Current Problems of Criminal Law Protection of Information Relations in the Border Sphere

Iryna Kushnir[†], Yurii Kuryliuk[††], Volodymyr Nikiforenko[†††], Yuliia Stepanova[††††]
Yaroslav Kushnir[†††††]
maxnik8888@gmail.com
[†]Department of administrative activity, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytsky, Ukraine
[††]Department of Theory and History of State and Law, National Academy of Management, Kyiv, Ukraine
[†††]First Deputy Head of the State Border Guard Service of Ukraine, Kyiv, Ukraine
[††††]Department of Research, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
[†††††] Department of Administrative Activity, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytsky, Ukraine

Summary

The article considers some issues of criminal law protection of information relations. With the emergence of new types of threats to Ukraine's national security in the field of protection and defense of the state border, the issues of development and strengthening of information protection become especially important. Proper compliance with information legislation also depends on the established responsibility for its violation, which rests on certain provisions of the Criminal Code of Ukraine. It is stated that these norms are placed in different sections and do not have a proper systematization. The article singles out the subjects of information relations in the border area, which are subject to criminal law protection: persons who are not bound by stable relations with the SBGS (who cross the state border of Ukraine, etc.); persons who are members of the SBGS (servicemen and employees); SBGS as a public authority (official and secret information, information about the activities of the agency, its officials, etc.).

Key words: *criminal law protection, information, information relations, border area.*

1. Introduction

At the present stage there is an intensive growth of the value and role of information, information resources and information technologies both in ensuring the rights of citizens to freely cross the state border, border security, and in the decision-making process by officials of the State Border Guard Service of Ukraine.

Regulatory regulation of information relations is important in the activities of public authorities, especially if it concerns components of the security and defense sector, in particular the SBGS, which is the administrator of information within the inviolability of the state border and protection of sovereign rights of Ukraine in its adjacent zone and exclusive (maritime) economic zone.

State and legal recognition of information relations, as well as responsibility for encroachment on them, has a short period, but at the same time the issues of responsibility and protection within the information sphere have already gained scientific interest. Mostly the issue of criminal law protection were included in the general review of responsibilities in the information sphere (L.P. Kovalenko, O.M. Seleznyova, G.M. Pisarenko, T.A. Kostetska, Y.E. Maksymenko, etc.). Protection of information relations from the standpoint of criminal law was studied by: M.V. Karchevsky (criminal-legal protection of information security), N.A. Savinova (criminal-legal support of information society development), O.K. Tugarova (criminal-legal support of information protection relations), etc. Theoretical and methodological developments of these scientists are fundamental in relation to a wide range of issues of information and border relations, but indicate the need for comprehensive systematic analysis, generalization and justification of areas for improvement in their integrated combination.

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.23

2. Theoretical Consideration

The activities of the SBGS cover a variety of external and internal areas within the protection of the state border and the organization of daily activities, so the information in its circulation is quite diverse. In addition, the order of access information is divided into open information and information with limited access [1]. Public information that was obtained or created in the process of performing their duties by SBGS officials or which is in the possession of SBGS bodies as subjects of power is open. Such information is open, so it is not subject to protection, and liability in this aspect may arise for the SBGS as managers of such information and only within the administrative and legal limits for refusal, failure to provide information or on other grounds provided by law [2]. Public information with limited access is confidential, secret and official [2]. Confidential is information about a natural person, as well as information to which access is restricted by a natural or legal person, the dissemination of such information is possible only at the request (consent) of the person in the manner prescribed by him, in accordance with the conditions and other cases specified by law [2].

Violation of the citizen's right to privacy, personal and family secrets entails criminal liability under Article 182 of the Criminal Code of Ukraine. AI Marushchak notes that the crime (Article 182 of the Criminal Code of Ukraine) implies another type of illegal means of access of citizens to information collection of confidential information about a person without his consent [3]. If the inviolability of private life was violated by an official of the SBGS as a result of official negligence, then if there are grounds for that, the act can be qualified under Art. 367 (425) of the Criminal Code of Ukraine. In this case, the victim of the crime can be any person (serviceman or person not related to service in the SBGS), without the consent of which the collected or disseminated confidential information was collected [4].

Article 163 of the Criminal Code of Ukraine provides for liability for breach of secrecy of correspondence, telephone conversations, telegraph or other correspondence transmitted by means of communication or computer. A qualifying feature is the commission of the same actions against statesmen or public figures or by an official, or with the use of special means intended for the secret removal of information. This article provides a number of illegal models of behavior of citizens regarding access to information [5].

