Economic Affairs, Vol. 68(Special Issue), pp. 987-993, May 2023
DOI: 10.46852/0424-2513.2s.2023.48

AESSRA

Review Paper

Political and Legal Aspects of Criminal and Administrative Responsibility for Information Security Offences in the Context of National Security of the Kyrgyz Republic

Bakyt D. Kakeshov[1]*, Baktygul K. Kanybekova[2], Nurman A. Seidakmatov[3], Aida O. Zheenalieva[1] and Almagul M. Kokoeva[4]

[1]Department of Criminal Law and Criminology, Kyrgyz National University named after Zhusup Balasagyn, Bishkek, Kyrgyz Republic
[2]Department of Theory and History of State and Law, Kyrgyz National University named after Zhusup Balasagyn, Bishkek, Kyrgyz Republic
[3]Institute of Law and State of the National Academy of Sciences of the Kyrgyz Republic, Bishkek, Kyrgyz Republic
[4]Faculty of Law and Customs, Kyrgyz-Uzbek International University named after B. Sydykov, Osh, Kyrgyz Republic

*Corresponding author: bakytkakeshov@gmail.com (**ORCID ID:** 0000-0003-1570-1072)

Received: 29-12-2022 **Revised:** 26-04-2023 **Accepted:** 06-05-2023

ABSTRACT

The research relevance is predefined by the peculiarities of modern state development taking place in the context of digitalization. This factor affects the dynamics of changes and transformations in both the political and legal institutions of the Kyrgyz Republic, which provokes the increased role of the information sphere in the state. The research aims to reveal political and legal instruments to influence individuals committing unlawful acts against information security in Kyrgyzstan. The analysis and synthesis, comparison, deduction, formal-legal and generalisation methods were used in the research. As a result, the modern information sphere includes both information and information infrastructure and persons performing operations with it. Thus, a separate system of regulation of social relations is being formed, which directly affects the state of security of modernised society. As a result, it can be established that the current society, both in Kyrgyzstan and in other states, is an information society and continues to develop on its basis. In this connection, the information sphere has acquired the character of a system-forming mechanism, based on which the functioning of public life, its political, economic and defence component, takes place. It has been established that the number of offences in the field of information security is growing, so there is a need to develop new legal instruments for their deterrence. The study revealed the role of the main state bodies and their activities in the sphere of counteraction to cyber threats in Kyrgyzstan.

HIGHLIGHTS

- The article aims to investigate political and legal instruments against information security offenses in Kyrgyzstan, considering digitalization's impact. It analyzes and synthesizes information, compares approaches, and highlights the information sphere's influence on societal security. It establishes modern society as an information society and emphasizes developing legal measures to deter offenses. The research also explores the roles of government bodies countering cyber threats in Kyrgyzstan.

Keywords: State Regulation of Information Activities, Digitalisation of Society, Modern Technology, Cyber-Extremism, Cyber-Security

How to cite this article: Kakeshov, B.D., Kanybekova, B.K., Seidakmatov, N.A., Zheenalieva, A.O. and Kokoeva, A.M. (2023). Political and Legal Aspects of Criminal and Administrative Responsibility for Information Security Offences in the Context of National Security of the Kyrgyz Republic. *Econ. Aff.*, **68**(Special Issue): 987-993.

Source of Support: None; **Conflict of Interest:** None

The effectiveness of public policy in ensuring and protecting information security is determined by various political and legal factors that influence the formation of quality strategies and plans in the state to protect citizens from various types of threats. The number of such threats is extremely high, so they can only be differentiated according to certain criteria, such as territoriality, the nature of probable harm, subjectivity (Cameron, 2021). At the same time, it should be noted that in modern conditions their system is expanding, which is due to the reform of social life. The latter is caused by the transformation of established social institutions, namely their modernisation in the light of information and communication technologies (Wiley *et al.* 2020). Their development and global spread in the world, including in Kyrgyzstan, has provoked significant changes in the life of society and citizens. The development of information and communication technologies has several advantages, such as increasing the digital consciousness of the people and modernizing some socially important processes. At the same time, globalization and informatisation in general have affected the number of threats, particularly in the information environment of the state. Thus, the relevance of research on information security is high today, due to the active course of the digitalization process both within Kyrgyzstan and other foreign countries (Patel and Chudasama, 2021; Nguyen and Reddi, 2021).

