

UDC 343.3/7

https://doi.org/10.33619/2414-2948/93/16

**SOME ISSUES OF COUNTERING CRIMINAL OFFENSES IN THE FIELD
OF INFORMATIZATION AND COMMUNICATIONS
IN THE REPUBLIC OF KAZAKHSTAN**

©*Kalguzhinova A.*, ORCID: 0000-0002-3812-7504, SPIN-code: 4577-8991,
Karaganda University named on E.A.Buketov,
Karaganda, Kazakhstan, *k_aigul_75@mail.ru*

©*Mashabaev A.*, J.D., Karaganda University named on E.A.Buketov,
Karaganda, Kazakhstan, *mashabaev.a@mail.ru*

©*Ozbekov D.*, J.D., Karaganda University named on E.A.Buketov,
Karaganda, Kazakhstan, *d_ozbekov@mail.ru*

**НЕКОТОРЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ УГОЛОВНЫМ
ПРАВОНАРУШЕНИЯМ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ
В РЕСПУБЛИКЕ КАЗАХСТАН**

©*Калгужинова А. М.*, ORCID: 0000-0002-3812-7504, SPIN-код: 4577-8991,
Карагандинский университет им. акад. Е.А. Букетова,
г. Караганда, Казахстан, *k_aigul_75@mail.ru*

©*Машабаев А. Ж.*, канд. юрид. наук, Карагандинский университет им. акад. Е.А. Букетова,
г. Караганда, Казахстан, *mashabaev.a@mail.ru*

©*Озбеков Д. О.*, канд. юрид. наук, Карагандинский университет им. акад. Е.А. Букетова,
г. Караганда, Казахстан, *d_ozbekov@mail.ru*

Abstract. According to official statistics, in recent years there has been an increase in the registration of crimes that have a pronounced «intellectual» character. The objectively recorded growth of criminal encroachments using information technology dictates the urgent need for theoretical research and generalization of law enforcement practice. The authors made an attempt on the basis of the integrated use of historical and statistical methods to show the impact of improving the substantive criminal legislation on the state of investigative and judicial practice in cases of criminal offenses in the field of informatization and communications. The history of the regulation of responsibility for cybercrime in the criminal laws of sovereign Kazakhstan is traced. As possible ways to increase the effectiveness of countering crimes committed using information systems, the authors formulated proposals to change the form of statistical reporting.

Аннотация. По данным официальной статистики в последние годы отмечается увеличение регистрации преступлений, носящих ярко выраженный «интеллектуальный» характер. Объективно фиксируемый рост криминальных посягательств с использованием информационных технологий диктует настоятельную необходимость в проведении теоретических исследований и обобщения правоприменительной практики. Авторы предприняли попытку на основе комплексного использования исторического и статистического методов показать влияние совершенствования материального уголовного законодательства на состояние следственно-судебной практики по делам об уголовных правонарушениях в сфере информатизации и связи. Прослежена история регламентации

ответственности за киберпреступления в уголовных законах суверенного Казахстана. В качестве возможных путей повышения эффективности противодействия преступлениям, совершаемым с использованием информационных систем, авторами сформулированы предложения об изменении формы статистической отчетности.

Keywords: telecommunications networks, Internet, method of committing crimes.

Ключевые слова: сети телекоммуникаций, Интернет, способ совершения преступлений.

The active introduction and widespread use of information technologies, computers and communications in numerous spheres of public life, the availability of the Internet create additional criminal threats and necessitate the criminalization of new types of criminal activity.

The main objective of this study is to analyze the state of crime in the field of telecommunications networks, including the Internet. This task will be solved by a consistent definition of the range of criminally punishable acts forming the subject of the study (criminal law unit); generalization of official statistics (criminological unit). Within the framework of this article, we will limit the research plane to the consideration of crimes, as a feature of which “the use of telecommunications networks, including the Internet” is fixed.

