to obtain material for the formulation of practical proposals for its improvement with the

borrowing of positive international experience. The following methods were also applied: system approach, induction, deduction, classification, and modelling. Combined in a complex, these methods allowed for achieving the set goal of the study. In order to best achieve the research objectives, their implementation was divided into three independent stages, namely: theoretical research, analytical research, and the development of practical proposals and recommendations based on the research conducted.

At the first stage of the study, the theoretical basis was analysed, the causal relationships between crimes of this type and the living conditions of society, the influence and role of information and communication technologies on the emergence and further development of cybercrime were investigated. At the second stage of the study, available statistical data on offences in the field of informatisation and communications was examined, which included a comparative analysis of existing topical problems and those that may potentially arise in the future in this area, with the help of the current national legislation of Kazakhstan, international legal acts, and legislation of other countries related to the fight against cybercrime.

At the final third stage, it was concluded that it is advisable to create new models of international cooperation to combat and prevent offences in the field of informatisation and communications. Moreover, in order to improve the legislative regulation of the issues of combating offences in the field of informatisation and communications, and eliminating its gaps, the original classification of offences of this type was proposed, based on the provision that the generally accepted classification dividing them into crimes committed through the use of digital technologies, and those whose object is information itself in the digital field, it does not fully reflect their specificity and isolation from other types of offences.

RESULTS AND DISCUSSION

The establishment of a digital world community, the processes of globalisation, the widespread use of information and communication technology have not only positive effects in the form of comfortable conditions for daily life and increased economic, social, and cultural cooperation between states, but also have a negative impact, with a growing number of transnational crimes, in particular, those committed in cyberspace. It is extremely difficult to combat cybercrime, prevent and investigate crimes of this nature, since the territory in which they were committed may not be limited only to the borders of one state. Law enforcement agencies of states around the world have a need both to understand the very nature of cybercrime, its causal relationships with the above-mentioned trends of a social and technological nature, and the need for theoretical

developments and recommendations for its prevention and control, which can be successfully applied in their practical activities.

Using, for example, the Internet, a criminal, staying in one country, can commit criminal acts with bank cards that belong to citizens of other states. This statement concerns almost all information-related crimes, in particular, those that infringe on the security of computer information. In this case, this refers both to the illegal access of the criminal to the information that belongs to one or another owner or user, and directly illegal access to the devices that contain it (computers, tablets, mobile phones, and other devices intended for transmission and exchange information). At the same time, another debatable question arises, what exactly is the object of this crime – the rights and interests of the individual in the field of safe handling of information that have been violated, or the totality of public relations for the safe use of information. The question arises about the sufficiency of the generally accepted qualification of offences in the field of informatisation and communications, such as those committed through the use of digital technologies, and those whose object is directly information in the digital field.

It is obvious that in such global conditions, in a digital world in which only virtual borders can exist, it is not possible to prevent or destroy criminal activity in the field of informatisation and communications by the efforts of law enforcement agencies of one state. Moreover, it can be stated that the existing mechanisms for combating organised crime in the field of informatisation and communications, and the existing models of international cooperation to combat it, seem ineffective and require a choice between rethinking the prospects for their further preservation, or their complete renewal, according to the new challenges facing law enforcement agencies of countries around the world in the fight against this type of crime. First of all, this refers to the rapid adaptation and transformation of cybercrime to new emerging information and communication technologies, and the reproduction of its new types according to them. Moreover, such type of offences in the field of informatisation and communications as cyber attacks, in particular, crimes against confidentiality, integrity, and availability of computer data and systems, creation, distribution, and use of malicious computer software on the Internet, which have become widespread in recent decades not only in Kazakhstan, but also in a number of European countries (ORUC and YERALAN, 2020).

This category of crime is particularly dangerous because it is not only an attack on the digital security of individuals or legal entities; such crimes can affect the interests of the entire state, as demonstrated by a number of cybercrimes, such as the hacking of official websites of public authorities, which resulted in the blocking of their activities. The conditions of modern human life, the ubiquity of information and communication technologies both facilitate their social,

economic, and political daily lives and create additional difficulties and obstacles. First of all, this refers to the fine line that exists between a person's personal life, its privacy, and information about a person that is freely available. These include, in particular, medical information about a person, which was demonstrated during the outbreak of the Covid-19 pandemic, information related to bank secrecy, in connection with the emergence of the ability to make monetary transactions using the Internet, and, for example, information about a person that contains details of their private life, in particular, due to the emergence of a wide network of social messengers.