This issue has been studied by several scientists analysing several components and revealing their effectiveness and priority in modern social life. A.I. Moldazhiev (2020) and R.A. Mamasadykov (2020) established that the main aspects of legal sciences in the context of ensuring national security are currently being modified due to the influence of several factors that provoke contradictions, such as competition the rule of international law and the basis of political and diplomatic settlement of controversial issues. They argued that such challenges may result in circumstances in which the national security of the state may be threatened. The conclusion they reached is appropriate to be applied in describing the theoretical foundations of the organisation of security policy in the state, which should be based on four areas, namely social, informational, organisational, and technical.

The research aims to identify and analyse the political and legal measures used in KR to identify and prevent offences in the field of information security in the state. The research formed several objectives, namely, to study the concepts and main political strategies in Kyrgyzstan to ensure the cybersecurity of society, disclose the basis methods and forms of influence on persons committing offences against information security, characterize the activities of state agencies on the issue of ensuring national security; to analyse the role of information security in the national security system of Kyrgyzstan in today's conditions. The problem of the study was to express the political and legal approaches and concepts of KR in the process of countering offences in the information sphere, as well as the protection of information security as one of the most important components of the mechanism of national security.

MATERIALS AND METHODS

The analysis method was used to examine the basic attributes of information and national security. It was used to investigate their properties, which helped to establish links between them. In addition, analysis was applied in the study of the main concepts and principles that form the basis for the formation of public policy in the information sphere. Thus, this method was used to divide the overall object of work into such components as information security, national security, and offences in the information environment. The synthesis method was necessary to express the dependence between the above components. The role and place of information security in the system of KR national security mechanisms were determined using this method.

The comparison method was used to compare the two categories, namely "information security" and "national security", expressing their common and distinctive features. In addition, it was also necessary to compare the activities and measures implemented by different state bodies in Kyrgyzstan in the process of combating cybercrime. The comparison was applied to examine the system of national legislation regulating information relations, imposing liability on persons violating it and comparing legal norms with each other.

The deduction method was used in the study to identify the specific concept and functions of information security among the general understanding of the directions and goals of national security. It was used to investigate the peculiarities of the current information environment at the expense of knowledge about the general processes of social life under the conditions of digitalization.

The research topic of this study relates to the legal plane, which necessitates the use of a special scientific method, namely the formal-legal method. It has been applied to examine the content and aims of the various legal acts aimed at regulating information legal relations. Thus, the formal-legal method was used to study the KR Laws: Law of the Kyrgyz Republic No. 31 "On electric and postal communications" (2008), Law of the Kyrgyz Republic No. 59 "On information of a personal nature" (2008), Law of the Kyrgyz Republic No. 6 "On copyright and related rights" (1998), Law of the Kyrgyz Republic No. 210 (15) "On the protection of state secrets of the Kyrgyz Republic" (2017), Law of the Kyrgyz Republic No. 83 "On the obligatory copy of documents" (1997), Law of the Kyrgyz Republic No. 149 "On martial law" (2009), Constitution of the Kyrgyz Republic (2021), Criminal Code of the Kyrgyz Republic No. 127 (2021), Convention on cybercrime (Council of Europe, 2001), "The Concept of Information Security of the Kyrgyz Republic for 2019-2023" (2019), "The Concept of National Security of the Kyrgyz Republic" (2021).

