CYBER SECURITY AND PERSONAL RIGHTS UNDER THE LEGISLATION OF UKRAINE

Iryna M. Sopilko
Doctor of Law, Professor, National Aviation University,
1 Lubomyr Husar Avenue, Kyiv, Ukraine, 03680
https://orcid.org/0000-0002-9594-9280
sopilko_i@ukr.net

Viktoriya B. Cherevatiuk
Candidate of Historical Sciences, Associate Professor,
National Aviation University
1 Lubomyr Husar Avenue, 1, Kyiv, Ukraine, 03680
https://orcid.org/0000-0002-4077-206X
vitacherev@ukr.net

Abstract. The aim of the article is to study the issue of achieving a balance between information protection in the cybersecurity system and freedom of expression in accordance with the position of the UN and the case law of the European Court of Human Rights. Research methods include the analysis of legislation on cybersecurity, generalization of legal information and cybersecurity practices. As a result, it was found out that in Ukraine the basic legal act on cyber security is the Law "On the basic principles of cyber security of Ukraine". The preamble of this Law defines the legal and organizational basis for protection of vital interests of citizens, society and state, national interests of Ukraine in cyberspace, main goals, directions and principles of state policy in cybersecurity, authorities of state bodies, enterprises, institutions, organizations, individuals and citizens in this field, the basic principles of coordination of their activities to ensure cybersecurity. Ukraine has ratified the Council of Europe Convention on Cybercrime of 23 November 2001. The Convention states that the fight against cybercrime is dictated, in particular, by the need to protect legitimate interests in the use and development of information technology. In particular, the Convention identifies the following types of cybercrime: offenses against the confidentiality, integrity and availability of computer data and systems; computer-related offenses; offenses related to child pornography; offenses related to copyright and related rights infringement. Finally, legal regulation of cybersecurity in Ukraine is based on the requirements of striking a balance between information protection and freedom of expression, the position of the UN and the case law of the European Court of Human Rights.

Key words: cybersecurity, cyberthreat, cybersecurity, cybercrime, cyberspace, personal data, public morality, intellectual property.

INTRODUCTION

The great strategist Winston Churchill said, "You have to pay for security, and in its absence, you have to pay back in full." However, as stated in the article, security is not created in exchange for rights and freedoms, but only together with them. This article emphasizes that the coexistence of rights and freedoms, on the one hand, and cybersecurity, on the other hand, is possible (Cyber security and/or human rights, 2018).

In democracies, the balance of rights and restrictions is set up in such a way that in order to exercise the rights of one, restrictions and obligations must be imposed on the other. This fully applies to the legal regulation of cyberspace. For example, one's desire to access information may be limited by the need to protect the other's personal data or trade secrets. Freedom of expression in cyberspace may be limited by the requirements of public morality. The desire to use pirated copies of audio and video products — the protection of intellectual property rights. According to prof. I.M. Sopilko, data leaks caused by cybersecurity gaps can have devastating consequences for any business. After all, this can undermine the company's reputation due to the loss of trust of consumers and partners. Also, leaking critical data can cost an organization its competitive advantage (Sopilko, 2021).

Thus, the problem of legal regulation of rights, freedoms and restrictions in cyberspace is relevant.

MATERIALS AND METHODS

In the scientific literature, cybersecurity and cybersecurity are associated with the rights and freedoms of citizens in a relatively small number of works. Article considers cybersecurity as a component of human rights information. The author's definition of the right to cybersecurity as an inalienable, inalienable right of a person to protect his important interests, including information rights, when using cyberspace. That is, the right to such a rule of law, which ensures, protects and defends human rights and freedoms when using cyberspace. It is proposed to include the right to cybersecurity to information human rights, but subject to appropriate legal regulation (Khobbi, 2020).

In the article concludes that at this stage of information technology development there is a threat to information security of Internet users. To achieve this complex task, the state needs to find a dynamic balance between freedom of speech, ensuring the right to information, its effective use as a means of civil society control over government actions, limiting the dissemination of classified information and maintaining moral and spiritual stability in society. Finding this balance will protect both the interests of society and the state, and promote the realization of the right of citizens to receive comprehensive and high-quality information (Yushchuk, 2009).

In the article among the components of cybersecurity policy, in particular, respect for fundamental values. All strategies place a strong emphasis on the need for cybersecurity policies to respect fundamental values, which typically include confidentiality, freedom of speech and the free exchange of information. Several strategies explicitly mention the need to maintain the openness of the Internet, and none of the strategies proposes to reduce openness in favor of enhancing cybersecurity. On the contrary, the openness of the Internet is usually described as a requirement for the further development of the Internet economy (Dziundziuk & Kotukh, 2020).