Such a line is fragile and bordering on both the preservation of the human right to inviolability of personal life and other legitimate rights that ensure the life of a person as a social individual. For example, human rights relating to the protection and defence of intellectual property rights are noted in this context, which is particularly relevant in the context of the widespread dissemination of information through the Internet and other information and communication technologies. This provision on the differentiation of personal and public information applies not only to individuals, but also to legal entities and their business activities, since most of the information about them can be obtained without any permission (for example, about their form of ownership, field of activity, or location of the head office). While the information that concerns the activities of public authorities, in many cases, is classified, based on the understanding of the need for a set of measures to ensure the security of the state.

In general, the academic world today defines two main types of crimes in the field of informatisation and communications: those that are committed directly through the use of computer technology and those that are committed by infringing on information or the right to it. If the first case refers, for example, to the spread of malware via the Internet, cyberterrorism, cyberbullying, cyber-attacks, then in the second case, the encroachment concerns information directly, in particular, it may be the dissemination of false information via the Internet to destabilise the social, political, or economic life of a country. Since the generally accepted classification of crimes in the field of information and communication does not fully reflect the specifics of these crimes, it is advisable to propose expanding it to the following types:

(1) Depending on the sphere to which criminal activity in the field of informatisation and communications is directed: economic (fraudulent withdrawal of funds from bank cards using computer technology), political (dissemination of knowingly untrue, false information about a particular political figure of the country using the Internet), social (dissemination of knowingly untrue, false information about increase in

prices for certain vital services for the population using the Internet in order to destabilise the situation in the country).

(2) Depending on the number of subjects targeted by criminal activity in the field of informatisation and communications: individual (cyberbullying, distribution and publication of intimate photos of a person on social networks) and collective (distribution and publication of classified information about the income of certain figures belonging to the same political party).

(3) Depending on the subjects themselves who are victims of criminal activity in the field of informatisation and communications: state (cyber-attacks on official websites that belong to state authorities), crimes against individuals (hacker attacks on a computer, mobile phone or other digital device belonging to an individual in order to obtain personal information), crimes against legal entities (hacker attacks on a computer, mobile phone, or other digital device belonging to a legal entity in order to obtain information representing a trade secret).

This classification is not the final result of research, it can be expanded with the help of other parameters. For example, as indicated earlier, it is possible to apply a more detailed classification to crimes that are committed in the field of information circulation: crimes related to the creation and use of information and communication technologies, and ways to ensure them; crimes related to the creation and further use of information resources based on the generation, collection, processing, preservation, accumulation, search, dissemination, and provision of information; crimes related to the protection of information and the rights to it of relevant subjects. With regard to crimes that are committed in the field of information circulation, it is also possible to consider separately the types of crimes committed in the field of communications, based on which stage of the process of ensuring information exchange has become the object of criminal misconduct: during the communication itself, routing, transmission or reception of signs, signals, written images, sounds or messages of any kind by radio, wired, optical, or other electromagnetic systems.

Practice demonstrates the fact that cybercrimes committed in the sphere or with the help of information and communication technologies are often committed in conjunction with other types of crimes. Thus, for example, such a crime as theft can be carried out in conjunction with the stealing and appropriation of official documents, unauthorised interference in the operation of an automated system, which leads to leakage of information or its forgery, violation of the order of its routing. From this example, it is clear that when sentencing for this crime, it will be taken into account that cybercrime in this context was an integral part of the crime plan, the purpose of which was the unlawful seizure of someone else's

property and money. In this case, when considering complex elaborate crimes, it is also necessary to note 'cyber-raiding', a popular scheme for committing cybercrimes, when officials authorised to make changes to state registers of property rights and information about legal entities enter false information into them, which gives their accomplices the opportunity to illegally seize the property of one or another enterprise, and, in some cases, even by itself, implying the interception of management and control functions by attackers.

Cybercrime, apart from its complex nature, which is reflected in its high adaptability to new information and communication technologies, is simultaneously complex, both for its prevention and for its investigation by the law enforcement agencies of a single state. In this regard, the already existing bilateral and multilateral international agreements on cooperation in the field of criminal proceedings on mutual assistance in the investigation of crimes in the field of informatisation and communications, to which the Republic of Kazakhstan is a party, as well as national legislation, require updating. It is also necessary to conduct a detailed analysis of the practice of combating cybercrime before concluding international legal acts for the future, to include effective mechanisms to combat it. As cybercrime itself changes, reproducing new types of crimes, in connection with the development of information and communication technologies, so it is necessary to change the legislation at the national and international levels, which regulates the fight against it, to ensure the effectiveness of the work of competent law enforcement organs in the new emerging realities of a rapidly changing world.