The generalisation method was used to establish the correlation between the level of development and protection of information security and the effectiveness of the national security of the state. In addition, this method was used to study the threats that arise in modern society and can harm the information interests of citizens.

RESULTS AND DISCUSSION

General aspects of information security regulation in the context of national security

The formation and development of state policy in the sphere of information security is based on a certain methodology. Its effectiveness depends on the consistency of the reform of the security imperative as a mechanism formed based on the principle of protecting the individual, as well as the nation, from subjective and objective threats. As a result, sustainable socio-economic development conditioned by preventive approaches takes place. As such, the separation of information security from the system of national security forms is an important stage in the process of countering the external threats facing the modern information society.

The analysis of the political and legal foundations of different types of liability for breaches of information security should consider the peculiarities of these concepts. Both national security and information security encompass and protect the system of national interests of society from threats of various kinds, both internal and external. Given this, a breach of information security has a direct impact on the protection of national security. This dependence allows to differentiate national security into several distinct spheres, namely geopolitical, protective, economic, political, social, environmental, psychological, and informational (Senol and Karacuha, 2020; Gunduz and Das, 2020).

The directions of the described national state security system can be formed, which include the formation of operational programs aimed at the protection of national interests; organization of activities of national security monitoring bodies; restoration of its mechanisms, deformed because of emergencies. Comparison of the ideas of ensuring national and information security allows to establish that they can be implemented with the systematic use of approaches and tools of economic, information and propaganda, social, legal, and mechanical types.

Specifics of the operation and influence of public authorities on information security Protection Kyrgyz Republic

Particular attention should be devoted to the activities of state bodies in the sphere of information and national security in general. The State Committee for National Security of the Kyrgyz Republic (SCNSKR), which is active internationally with the Organization for Security and Co-operation in Europe (OSCE) Programme Office, should be mentioned first. As a result, a memorandum of cooperation on cyber security was concluded between them in Bishkek in 2021 with Kaspersky Cyber Security (State Committee for…, 2021).

The latter is an advanced international company operating in the field of information security as well as digital protection. This agreement is aimed at long-term international cooperation until 2030, and one of its main objectives is to build and implement a quality KR cyber security framework. The effectiveness of joint international work is evidenced by statistical data, as just six months after its implementation more than 60,000 phishing page attempts were blocked in Kyrgyzstan, thereby preventing the commission of information criminal offences (Alymbaeva and Alimakhunov, 2021).

Further consideration should be given to the operation of the Service for Regulation and Supervision in the Communications Industry under the Ministry of Digital Development of the Kyrgyz Republic (SRSCI), which aims to build a modernized, highly developed National Information Transmission Network, as well as its implementation in the international information environment. To analyse the main directions of SRSCI, it is worthwhile to consider the report for 2022, describing the information policy components implemented by it during the year (Report on the results…, 2022). SRSCI is of particular interest not only to other state authorities but also to the mass media and participants in the KR telecommunications market. An analysis of this document shows that cellular communication is an integral part of society's activities, as well as the global Internet. Regarding legal activities, SRSCI has been active in identifying threats to information security by monitoring telecommunications operators. Accordingly, in 2022 administrative penalties were applied, namely, fines were imposed on 33 entities for violating norms of operation in the field of electric and postal communications (Alymbaeva and Alimakhunov, 2021).

Legal aspects of information security regulation Kyrgyz Republic

The political foundations of information security protection in Kyrgyzstan were disclosed, and attention should be devoted to legal means. It is necessary to define the essence of information security when studying information crimes and security in general. Thus, according to Point 1.1 of the Concept of National Security of the Kyrgyz Republic (2021), the concept of "information security" is to be interpreted as the state of protection of individuals, society, and the state from information threats. In addition, this document discloses the content of internal and external threats that can be against the system of national security. It can be seen that clause 16 of the Concept of National Security of the Kyrgyz Republic (2021) identifies one of the internal threats, namely insufficient capacity to protect information space and domestic information resources, as well as the lack of significant progress in creating modern information and communication technologies and information space protection. The close relationship between national security and information security is evidenced by Section 4, Paragraph 20, which identifies the provision of information security by the state and the protection of citizens' data as one of the goals of the former. Also, in the Concept of National Security of the Kyrgyz Republic (2021) a separate Section 6.8 called "Information Security" is formed, which includes provisions on the key problems in this area, its objectives, and ways of their implementation. Thus, the Concept of National Security of the Kyrgyz Republic (2021) reveals general principles and tools for ensuring national security, highlighting information security as its separate component.