In the course of writing the article, the theoretical material of Kazakh and Russian scientists, domestic legislation, as well as law enforcement practice were studied and used. The analysis of the norms on liability for criminal offenses in the field of informatization and communications under the criminal laws of the Republic of Kazakhstan of 1997 and 2014 is carried out. The general scientific dialectical method of cognition of social processes made it possible to investigate the problem from the point of view of the relationship between law and social processes taking place in society that require accounting and regulation. Formal-legal, historical-legal, comparative-legal methods, the method of structural-system analysis was used as private-scientific methods.

Historically, the regulation of responsibility for cybercrime in the criminal legislation of independent Kazakhstan is associated with article 227 of the Criminal Code of the Republic of Kazakhstan of 1997. The composition “Unlawful access to computer information, creation, use and distribution of malicious computer programs” belonged to the group of crimes in the field of economic activity [1]. Ten years later, another corpus delicti was included in the Criminal Code by the Law of the Republic of Kazakhstan dated January 08, 2007 (Article 227-1 of the Criminal Code of the Republic of Kazakhstan).

The Law of the Republic of Kazakhstan dated January 6, 2012 “On National Security of the Republic of Kazakhstan” identified information security as an independent type of national security. The normative definition of information security is fixed in the following wording: “this is the state of protection of the information space of the Republic of Kazakhstan, as well as the rights and interests of man and citizen, society and the state in the information sphere from real and potential threats, which ensures sustainable development and information independence of the country”.

The year 2014 can be called significant in terms of the significance of the changes made. In the Criminal Code of the Republic of Kazakhstan of 1997, as amended by the Law of the Republic of Kazakhstan dated April 23, 2014, Chapter 7-1 of the Criminal Code “Crimes against the security of information Technologies” was allocated, which includes nine elements of crimes. On July 03, 2014, a new criminal law of the country was adopted, Chapter 7 of which established responsibility for “Criminal offenses in the field of informatization and communications”. The number and signs of the composition of criminal offenses are preserved in the previous edition. At the same time, the

“use of information and communication networks” was provided as a sign (mandatory or qualifying) of other elements of criminally punishable acts.

Responsibility for independent compositions was provided for “Disruption of the operation of an information system or telecommunications networks” (Article 207 of the Criminal Code), “Creation, use or distribution of malicious computer programs and software products” (Article 210 of the Criminal Code).

Illegal access to an information system or modification of information transmitted over telecommunications networks have a qualifying value in the composition of theft (paragraph 4) of Part 2 of Article 188 of the Criminal Code) and causing property damage by deception or abuse of trust (paragraph 3) of Part 3 of Article 195 of the Criminal Code).

“The use of ... telecommunications networks” was fixed in the number:

- a mandatory feature of the compositions “Incitement of social, national, tribal, racial, class or religious discord” (Part 1 of Article 174 of the Criminal Code), “Actions provoking continued participation in a strike recognized by the court as illegal” (part 1 of Article 402 of the Criminal Code of the Republic of Kazakhstan);

- the qualifying sign of the compositions “Insult” (Part 2 of Article 131 of the Criminal Code); “Propaganda or public calls to unleash an aggressive war” (Part 2 of Article 161 of the Criminal Code); “Dissemination of deliberately false information” (paragraph 3) of Part 2 of Article 274 of the Criminal Code); “Encroachment on the honor and dignity of the President of the Republic of Kazakhstan and obstruction of his activities” (Part 2 of Article 375 of the Criminal Code); “Encroachment on the honor and dignity of a deputy of the Parliament of the Republic of Kazakhstan and obstruction of his activities” (Part 2 of Article 376 of the Criminal Code); “Insulting a representative of the authorities” (Part 2 of Article 378 of the Criminal Code).