Confidential information is information, access to which is restricted in accordance with the law, the disclosure of which may harm the person, society and the state. The list of information constituting a state secret in the field of protection of the state border is provided by the order of the Security Service of Ukraine from "On approval of the Code of information constituting a state secret". The Criminal Code of Ukraine provides for liability for disclosure of information of this nature in accordance with Article 328 "Disclosure of State Secrets". In case of loss of documents or other material carriers of secret information containing a state secret, there is a liability under Article 329 of the Criminal Code of Ukraine. Thus, in particular, the Judgment in case No. 127/19700/15-k of the Vinnytsia City Court of the Vinnytsia Region of September 18, 2015, in which Person_1 of the driver is a courier of the Vinnytsia Regional Special Communication Center of the state special communication enterprise, who was informed with the requirements of regulations governing the activities of special communications, in violation of paragraph 5.16 of the Instructions on the technology of reception, processing, storage, transportation and delivery of special communications, approved by the State Committee for Communications and Informatization of Ukraine from 02 July 1999 No. 21 secretly, p.p. 5.1.27, 5.1.30, Technological map of the workplace of a courier who performs a road route for the transportation of letter items, approved by the Deputy Director for Production on August 11, 2004. No. 73 for official use, item 2. 21 of the job description of the driver performing duties of the courier on combination from January 3, 2014, didn't check existence of the operating special permission for carrying out the activity connected with the state secret in the specified institution and handed over the above package with the requisites "Secretly" to the employee of the office PERSON_3, that there is no admission and access to state secrets, which in turn put his signature and imprint of the seal of the institution in the register No. 176 courier and later read the contents of the package , which contained request No. 15/894 secretly dated March 17, 2015 to the SBGS Administration to conduct an inspection under the Law of Ukraine "On Purification of Power" regarding an intelligence officer, with the attachment of non-secret documents. He was found guilty of committing a crime under Part 1 of Article 328 of the Criminal Code of Ukraine [6].

Вій SBGS officers in the case of disclosure of information of a military nature, which is a state secret, in the absence of signs of treason are liable in accordance with Art. 422 of the Criminal Code of Ukraine. L.F. Daderko, having investigated the issue of criminal liability for disclosure of state secrets, notes that servicemen for disclosure of information of a non-military nature, but which constitute a state secret, are liable under Art. 328 of the Criminal Code of Ukraine. Although, the scientist continues, there is no direct indication of this in this article, the servicemen are still special subjects [7].

Disclosure of information of a military nature that constitutes a state secret may take place in any way, including the use of mobile communications, as evidenced by case law. Thus, the verdict in case No. 760/8755/15-k

of the Solomyansky District Court of Kyiv found Person_1 (serviceman) guilty of committing a crime under Part 1 of Art. 422 of the Criminal Code of Ukraine, who during the use of mobile communication with his acquaintances repeatedly, disclosed information of a military nature, which according to Art. 4.4.7, 4.4.9, 4.4.5, 4.4.4, 4.4.3, 4.4.12 on secrecy constitute a state secret in the absence of signs of treason. As a result of the leak of information on the organization of intelligence activities, the national security of Ukraine in the field of state security and law enforcement was damaged, as the fact of using artificial satellites to probe the earth's surface was revealed, which will allow the interested party to take technical measures to disguise their positions. for the purpose of misleading, which may lead to the impossibility of obtaining intelligence information in the interests of units engaged in intelligence activities, and to reduce the state's defense capabilities [8].

Criminal liability for espionage, ie transfer or collection for transfer to a foreign state, foreign organization or their representatives of information constituting a state secret, provided by Articles 111 of the Criminal Code of Ukraine (in case of these acts by a citizen of Ukraine) and 114 of the Criminal Code of Ukraine foreigner or stateless person). According to the Law of Ukraine "On Military Duty and Military Service", only citizens of Ukraine may serve in the SBGS, while the law does not prohibit foreigners and stateless persons from holding the position of SBGS employees. In this regard, we can conclude that espionage acts committed by SBGS servicemen can be qualified only under Art. 111 of the Criminal Code of Ukraine, employees of the SBGS - as Art. 111, and Art. 114 of the Criminal Code of Ukraine (depending on their citizenship).