It is indisputable that the main value of any democratic state is the life, health, freedom, security of the citizens of this country, and its main task is to ensure the legitimate rights and interests of its citizens, and protection in case of their violation. According to the Constitution of the Republic of Kazakhstan (1995), the process of building a sovereign, democratic, secular, legal, and social state is inextricably linked with the idea of increasing the effectiveness of measures to combat phenomena that hinder this process, one of which are offences (AYUPOVA et al., 2021). Modern information and communication technologies expand the capabilities of a person in various spheres of their activity, help in the implementation of the principle of freedom of capital, goods, services, and labour, at the same time, open up new opportunities for the implementation of illegal acts. Criminal behaviour through technology is often the result of people taking technologies designed for one purpose and finding new, illegal ways to use them (GRAHAM and SMITH, 2019a). Despite the indicated negative trend, the steady increase in the use of online resources and the responsible approach of governments to the prevention of cybercrime have created an ecosystem that requires the empowerment of people (KIKERPILL, 2020). The typology of

cybercrime in the world, as a rule, focuses on three different topics: the characteristics of offenders, the types of crimes committed by cybercriminals, and sentences imposed on cybercriminals (HADZHIDIMOVA and PAYNE, 2019). This classification is quite generalised and does not fully reflect the specifics of crimes in the field of informatisation and communications. In addition, in each state, cybercrime has its own characteristics.

Therefore, as noted by S. Zabikh (2020), the key problems in the Republic of Kazakhstan in the field of information security are the prevalence of malware on personal computers and mobile devices, low legal literacy of the population, information and communication technology workers, and heads of information security organisations; violation by state and non-state actors of informatisation and users of information and communication technology services established technical standards; personnel errors and technological failures; actions of international criminal groups, communities, and individuals on embezzlement in the financial and banking sector. Digital illiteracy among the population in many countries, including Kazakhstan, among older and elderly people, makes them easy victims of crimes in the field of informatisation and communications. This statement is confirmed by the results of studies that show that awareness of cyber threats mediates the relationship between knowledge and defensive behaviour, but only if the knowledge is specific and relates to IT protection courses (KLEIN et al., 2022).

The main legal enactment in the Republic of Kazakhstan, which is dedicated to combating crimes in the field of informatisation and communications, is its Criminal Code of the Republic of Kazakhstan (2014). Thus, Chapter 7 provides for such crimes in this area as unlawful access to information, to an information system, or a telecommunications network, unlawful destruction or modification of information; disruption of an information system or telecommunications networks; unlawful possession of information; coercion to transfer information; creation, use or distribution of malicious computer programmes and software products; illegal distribution of restricted access electronic information resources; provision of services for the placement of Internet resources pursuing illegal purposes; illegal modification of the identification code of a cellular subscriber device, subscriber identification device, and the creation, use, distribution of programmes to change the identification code of a subscriber device. The Law of the Republic of Kazakhstan No. 349-I "On State Secrets" (1999), which defines the legal basis and a unified system for protecting state secrets in the interests of ensuring national security of the Republic of Kazakhstan, and Law of the Republic of Kazakhstan No. 567-II "On Communications" (2004), which provides the legal basis for activities in the field of communications in the Republic of Kazakhstan, defines the powers state

bodies that regulate this activity, the rights and obligations of individuals and legal entities to whom it is provided or who use communication services.

However, despite the existence of legal acts that regulate the issues of combating crimes in the field of informatisation and communications, the available statistical data in the Republic of Kazakhstan indicate that the number of completed cases, including those sent to court, for crimes registered in the territory of Kazakhstan committed in the field of informatisation and communications is decreasing: in 2017, only 2.8% of the registered cases were sent to court, in 2015 – 13% (24), in 2016 – 22% (29) (TEMIRALIEV and OMAROV, 2019). Moreover, such a problem is not on the agenda exclusively of the law enforcement agencies of the Republic of Kazakhstan, all countries of the world face similar problems, including, for example, Spain, in which there is a tendency to understate information to the police with widespread cyberbullying, which has certain negative consequences for anti-crime policies (KEMP et al., 2020). The reason for this problem lies in the unsystematic structure of the criminal justice bodies and their qualifications, competent in solving such crimes, so many urgent problems of informatisation arise due to the fact that society has not sufficiently covered the process of training and retraining of young employees, which does not fully meet modern requirements (RASULEV and SADULLAYEV, 2021).