In the future, the criminal policy was aimed at specifying terminology and tightening responsibility. At the same time, comprehensive adjustments due to the adoption of a special Law of the Republic of Kazakhstan “On Informatization” were introduced into the Criminal Code by the Law of the Republic of Kazakhstan dated November 24, 2015. The signs of “information and communication networks” were replaced by “telecommunications networks”; “information and communication network” by “telecommunications networks”; “information and communication network” by “telecommunications network”. Article 147 of the Criminal Code provides for an alternative composition “Dissemination of information about a person’s private life that constitutes his personal or family secret without his consent or causing significant harm to the rights and legitimate interests of a person as a result of illegal collection and (or) processing of other personal data”. The qualifying feature is the commission of the specified act “... using telecommunications networks” (Part 5 of Article 147 of the Criminal Code).

The innovations of the criminal law reflecting the consolidation of the “use of the telecommunications network” as an aggravating feature of the elements of crimes are presented in Table 1.

The current criminal legislation provides in various chapters of the Special Part of the Criminal Code for responsibility for the following criminal offenses committed with the help of information and communication technologies:

- 1) Criminal offenses against the person: — Driving to suicide, Insulting;
- 2) Criminal offenses against the family and minors — Involving a minor in committing criminal offenses, Involving a minor in prostitution;
- 3) Criminal offenses against constitutional and other human and civil rights and freedoms — Violation of the inviolability of private life and the legislation of the Republic of Kazakhstan on

personal data and their protection, Illegal violation of the secrecy of correspondence, telephone conversations, postal, telegraphic or other messages;

4) Crimes against the peace and security of mankind — Propaganda or public calls to unleash an aggressive war, Inciting social, national, tribal, racial, class or religious discord;

5) Criminal offenses against the foundations of the constitutional system and the security of the state — Propaganda or public calls for the seizure or retention of power, as well as the seizure or retention of power or forcible change of the constitutional system of the Republic of Kazakhstan, Separatist activity;

6) Criminal offenses against property — Theft, Fraud, Causing property damage by deception or abuse of trust;

7) Criminal offenses against public safety and public order — Mass riots;

8) Criminal offenses against the order of management — Threat or violent actions against a representative of the authorities;

9) Criminal offenses against justice and the order of execution of punishments, constitutional proceedings — Threat or violent actions in connection with the implementation of constitutional proceedings, justice or pre-trial investigation.

Table 1

IMPROVEMENT OF THE NORMS OF THE CRIMINAL CODE OF THE REPUBLIC
 OF KAZAKHSTAN REGARDING THE REGULATION
 OF THE QUALIFYING FEATURE “USING ... TELECOMMUNICATIONS NETWORKS”

<i>Formulation of the feature</i>	<i>Article of the Criminal Code of the Republic of Kazakhstan</i>	<i>Footing</i>
“Using ... telecommunications networks”	Article 179. Propaganda or public calls for the seizure or retention of power, as well as the seizure or retention of power or forcible change of the constitutional order of the Republic of Kazakhstan	The Law of the Republic of Kazakhstan dated July 26, 2016 “On Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on payments and payment systems”
	Article 180. Separatist activities	
	Article 256. Propaganda of terrorism or public calls to commit an act of terrorism	
“Through the use of telecommunications networks, including the Internet”	Article 373. Public insult and other encroachment on the honor and dignity of the First President of the Republic of Kazakhstan — Elbasy, desecration of images of the First President of the Republic of Kazakhstan — Elbasy, obstruction of the legitimate activities of the First President of the Republic of Kazakhstan — Elbasy	The Law of the Republic of Kazakhstan dated July 11, 2017 “On Amendments and Additions to Some legislative acts of the Republic of Kazakhstan on their alignment with the norms of the Constitution of the Republic of Kazakhstan”
	Article 105. Driving to suicide	
“Through the use of telecommunications networks, including the Internet”	Article 132. Involvement of a minor in the commission of criminal offenses	The Law of the Republic of Kazakhstan dated July 2, 2018 “On Amendments and Additions to some Legislative Acts of the Republic of Kazakhstan on the protection of children from information harmful to their health and development”
	Article 134. Involvement of a minor in prostitution	

<i>Formulation of the feature</i>	<i>Article of the Criminal Code of the Republic of Kazakhstan</i>	<i>Footing</i>
“Using ... telecommunication networks”	Article 316. Cruel treatment of an animal	The Law of the Republic of Kazakhstan dated December 30, 2021 “On Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on responsible treatment of animals”