An essential feature of treason is the infliction of specific damage to information interests. Such interests in the border area, which are within the criminal law protection of Art. 111 of the Criminal Code of Ukraine, in our opinion, is the protection of information: SBGS to ensure the protection and defense of the state border of Ukraine; in information and information-analytical activity; in the functioning of telecommunication and information-telecommunication systems, automated control systems; on the activities of SBGS staff to perform the tasks, etc.

An analysis of normative sources and the scientific literature has shown a lack of unity in the understanding of the concept of "information security", which is necessary to define the object of the crime of "treason" and the correct classification of crimes against national security in general. Given this, it is necessary to normative consolidation of this concept, as well as to determine the content of information security of the state in the border area, as experience has shown that the inviolability of Ukraine's territorial integrity is closely correlated with state border protection [9].

Official information is information contained: in the documents of the SBGS, which constitute internal official correspondence; report notes; recommendations related to the protection of the state border or the exercise of control functions, the decision-making process and

public discussion and / or decision-making; information collected in the process of operational and investigative activities in the field of national defense and which is not classified as a state secret. For the transfer or collection for the purpose of transfer to foreign enterprises, institutions, organizations or their representatives of such information collected in the course of operational and investigative activities in the field of national defense, the person to whom this information was entrusted or became known in connection with official duties in the absence of signs of treason or espionage, criminal liability under Art. 330 of the Criminal Code of Ukraine.

Pointing to the excessive detailing of classified information that is under criminal law protection, OO Semenyuk offers his own approach to its differentiation. The scientist proposes to apply to the secret of an individual, confidential and state, the concept - "someone else's secret". He divides all crimes that encroach on "another's secret" into: illegal possession of another's secret; disclosure of another's secret; loss of material carriers containing someone else's secret [10]. It is interesting in the views of O.O. Semenyuk that the scientist equates all kinds of limited information. Such a position requires the coordination of the types of information enshrined in legislation, in particular in the Law of Ukraine "On Information" and other laws [10].

The existence of a separate section in the Criminal Code of Ukraine, devoted to "computer crimes", is associated with the growing role and scale of computer information systems in society, the popularity of global computer networks in all areas, which led to the emergence and permanent dynamics of various criminal encroachments related to the theft, misrepresentation or destruction of computer information, misuse of computers, as well as intentional disruption of computers [11].

Due to the use of information technologies, a large amount of information is processed, which is realized through the creation and application of information, telecommunication and information-telecommunication systems, as well as automated control systems, which are important for the protection of the state border. SBGS activities, which must comply with European trends in border security, ensure the national security of Ukraine and are a necessary component of the functioning of information and telecommunication systems of the SBGS. This is due to the need to protect human rights to access public information in the border area, protect information systems, networks and electronic information resources of

the SBGS, expand the use of information technology in the management of border units and public services, reliable exchange of information on control of persons, vehicles and cargoes crossing the state border within the functioning of the integrated interdepartmental automated system, as well as prevention of unauthorized interference in other departmental information resources in need of protection.

Bodies and subdivisions of the SBGS create and use information systems in the interests of state border protection, including data banks on persons who have crossed the state border of Ukraine, persons who have committed offenses against which are within the competence of the SBGS, persons who are not allowed by law entry into Ukraine or temporarily restricted the right to leave Ukraine, invalid, stolen and lost documents for the right to travel abroad and in other cases provided by the laws of Ukraine [12]. Due to the importance of such information, which has national, departmental and personal significance and is stored in the information resources of the SBGS, it is important to implement and maintain comprehensive measures for technical protection of information; prevention of unauthorized access to information and legal means of regulation, protection and defense of relevant information.

Therefore, the issue of protection of the content of processed information (transmitted, stored) in the communication (technological) systems of the SBGS, necessitates all effective mechanisms of protection not only technical but also criminal. Thus, on December 2, 2019, another fact of selling official data was documented, for which the senior lieutenant investigator of the National Police received UAH 1,300, after which he was detained in accordance with Art. 208 of the Criminal Procedure Code of Ukraine by the military prosecutor's office of the Kyiv garrison together with the territorial department of the DBR in Kyiv and the SBGS. The investigator received funds from the territory of the Russian Federation for the unauthorized sale of official information stored in computers and automated systems. The attacker sold information about persons, which is stored and processed in the automated subsystem "Risk" of the information and telecommunication system (hereinafter - ITS) "Gart-1", database "Arkan", "ARMOR" and others. Thus, on January 22, March 22 and May 14, 2019, the police officer received funds for his "services" in the total amount of UAH 16,350 "[13].