There is also no comprehensive approach in the legislation of the Republic of Kazakhstan on the issue of criminal liability for crimes committed in the field of informatisation and communications, therefore, there is an obvious need for a more detailed description and classification of crimes in this area, which would help prevent negative trends in combating cybercrime at the present stage. It is the consolidation of specific signs of cybercrime at the legislative level in the Republic of Kazakhstan that would assist in creating its universal definition, which can be used in the future in international conventions, and in international criminal investigation (MAČÁK, 2017). Among the reasons for the wide spread of crimes in the field of informatisation and communications in the Republic of Kazakhstan, it should also be noted the low level of cyber literacy and knowledge of the basics of cyber hygiene among the population, equally, both individuals and legal entities, as mentioned earlier. At the same time, the acquisition of knowledge or skills related to the types and content of cybercrime is an important condition in the digital age (SOYLU et al., 2021; BYELOV, 2018).

A significant legislative gap is the absence of a single universal international treaty on cybercrime, there are only basic convention bases, which are contained in the provisions of existing regional agreements, such as the Computer Crime Convention (2001) and Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic

nature committed through computer systems (2003); Arab Convention on Combating Information Technology Offences (2010); Agreement on cooperation between the Member States of the Commonwealth of Independent States in combating crimes in the sphere of computer information (2001); Agreement between the governments of the member states of the Shanghai Organization on Cooperation in the field of ensuring international information security (2009); African Union Convention on Cyber Security and Personal Data Protection (2014). Obviously, the absence of such a universal legal act regulating the issues of combating cybercrime and prevention of crimes in the field of information and communication significantly complicates cooperation, both between the Republic of Kazakhstan and other states, in the field of criminal proceedings in the said sphere.

CONCLUSIONS

Thus, the rapid information development of society and the introduction of the Internet and other computer systems into all spheres of public life, such as the education system with the use of distance learning methods or in public administration with the introduction of e-democracy technologies, are accompanied by negative phenomena for the world community, along with positive achievements for it. The most dangerous for Kazakhstan, and for other countries of the world, are those phenomena of an unlawful and destructive nature that lead to an increase in the number of crimes committed in the use of electronic devices (computers), systems, and computer networks, as well as telecommunication networks, since they inhibit positive trends in the development of society in the social, political, and economic spheres, they cause material damage to the state, individuals, and legal entities, that is, they are destructive in their content for all subjects of information relations.

Criminal offences committed in the field of information and communication are to be understood as illegal acts committed through the use of information and communication networks, and those committed directly through the illegal access and use of information. The peculiarities of the formulation of the norms of the national legislation of Kazakhstan regarding this category of crimes complicate to a certain extent, and in some cases practically make their application impossible, provoke errors in the qualification of crimes, and also cause their ambiguous understanding by law enforcement and judicial officials. Considering both the specifics of crimes in the field of informatisation and communications, and the speed of their spread, it is necessary to actively work with practising lawyers and legal theorists to develop innovative methods to prevent and spread such crimes. This paper concerns both the updating of the legislation of the Republic of Kazakhstan, and the revision of existing

international agreements in this area of criminal proceedings. It is also necessary to take measures to increase the literacy of the population regarding cybersecurity, and to involve in such professional development not only physically, but also legal entities and representatives of public authorities.

REFERENCES

Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. (2003). https://rm.coe.int/168008160f.

African Union Convention on Cyber Security and Personal Data Protection. (2014). https://cutt.ly/HXa7sHn.

Agreement between the governments of the member states of the Shanghai Organization on Cooperation in the field of ensuring international information security. (2009). https://lex.uz/ru/docs/2068478.

Agreement on cooperation between the Member States of the Commonwealth of Independent States in combating crimes in the sphere of computer information. (2001). https://cis.minsk.by/page/866.

Arab Convention on Combating Information Technology Offences. (2010). https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

AYUPOVA, Z., KARAEV, A., MATAEVA, M., NECHKIN, A. & OSTAPOVICH, I. (2021). *Constitution of the Republic of Kazakhstan: doctrine and practice (to the 25th anniversary of the Constitution of the Republic of Kazakhstan).* Moscow: Publishing Center RIOR.