The general conclusions of the analysis of the amendments and additions made to the Criminal Code of the Republic of Kazakhstan are the following. In the current criminal legislation, the protection of computer information and information systems, in addition to an independent chapter, is provided for in most chapters of the Criminal Code of the Republic of Kazakhstan. There is a tendency to increase the composition of crimes in which “the use of ... telecommunications networks” is fixed as an aggravating feature. In all articles of the Criminal Code, this feature is fixed among the signs of qualified personnel, with the exception of Article 134 of the Criminal Code, in which it is provided for in a specially qualified composition (paragraphs 1-1) of Part 3 of Article 134 of the Criminal Code). The constant updating of criminal legislation is aimed at effective and preventive provision of information security of the individual, society, and the state as a whole. In the process of modernization of criminal legislation, the increased degree of public danger, the objectively occurring prevalence and intensity, the social and criminological validity of “the use of telecommunications networks, including the Internet” in the commission of criminal offenses are taken into account.

In all types of criminal offenses, the qualifying attribute characterizes the method of committing the crime. At the same time, the legislator used various methods of constructing and formulating an aggravating feature:

- through the use of telecommunications networks, including the Internet,
- publicly or using mass media or telecommunications networks,
- by illegal access to the information system or changing information transmitted over telecommunications networks,
- in a public speech, a publicly displayed work, in the mass media or using telecommunications networks, including via the Internet,
- publicly or using mass media or telecommunications networks,
- using mass media or telecommunications networks.

In the process of qualification of the analyzed aggravating circumstance, it is necessary to use the definitions that are disclosed in the Law of the Republic of Kazakhstan “On Informatization” of November 24, 2015 (as amended) and “On Communications” of July 5, 2004 (as amended).

The Law of the Republic of Kazakhstan “On Informatization” defines an information system as follows: “an organizationally ordered set of information and communication technologies, service personnel and technical documentation that implement certain technological actions through information interaction and are designed to solve specific functional tasks”.

According to the Law of the Republic of Kazakhstan dated July 5, 2004 “On Communications”, telecommunications networks are understood as “a set of telecommunications facilities and communication lines that ensure the transmission of telecommunications messages, consisting of switching equipment (stations, substations, hubs), linear cable structures (subscriber lines, connecting lines and communication channels), transmission systems and subscriber devices”. The Law “On Informatization” classifies information systems into types according to various criteria: depending on the form of ownership-state and non-state, depending on the degree of access

— public and restricted access” (Article 37). Accordingly, public information systems contain public electronic information resources, information systems of limited access — electronic information resources of limited access. In turn, restricted access information systems are divided into: “1) information systems in protected execution classified as state secrets, the protection of which is carried out using state encryption tools and (or) other means of protecting information constituting state secrets, in compliance with the requirements of the secrecy regime; 2) confidential information systems”. The study of special literature shows various formulations of the type of crime we are analyzing: “Internet crime” (crime on the Internet) [2], “cyber-crime” [3], “crime in the field of computer information” [4], “information crime” [5], “crime in the field of high technologies” [6] and others. At the same time, the initial positions for the identification of an independent type (type) of crime are contained in the above-mentioned norms of the criminal law.

Thus, under the crime in the field of telecommunications networks, including the Internet, in the following, we will understand the totality of criminal offenses committed in cyberspace with or through telecommunications networks, in specific conditions of place and time. The criminological block of the study is presented by summarizing the reports of Form no. 1-M “On registered criminal Offenses” of the Committee on Legal Statistics and Special Records of the Prosecutor General’s Office of the Republic of Kazakhstan (<https://goo.su/V6Ioy7e>).

The year 2018 was taken as a basis, taking into account the criminalization of the sign of committing crimes “using telecommunications networks, including the Internet” (Table 2). Due to the fact that the report forms posted in the public domain do not highlight statistical indicators on qualifying grounds, we will limit ourselves to reviewing data on registered criminal offenses in the field of informatization and communications.