Widespread use of computer technology in the SBGS necessitates the use of legal mechanisms for technical protection of information security, which is reflected in a separate section of the Criminal Code of Ukraine, namely in Chapter XVI "Crimes in the use of electronic computers (computers), systems and computers computer networks and telecommunication networks ". In it, the legislator enshrined six types of crimes (Articles 361, 361-1, 361-2, 362, 363, 363-1 of the Criminal Code of Ukraine), which may take place in the activities of the SBGS. The objective side of these crimes is expressed in the following forms:

unauthorized interference in the work of electronic computers (computers), automated systems, computer networks or telecommunication networks (Part 1 of Article 361 of the Criminal Code of Ukraine);

creation for the purpose of use, distribution or sale, as well as distribution or sale of malicious software or hardware intended for unauthorized interference in the work of electronic computers (computers), automated systems, computer networks or telecommunication networks (h 1 Article 361-1 of the Criminal Code of Ukraine);

unauthorized sale or dissemination of information with limited access, which is stored in electronic computers (computers), automated systems, computer networks or on media of such information, created and protected in accordance with applicable law (Part 1 of Article 361- 2 of the Criminal Code of Ukraine);

unauthorized change, destruction or blocking of information (Part 1 of Article 362 of the Criminal Code of Ukraine) and unauthorized interception or copying of information (Part 2 of Article 362 of the Criminal Code of Ukraine), which is processed in computers, automated systems or computers computer networks or stored on the media of such information; violation of the rules of operation of electronic computers (computers), automated systems, computer networks or telecommunication networks or the procedure (rules) for protection of information processed in them (Article 363 of the Criminal Code of Ukraine); intentional mass distribution of telecommunication messages, carried out without the prior consent of the addressees (Part 1 of Article 363-1 of the Criminal Code of Ukraine) [14].

Approaching thoroughly the issue of improving the criminal law protection of information relations in the development of the information society in Ukraine, N.A. Savinova proves the need for an effective and efficient Concept of criminal law support for the development of the information society in Ukraine. It determines that the main purpose of such a Concept should be recognized by the achievement of criminal law measures necessary for the development of the information society in Ukraine the level of security of its basic resources and values from socially dangerous encroachments, information space security as a state of information security [15].

The concept of criminal law support for the development of the information society of Ukraine should reflect the state's attitude to comprehensive and consistent implementation and implementation of all stages of the Concept and its implementation, because only their harmony will effectively counteract socially dangerous acts that encroach on resources and values of the information society.].

The development of the information society has led to the emergence of various types of destructive influence on the consciousness, which are outside the law on criminal liability, to such N.A. Savinov includes:
1) transformed crime - a group of crimes that can be committed using remote communications;
2) cyber terrorism - a set of terrorist acts carried out in the form of remote communications in cyberspace;
3) cyber intervention - a set of aggressive actions in cyberspace aimed at interfering in the way of remote communications in the internal and external affairs of states in order to harm their sovereignty or the proper functioning of its governing bodies or major spheres of life, as well as similar actions regarding orderly interstate activities associations and their governing bodies;
4) information expansion - socially dangerous actions aimed at deliberate seizure for the purpose of further use in their favor of the information space, or a significant part of the information space of a particular state or group of states;
5) manipulation of the consciousness of the population - intentional influences on the consciousness of the population or its specific group, which is carried out using the information space [16-18].
The complexity, versatility and importance of information in modern society is reflected in the relations in the field of state border protection [19-21]. Accordingly, this is taken into account in criminal law. Crimes related to information in the border area include criminal liability:
for violation of the established procedure for access to information protected by law;
providing knowingly false information (criminal fraud);
use of information for criminal influence (threat);
concealment of information when there is an obligation to provide it.

Conclusions

Legal means of protection and defense of information relations require a comprehensive approach to improving the rules that determine the grounds, procedure and measures of application of negative remedies to violators, regardless of their legal status. Criminal protection of information relations and information is also carried out by establishing sanctions for interference in the work of information technologies, resources, databases, their damage, violation of the integrity of information, etc. Information can be the object, subject and means of committing crimes in the border area.
In general, the development of the information society determines the creation of appropriate conditions in the activities of the SBGS in two main areas:
first, access of citizens or interested authorities to open public information;
secondly, ensuring the protection of information with limited access, which has become known and processed in connection with the tasks of the state (regardless of the storage medium) [20].
The onset of criminal liability for the most serious violations of Ukrainian legislation on information as one of the types of liability, which is applied along with disciplinary, civil and administrative, is one of the means of protecting information relations, taking into account access to information and its protection in the border area.