BOSSLER, A. M. & BERENBLUM, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499.

BUIL-GIL, D., MIRÓ-LLINARES, F., MONEVA, A., KEMP, S. & DÍAZ-CASTAÑO, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *1*(13), S47–S59.

BYELOV, D. (2018). Human rights for information in social networks: Constitutional aspect. *Journal of Legal Studies*, *22*(36), 49–52.

Computer Crime Convention. (2001). https://rm.coe.int/1680081580.

Constitution of the Republic of Kazakhstan. (1995). https://online.zakon.kz/document/?doc_id=1005029#sub_id=0.

Criminal Code of the Republic of Kazakhstan. (2014). https://online.zakon.kz/document/?doc_id=31575252#sub_id=0.

DZHANADILOV, O. M. & AZHIBAYEV, M. G. (2019). Problems of countering criminal offenses in information and communication networks. *Journal of Advanced Research in Law and Economics*, *10*(1), 134–143.

GRAHAM, R. S. & SMITH, S. K. (2019a). Organized cybercrime. *Cybercrime and Digital Deviance*, *1*, 133–150.

GRAHAM, R. S. & SMITH, S. K. (2019b). Understanding cybercrime in the digital environment. *Cybercrime and Digital Deviance*, *1*, 9–26.

HADZHIDIMOVA, L. I. & PAYNE, B. K. (2019). The profile of the international cyber offender in the U.S. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(1), 40–55.

HAWDON, J., PARTI, K. & DEARDEN, T. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*, 546–562.

JOMARTOVA, S., MAZAKOV, T., MUKHAEV, D., MAZAKOVA, A. & TOLEGEN, G. (2021). Intelligent System for Assessing the Socio-economic Situation in the Region. *Communications in Computer and Information Science*, *1463*, 437–447.

KEMP, S., MIRÓ-LLINARES, F. & MONEVA, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(4), 293–312.

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.

KLEIN, G., ZWILLING, M. & LESJAK, D. (2022). A comparative study in Israel and Slovenia regarding the awareness, knowledge and behavior regarding cyber security. *Research Anthology on Business Aspects of Cybersecurity*, *10*, 128–147.

Law of the Republic of Kazakhstan No. 349-I "On State Secrets". (1999). https://online.zakon.kz/Document/?doc_id=1012633.

Law of the Republic of Kazakhstan No. 567-II "On Communications". (2004). https://online.zakon.kz/Document/?doc_id=1049207.

MAČÁK, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law*, *30*(4), 877–899.

NURDAULET, I., TALGAT, M., ORKEN, M. & ZIYATBEKOVA, G. (2018). Application of fuzzy and interval analysis to the study of the prediction and control model of the epidemiologic situation. *Journal of Theoretical and Applied Information Technology*, *96*(14), 4358–4368.

ORUC, S. & YERALAN, S. (2020). A meta-study on future work in information and communication technologies. *Heritage and Sustainable Development*, *2*(2), 114–122.

RASULEV, A. & SADULLAYEV, G. (2021). Training of personnel in the field of countering cybercrime: The need and the requirement of time. *The American Journal of Political Science Law and Criminology*, *3*(2), 123–130.

SOYLU, D., MEDENI, T. D., ANDEKINA, R., RAKHMETOVA, R. & ISMAILOVA, R. (2021). *Identifying the cybercrime awareness of undergraduate and postgraduate students: example of Kazakhstan.* Nur-Sultan: Astana IT University.

SULEIMENOV, I. E., MATRASSULOVA, D. K., MOLDAKHAN, I., VITULYOVA, Y. S., KABDUSHEV, S. B. & BAKIROV, A. S. (2022). Distributed memory of neural networks and the problem of the intelligence`s essence. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 510–520.

TEMIRALIEV, T. S. & OMAROV, E. A. (2019). Problems of counteraction to crimes committed with the use of information systems and the ways of their solution. *Bulletin of the Institute of Legislation of the Republic of Kazakhstan*, *1*(55), 93–99.

YERJANOV, T. K., BAIMAGAMBETOVA, Z. M., SERALIEVA, A. M., ZHAILAU, Z. & SAIRAMBAEVA, Z. T. (2018). Legal issues related to combating cybercrime: Experience of the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics*, *8*(7), 2276–2291.

ZABIKH, S. (2020). International experience of legal support of information security and the possibilities for its application in the Republic of Kazakhstan. *Przegląd Politologiczny*, *3*, 71–85.

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