Recommendation CM / Rec (2016) 5 of the Committee of Ministers of the Member States on Internet Freedom (adopted by the Committee of Ministers on 13.04.2016 at the 1253rd meeting of the Ministers' Deputies) states that Internet governance mechanisms at national, regional or global level should be based on the understanding of Internet freedom. Any national decision or action aimed at restricting human rights and fundamental rights on the Internet must comply with international obligations and, in particular, be based on the law.

Therefore, the stated topic is relevant. This issue has been partially investigated in the works of co-authors (Dziundziuk & Kotukh, 2020; Cherevatiuk et al., 2022).

RESULTS AND DISCUSSION

According to Art. 3 of the Constitution of Ukraine, man, his life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value. Human rights and freedoms and their guarantees determine the content and direction of the state. The state is accountable to the people for its activities. The establishment and protection of human rights and freedoms is the main duty of the state. Thus, the state policy in the field of cybersecurity as part of the state's activities is aimed primarily at ensuring the constitutional rights of citizens.

In particular, Professor G.V. Foros (2019) believes that although the 1996 Constitution of Ukraine, as in the constitutional legislation of most foreign countries, defines the definitions of "cybersecurity", "cybercrime" and derivatives, but the key task in this area of state activity, which fundamental rights of human beings, as enshrined in the relevant international agreements reaffirming the right of everyone to freedom of opinion and the right to freedom of expression, including the right to seek, receive and impart information and ideas regardless of frontiers. , as well as the right to respect for private life, including in cyberspace (Foros & Zhohov, 2019). In particular, the authors emphasize that the cornerstone of one of the first regulations in this area— the Council of Europe Convention on Cybercrime of 23 November 2001— identified the need to strike the right balance between law enforcement interests and respect for fundamental human rights, as enshrined in the Council of Europe Convention[4]. on the Protection of Human Rights and Fundamental Freedoms of 1950, the United Nations International Charter of Civil and Political Rights of 1966 and other relevant international human rights treaties reaffirming the right of everyone to freedom of opinion, and the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and the right to respect for private life. The right to protection of personal information is also noted, as provided for in the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The basic legal act in Ukraine in the field of cyber security is the Law of Ukraine dated 05.10.2017 № 2163-VIII "On the basic principles of cyber security of Ukraine" (hereinafter— the Law № 2163-VIII). Thus, the preamble of this Law emphasizes that the Law defines the legal and organizational basis for protecting the vital interests of man and citizen, society and state, national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in cybersecurity, powers of state bodies. enterprises, institutions, organizations,

[4] Конвенцію ратифіковано Україною із застереженнями і заявами Законом від 07.09.2005 № 2824-IV

individuals and citizens in this field, the basic principles of coordination of their activities to ensure cybersecurity. In paragraph 5 of Art. 1 of the Law № 2163-VIII cybersecurity is defined as the protection of vital interests of man and citizen, society and the state in the use of cyberspace, which ensures sustainable development of information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security in cyberspace.

According to Part 1 of Art. 3 of the Law № 2163-VIII, the legal basis for cybersecurity of Ukraine is the Constitution of Ukraine, laws of Ukraine on the basics of national security, principles of domestic and foreign policy, electronic communications, protection of state information resources and information required by law, this and other laws Ukraine, the Convention on Cybercrime, other international treaties approved by the Verkhovna Rada of Ukraine, decrees of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine, as well as other regulations adopted in pursuance of the laws of Ukraine.

Thus, as noted above, the activities of the Ukrainian state in the field of cybersecurity are based on the Constitution of Ukraine and the Convention on Cybercrime, in particular, in the context of ensuring the constitutional rights of citizens. According to paragraph 1 of Part 1 of Art. 4 of the Law № 2163-VIII, the objects of cybersecurity are: constitutional rights and freedoms of man and citizen. According to Part 3 of Art. 5 of the Law № 2163-VIII, the Cabinet of Ministers of Ukraine in the field of cybersecurity ensures the formation and implementation of state policy in the field of cybersecurity, protection of human and civil rights and freedoms, national interests of Ukraine in cyberspace, fight against cybercrime; organizes and provides the necessary forces, means and resources for the functioning of the national cybersecurity system; formulates requirements and ensures the functioning of the information security audit system at critical infrastructure facilities (except for critical infrastructure facilities in the banking system of Ukraine). According to paragraph 1 of Part 1 of Art. 7 of the Law № 2163-VIII, cybersecurity in Ukraine is based on the principles of: 1) the rule of law, legality, respect for human rights and fundamental freedoms and their protection in the manner prescribed by law.

In pursuance of the provisions of this Law, the National Security and Defense Council (NSDC) of Ukraine adopted a decision of 14.05.2021 "On the Cyber-Security Strategy of Ukraine", which (Strategy) was approved by the Decree of the President of Ukraine of 26.08.2021 № 447/2021 Strategy). Chapter 4 "National Cyber-Security System: Principles of Development" of this Strategy emphasizes that Ukraine seeks to create the most open, free, stable and secure cyberspace in the interests of human rights and freedoms, social, political and economic development. Ukraine will build a national system of cybersecurity, based, in particular, on the balanced provision of the needs of the state and the rights of citizens, the rule of law, respect for fundamental values, human and civil rights. Section 5 "Priorities of Cyber Security of Ukraine and Strategic Goals" of the Strategy prioritizes cyber security of Ukraine, in particular, the protection of cyberspace to protect the sovereignty of the state and the development of society; protection of the rights, freedoms and legitimate interests of the citizens of Ukraine in cyberspace.