References

[1] On information: Law of Ukraine of October 2, 1992. Information of the Verkhovna Rada of Ukraine. 1992. No 48. St. 650. With changes.

[2] On access to public information: Law of Ukraine of January 13, 2011. Information of the Verkhovna Rada of Ukraine. 2011. No 32. St. 314.

[3] Marushchak A.I. Information law: Access to information: a textbook. Kyiv: KNT, 2007. 532 p.

[4] Kushnir I.P. Issues of criminal law protection of information in the functioning of the State Border Guard Service of Ukraine. Current issues of criminal law, process, criminology and operational and investigative activities: abstracts of the II All-Ukrainian scientific-practical conference (Khmelnytsky, March 2, 2018). Khmelnytsky: NADPSU Publishing House, 2018. P. 169-172.

[5] Marushchak A.I. Information law: Access to information: a textbook. Kyiv: KNT, 2007. 532 p.

[6] The verdict in case No. 127/19700/15-k of proceedings No. 1-kp / 127/1180/15 of the Vinnytsia City Court of the Vinnytsia Region of September 18, 2015. URL: http://www.reyestr.court.gov.ua/Review/50803207

[7] Daderko L.F. Criminal liability for disclosure of state secrets. Scientific Bulletin of the International Humanities University. Jurisprudence. 2013. No 6-2. T. 2. pp. 82–85.

[8] Judgment in case No. 760/8755/15-k of proceedings No. 1-kp / 760/655/15 of the Solomianskyi District Court of Kyiv of 18 May 2015. URL: http: //www.reyestr.court .gov.ua / Review / 44222629.

[9] Kushnir I., Stepanova Y. Information security of the state in the border area as an object of treason. National law journal: theory and practice. 2018. No. 4 (32). T. 1. pp. 123-126.

[10] Semenyuk O.O. Prospects for the development of criminal law in the field of information protection with limited access. Legal Ukraine. 2017. No 1. pp. 44-56.

[11] Pravdyuk S.A. Computer offenses and information offenses: aspects of the relationship. Scientific Bulletin of the National University of Life and Environmental Sciences of Ukraine. 2013. Vip. 182. Part 3.

[12] On the State Border Guard Service of Ukraine: Law of Ukraine of April 3, 2003. Information of the Verkhovna Rada of Ukraine. 2003. No 27. art. 208.

[13] In the Kharkiv region, a police officer sold restricted information in Russia. URL: https://www.unian.ua/society/10809143-na-harkivshchini-policeyskiy-prodavav-v-rf-informaciyu-z-obmezhenim-dostupom.html.

[14] Tugarova O.K. Criminal and legal support for the protection of information relations. Scientific Bulletin of Kherson State University. Legal sciences. 2015. Vip. 4. T. 3. pp. 61-66.

[15] Savinova N.A. Improvement of criminal and legal support for the development of the information society in Ukraine. Legal informatics. 2012. No 2 (34). with. 60-65.

[16] Savinova N.A. Criminal-legal policy of ensuring the development of information society in Ukraine: dis ... Dr. Jurid. Science. : 12.00.08. Lviv. 2013. 510 p.

[17] Zadorozhnia H., Mykhtunenko A., Kuryliuk Y. et al. (2021). Protection of Information Sovereignty as an Important Component of the Political Function of the State. International Journal of Computer Science and Network Security. Vol. 21. No.9. pp. 151–154.

[18] Iasechko S., Kuryliuk Y., Nikiforenko V. et al. (2021). Features of Administrative Liability for Offenses in the Informational Sphere. International Journal of Computer Science and Network Security. Vol. 21. No.8. pp. 51–54.

[19] Kuryliuk Y., Khalymon S. (2020). Criminal profile of migrants' smuggler across the State Border of Ukraine. Amazonia Investiga. Vol. 9, No. 27. pp. 195–208.

[20] Svitlana Iasechko, Alla Ivanovska, Tetyana Gudz, Mykola Marchuk, Oleksandr Venglinskyi, Alla Tokar Information as An Object of Legal Regulation in Ukraine/ IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.5, pp. 237-242 https://doi.org/10.22937/IJCSNS.2021.21.5.33.

[21] Nikiforenko V. (2021). Modern Threads to the National Security of Ukraine Related to Incomplete Legal Formalization Process of Ukrainian State Border. Cuestiones Politicas. Vol. 39. No. 68. pp. 866–881.