Particular attention should be devoted to the Concept of Information Security of the Kyrgyz Republic for 2019-2023" (2019), as its analysis allows to highlight the key problems in this area. These include: low level of security, ungovernability and lack of ownership of both legal and technical regulation of the information environment; rise of cybercrime; lack of preventive measures for cross-border cybercrime in the context of digitalisation; multi-complicated monitoring of the performance of Internet resources.

The legal problems described above contribute to society's insecurity against dangerous content disseminated on the Internet or through other information and communication technologies. Analysis of the legal concept of KR allows to note that in addition to external threats, there are active internal sources of threats, such as ineffective legislation, in the context of protecting users and limiting their access to publications of a destructive nature. In particular, the Constitution of the Kyrgyz Republic (2021) defines the basic principles based on which information is protected in the republic,

as well as the duties and responsibilities for their violation on the part of the subjects of the information environment. This document defines the role of the Cabinet of Ministers of the Kyrgyz Republic in the process of ensuring national security (art. 91), as well as the rights of citizens to receive, store and disseminate information (art. 33) and to express thoughts and opinions (art. 32) (Constitution of the…, 2021).

An analysis of the new Criminal Code of the Kyrgyz Republic No. 127 (2021) differs significantly from the previous version as it envisages the enshrinement of Chapter 40 under the title "Crimes against cyber-security" establishing liability for offences in the field of computer information. It contains four criminal offences, including: unauthorised access to computer information and electronic documents, or an information system or telecommunications network (Article 319); creation of malicious software products (Article 320); cyber-sabotage (Article 321); mass distribution of digital messages (Article 319).

Analysis of legal doctrine in the context of development and information security

M.E. Whitman and H.J. Mattord (2022) focused on international cooperation to prevent the spread of crimes against information benefits. They argue that information security has become particularly relevant due to the proliferation of the Internet and its mass use by citizens. The researchers believe that as a result, there has been a large-scale development of cybercrime, which is currently not limited to the characteristics of specific crimes, as this type of illegal activity is committed on the global information network. As such, it shares several features with all types of crime against the information and telecommunication environment, in which it is information that is the object of criminal attack. G. Culot *et al.* (2021) note that the list of such criminal offences includes pornography, fraud, the production and distribution of malware and the theft of sensitive material.

O.A. Panchenko (2020) focused on the experience of Ukraine in the field of the formation of legal institutions aimed at combating criminal offences in the field of information. Thus, he found that the main regulations governing this issue in Ukrainian society include Law of Ukraine No. 27-28 "On the Concept of the National Informatization Program" (1998) and Law of Ukraine No. 31 "On national security of Ukraine" (2018). In addition, there are special documents, such as Decree of the President of Ukraine No. 392/2020 "On the National Security Strategy of Ukraine" (2020), which provides for the establishment and operation of a special new authorised body as a working body, in particular the National Cyber Security Coordination Centre.

In contrast to previous researchers, B.J. Kilishbayevich (2023), K. Prislan *et al.* (2020), and K. Hughes-Lartey *et al.* (2021) analysed the overall role and importance of information security for modern society. In their opinion, the current stage of human development is characterised by a significant increase in the role of the information environment, a component of which is not only information but also the information infrastructure, the people who perform operations with data, as well as the mechanisms of regulation of this type of social relations. B.J. Kilishbayevich (2023) in his study notes that the information sphere in the context of the factor of social activity is reflected in the level of development of political, economic, social and defence sectors of the state. K. Prislan *et al.* (2020) point out that in the current societal conditions of both political and socio-economic development, there is an intense competition between the benefits such as the free flow, and exchange of information and the need to protect citizens from its negative impact, namely the maintenance of certain restrictions on the use of data.