Table 2

DYNAMICS OF CRIMINAL OFFENSES REGISTERED IN THE REPUBLIC OF KAZAKHSTAN
 IN THE FIELD OF INFORMATIZATION AND COMMUNICATIONS, FOR THE PERIOD 2018-2022

	2018	2019	2020	2021	2022
Registered criminal offenses in the field of informatization and communications	72	108	62	74	85

With regard to the above data, we have taken into account that they do not reflect the true state of affairs, since they have a high degree of latency. According to official statistics, criminal offenses in the field of informatization and communications are characterized by insignificant absolute indicators. In the form of an official report posted in the public domain, statistical indicators on qualifying signs of criminal offenses are not highlighted. Of all the elements of criminally punishable acts, only “Internet fraud” is singled out separately (Table 3).

Table 3

DYNAMICS OF FRAUD REGISTERED IN THE REPUBLIC OF KAZAKHSTAN,
 FOR THE PERIOD 2018-2022

	2018	2019	2020	2021	2022
Fraud facts have been registered	29282	32286	33759	41083	43499
Registered facts of Internet fraud	517	7769	14220	21405	20569

As can be seen, over the period 2018-2022, there is a tendency to increase in registered cases of fraud, including Internet fraud in Kazakhstan, which is largely due to the intensification of preventive activities. In 2017, the Cybersecurity Concept “Cyber Shield of Kazakhstan” and the State Program “Digital Kazakhstan” were adopted. The approved Action Plan for the

implementation of the Cybersecurity Concept “Cybersecurity of Kazakhstan” until 2022 highlights organizational and legal, organizational and technical measures, measures for human potential management, popularization of measures for the safe use of information and communication technologies. During the period of implementation of the Concept of “Cybersecurity of Kazakhstan”, certain results have been achieved in cybersecurity, in particular, a market for high-quality professional services has been created, educational grants in this specialty have been increased, the culture of cybersecurity has been increased, round-the-clock monitoring of electronic government informatization facilities is provided.

In most cases, the use of information systems in fraudulent acts has a so-called “ordinary” character, since it is committed everywhere, more often against individuals. The difficulties in the criminal legal assessment of Internet fraud are caused by the use of special terminology, the modernization of computer programs and remote banking technologies, the lack of control over the placement of deliberately false information in information systems. It should also be noted that the statistical report of Form no. 1-M includes Appendix 1 “Information on registered offenses with the use of weapons and technical means” (<https://goo.su/V6Ioy7e>). Thus, in 2018, the bodies of legal statistics took into account 49 criminal offenses committed with the use of computer technology, in 2019 — 61, in 2020 — 432, in 2021 — 202, in 2022 — 151. As you can see, there are significant fluctuations in the registration of criminal acts: a consistent increase from 2018 to 2019, a sharp increase, almost seven times in 2020, then a halving in 2021, by one third in 2022. Thus, the statistical indicators highlighted in official statistics do not allow us to fully obtain information about the state and qualitative originality of crime in the field of telecommunications networks, including the Internet. At the same time, objective and real statistical data are needed to develop effective and efficient measures to prevent this type of crime, as well as other types of crime. Therefore, we consider it necessary to change the form of statistical reporting 1M “On registered criminal offenses and the results of the activities of criminal prosecution authorities”.

Resolution of the Government of the Republic of Kazakhstan dated March 28, 2023 no. 269 approved the Concept of Digital Transformation, development of the information and communication technologies and cybersecurity industry for 2023-2029. In order to resist hacker attacks and hacks, it is planned to further develop and maintain the created digital infrastructure of “Cyber Shield of Kazakhstan”. With the use of available online services (applications), citizens will be trained in the basics of cyber hygiene and fraud prevention.