Based on the foregoing, the effective functioning of national policy and national security is possible through the qualitative development of information security. The analysed studies show that this link is essential, as it unites all the main elements of national policy in a modernised society.

CONCLUSION

Based on this study, it can be established that information security plays an important role in protecting the information environment of the state as well as its resources. Given this, the level of its development depends on the satisfaction of information benefits and interests of society and the state, which affects their legal status as subjects of information legal relations. The study has established that the main department of

information security, as a structural component of national security, is the protection of citizens, in particular users of information and communication technologies, from the negative influence of external and internal factors. The latter provokes the formation of protection threats, as well as the integrity and availability of electronic data and materials. It has been argued in the paper that the development of information security and its effective provision is a necessary factor for improving the quality and effectiveness of state policy in the sphere of national security.

A separate focus in the study was given to the peculiarities of activities of some KR state bodies in the field of counteraction to crimes committed against information objects, namely the State Committee of National Security, the Ministry of Digital Development, and the State Agency of Communications. In addition, the study mentioned various types of legal acts relating to the criminalization of illegal acts in the information sphere. Based on this, it can be established that Kyrgyzstan, as a state, should implement an effective policy to develop the information environment and its security to prevent information expansion by other states or entities. This approach will ensure the rapid and successful integration of KR into the international information space. The study found that the development of society and technology is dynamic, which forms the obligation of the state to carry out a systematic review of legal institutions and update them following the requirements of the times so that they can function effectively and prevent the spread of information crimes.

The study devoted emphasis to the impact of new risks in the digital society on the criminalization of certain types of acts, namely extremism and cyber-extremism. The example of these crimes demonstrates the state's approach to protecting information security in the current environment and the development of criminal legislation. Consequently, the development of methodological principles and foundations for Kyrgyzstan's information security should continue, considering the scientific potential and practical recommendations. Consequently, as a result of the development of information policy at a high level, it will be possible to improve the state of information security of the state. Future research papers should focus on the specifics of the qualification of digital crimes.

REFERENCES

Alymbaeva, Z.A. and Alimakhunov, A.K. 2021. Threats and challenges to the information security of Kyrgyzstan. *Bulletin of Sci. and Practice,* **7**(2): 266-270.

Cameron, I. 2021. National security and the European Convention on Human Rights. 509 p. Brill, Leiden, Netherlands.

Constitution of the Kyrgyz Republic. 2021. Available in https://constsot.kg/wp-content/uploads/2022/06/constitution-of-the-kyrgyz-republic.pdf (Last Accessed on 9th June, 2023).

Council of Europe. 2001. Convention on cybercrime. Available in https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf (Last Accessed on 9th June, 2023).

Criminal Code of the Kyrgyz Republic No. 127. 2021. Available in https://cis-legislation.com/document.fwx?rgn=136047 (Last Accessed on 9th June, 2023).

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. 2021. The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM J.,* **33**(7): 76-105.

Decree of the President of Ukraine No. 392/2020 "On the National Security Strategy of Ukraine". 2020. Available in https://www.president.gov.ua/documents/3922020-35037 (Last Accessed on 9th June, 2023).

Gunduz, M.Z. and Das, R. 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks* **169**: 107094.

Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z. 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon,* **7**(3): e06522.

Kilishbayevich, B.J. 2023. Philosophical analysis of manipulation and information security problems. *Int. J. Edu., Soc. Sci. & Human.,* **11**(2): 754-758.