The concept of the legal policy of the Republic of Kazakhstan until 2030, approved by the Decree of the President of the Republic of Kazakhstan dated October 15, 2021 no. 674, among the priority areas fixes the need for “codification of legislation in the field of information and communication technologies, communications, data processing, digital assets, industrial automation, information security, machine learning and artificial intelligence, protection of rights subjects of personal data”, as well as “the introduction of a separate offense, providing for responsibility for the use of artificial intelligence for criminal purposes”. For the purpose of uniform interpretation and application of the norms of the criminal law on crimes committed using telecommunications networks, including the Internet, we consider it necessary to clarify the issues of their qualification and differentiation with related crimes at the level of regulatory decisions of the Supreme Court of the Republic of Kazakhstan.

References:

1. Amanzholova, B. A., Bazarova, G. S., Kalguzhinova, A. M., & Ualieva, Z. B. (2016). Criminal Policy against Economic Offenses in Kazakhstan. *Journal of Advanced Research in Law and Economics*, 7(5 (19)), 972-981.

2. Dremlyuga, R. I. (2008). Internet-prestupnost'. Vladivostok. (in Russian)
3. Biekenov, N. A. (2014). Nekotorye problemy obespecheniya kiberbezopasnosti v Respublike Kazakhstan. *Vestnik Instituta zakonodatel'stva i pravovoi informatsii Respubliki Kazakhstan*, (1 (33)), 16-20. (in Russian)
4. Kozachenko, I. Ya., & Novoselov, G. P. (2015). Uголовное право. Osobennaya chast'. Moscow. (in Russian)
5. Piskunova, E. V. (2018). Informatsionnaya prestupnost': uголовно-pravovye i kriminalisticheskie aspekty. *Gosudarstvo i pravo v novoi informatsionnoi real'nosti*, (1), 248-266. (in Russian). <https://doi.org/10.31249/pras/2018.01.12>
6. Chirkov, D. K., & Sarkisyan, A. Zh. (2013). Prestupnost' v sfere vysokikh tekhnologii: tendentsii i perspektivy. *Voprosy bezopasnosti*, (2), 160-181. (in Russian). <https://doi.org/10.7256/2306-0417.2013.2.608>

Список литературы:

1. Amanzholova B. A., Bazarova G. S., Kalguzhinova A. M., Ualieva Z. B. Criminal Policy against Economic Offenses in Kazakhstan // *Journal of Advanced Research in Law and Economics*. 2016. V. 7. №5 (19). P. 972-981.
2. Дремлюга Р. И. Интернет-преступность. Владивосток, 2008. 238 с.
3. Биекенов Н. А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан // *Вестник Института законодательства и правовой информации Республики Казахстан*. 2014. №1 (33). С. 16-20.
4. Козаченко И. Я., Новоселов Г. П. Уголовное право. Особенная часть. М.: Юрайт, 2015.
5. Пискунова Е. В. Информационная преступность: уголовно-правовые и криминалистические аспекты // *Государство и право в новой информационной реальности*. 2018. №1. С. 248-266. <https://doi.org/10.31249/pras/2018.01.12>
6. Чирков Д. К., Саркисян А. Ж. Преступность в сфере высоких технологий: тенденции и перспективы // *Вопросы безопасности*. 2013. №2. С. 160-181. <https://doi.org/10.7256/2306-0417.2013.2.608>

*Работа поступила
в редакцию 14.07.2023 г.*

*Принята к публикации
23.07.2023 г.*

Ссылка для цитирования:

Kalguzhinova A., Mashabaev A., Ozbekov D. Some Issues of Countering Criminal Offenses in the Field of Informatization and Communications in the Republic of Kazakhstan // *Бюллетень науки и практики*. 2023. Т. 9. №8. С. 154-161. <https://doi.org/10.33619/2414-2948/93/16>

Cite as (APA):

Kalguzhinova, A., Mashabaev, A., & Ozbekov, D. (2023). Some Issues of Countering Criminal Offenses in the Field of Informatization and Communications in the Republic of Kazakhstan. *Bulletin of Science and Practice*, 9(8), 154-161. <https://doi.org/10.33619/2414-2948/93/16>