Law of the Kyrgyz Republic No. 149 "On martial law". 2009. Available in http://cbd.minjust.gov.kg/act/view/ru-ru/202647/10?cl=ru-ru (Last Accessed on 9th June, 2023).

Law of the Kyrgyz Republic No. 210 (15) "On the protection of state secrets of the Kyrgyz Republic". 2017. Available in http://cbd.minjust.gov.kg/act/view/ru-ru/111719 (Last Accessed on 9th June, 2023).

Law of the Kyrgyz Republic No. 31 "On electric and postal communications". 1998. Available in http://cbd.minjust.gov.kg/act/view/ru-ru/42 (Last Accessed on 9th June, 2023).

Law of the Kyrgyz Republic No. 59 "On information of a personal nature". 2008. Available in https://ihl-databases.icrc.org/en/national-practice/law-kyrgyz-republic-information-personal-nature-2008 (Last Accessed on 9th June, 2023).

Law of the Kyrgyz Republic No. 6 "On copyright and related rights". 1998. Available in https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/kg/kg146en.html (Last Accessed on 9th June, 2023).

Law of the Kyrgyz Republic No. 83 "On the obligatory copy of documents". 1997. Available in https://cis-legislation.com/document.fwx?rgn=135 (Last Accessed on 9th June, 2023).

Law of Ukraine No. 27-28 "On the Concept of the National Informatization Program". 1998. Available in https://zakon.rada.gov.ua/laws/show/75/98-вр#Text (Last Accessed on 9th June, 2023).

Law of Ukraine No. 31 "On national security of Ukraine". 2018. Available in https://zakon.rada.gov.ua/laws/show/2469-19#Text (Last Accessed on 9th June, 2023).

Mamasadykov, R. A. 2020. Problems of ensuring the national security of the Kyrgyz Republic. *Int. J. of the Humanities and Natural Sci.,* **10-1**(49): 176-178.

Moldazhiev, A.I. 2020. Terrorism as a threat to national security. *Int. J. Humanities and Natural Sci.,* **11-2**(50): 74-79.

Nguyen, T.T. and Reddi, V.J. 2021. Deep reinforcement learning for cyber security. In IEEE Transactions on Neural Networks and Learning Systems. Institute of Electrical and Electronics Engineers, Piscataway, USA. Available in https://arxiv.org/abs/1906.05799 (Last Accessed on 9th June, 2023).

Panchenko, O.A. 2020. Information security in the context of challenges and threats to national security. *Public Administration and Local Self-Government*, **2**(45): 57-63.

Patel, K. and Chudasama, D. 2021. National security threats in cyberspace. *National J. of Cyber Security Law*, **4**(1): 12-20.

Prislan, K., Mihelič, A. and Bernik, I. 2020. A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, **15**(9): e0238739.

Report on the results of the activities of the Communications Regulation and Supervision Service for 2022. 2022. Available in http://surl.li/hlcac (Last Accessed on 9th June, 2023).

Senol, M. and Karacuha, E. 2020. Creating and implementing an effective and deterrent national cyber security strategy. *J. of Engineering*, **2020**: 5267564.

State Committee for National Security will cooperate with Kaspersky Lab in the field of cybersecurity. 2021. Available in https://www.ktrk.kg/ru/news/s/63139 (Last Accessed on 9th June, 2023).

The concept of information security of the Kyrgyz Republic for 2019-2023. 2019. Available in http://cbd.minjust.gov.kg/act/view/ru-ru/13652 (Last Accessed on 9th June, 2023).

The concept of national security of the Kyrgyz Republic. 2021. Available in http://cbd.minjust.gov.kg/act/view/ru-ru/430815?cl=ru-ru (Last Accessed on 9th June, 2023).

Whitman, M.E. and Mattord, H.J. 2022. Principles of information security. 658 p. Cengage Learning, Boston, USA.

Wiley, A., McCormac, A. and Calic, D. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security* **88**: 101640.