In Section 3 "National Cyberspace: Challenges and Cyber Threats" Strategies are identified as threats to Ukraine's cybersecurity:

— hybrid aggression of the Russian Federation (RF) against Ukraine in cyberspace. The aggressor state is constantly increasing the arsenal of offensive cyber weapons, the use of which can cause irreparable, irreversible destructive consequences. Cyber-attacks of the Russian Federation are aimed primarily at information and communication systems of state bodies of Ukraine and objects of critical information infrastructure in order to disable them (cyber diversion), gain covert access and control, intelligence and intelligence activities. Cyberattacks are also actively used by the aggressor state as an element of special information operations aimed at manipulating the population, interfering in electoral processes and discrediting Ukrainian statehood; cybercrime, which harms information resources, social processes, personally citizens, reduces public confidence in information technology and leads to significant material losses. The use of cyberspace to commit crimes against the national security of Ukraine, as well as criminal offenses related to money laundering, trafficking in human beings, illicit handling of weapons, ammunition or explosives, illicit trafficking in narcotic drugs and psychotropic substances is becoming widespread. , their analogues or precursors and other objects and substances that threaten human life and health, etc .;

— organized and sponsored by governments of other states cyberattacks related to the theft for political, economic or military purposes of sensitive information (cyber espionage) and the implementation of intelligence and subversive activities. Features of such cyberattacks are their duration, complexity and hidden nature, which complicates their prevention, detection and neutralization;

— use of cyberspace by terrorist organizations to commit acts of cyberterrorism, financial and other support for terrorist activities.

The defense component of cybersecurity is described, in particular, in the Strategy of Military Security of Ukraine, adopted by the National Security and Defense Council on March 25, 2021 and approved by the Decree of the President of Ukraine of March 25, 2021 № 121/2021. As stated in this Strategy, "at the national level, the Russian Federation remains a military adversary of Ukraine, carrying out armed aggression against Ukraine, temporarily occupying the territory of Ukraine, systematically using military, political, economic, informational, psychological, space, cyber and other means. that threaten the independence, state sovereignty and territorial integrity of Ukraine. "

As noted by I.R. Maltseva (with co-authors), cybersecurity— one of the most important components of the entire defense system in the armed forces of Ukraine (Maltseva et al., 2020). A. Khudoliy (2019) emphasizes that in recent years cyber security has become a priority for the modern army. Active hybrid warfare, which accompanies the physical phase of hostilities, is forcing the Ukrainian military to intensify efforts in this direction (Khudolii, 2019). The aggressor actively uses cyberspace not only against Ukraine, but also against other states. The article mentions cyberattacks as a threat to the country's defense. The latter is especially clearly confirmed after the beginning of the large-scale armed invasion of the Russian Federation into Ukraine on February 24, 2022. Thus, according to the American company Microsoft, since the beginning of the war, Russian hackers have committed almost 240 cyber-attacks against Ukraine— businesses and government agencies. Attacks were often aimed at destroying computer systems, but some were also aimed at gathering intelligence or spreading misinformation.

Another component of cybersecurity threat in Ukraine is cybercrime. It was noted above that Ukraine has ratified the Council of Europe Convention on Cybercrime of 23 November 2001. The Convention states that the fight against cybercrime is dictated, in particular, by the need to protect legitimate interests in the use and development of information technology. In particular, the Convention identifies the following types of cybercrime:

— offenses against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, device abuse).

The criminalization of these illegal actions ensures the rights of individuals to collect, store, use and disseminate information, access to reliable and objective information;

— computer-related offenses (computer-related counterfeiting; computer-related fraud).

The criminalization of these illegal actions ensures the rights of individuals to preserve the inviolability of those rights that are recorded in computer systems, such as the inviolability of credentials on property rights, or credentials on individuals' money accounts or securities accounts, and so on. For example, according to Russian data, on April 12, 2022 it became known that in 2021 fraudsters stole 13.5 billion rubles from bank customers, making more than 1 million unauthorized transfers from bank cards and accounts. From these funds, banks were able to return to the affected citizens of only 6.8%, or 920 million rubles (Russian hackers have launched…, 2022; Losses of banks from cybercrime, 2022). The level of refunds is falling for the second year in a row amid rising thefts. At the same time, it is reported that in Ukraine there are quite high rates of cybercrime detection in the banking sector— up to 80% of stolen funds are returned to the owners;

— Offenses related to child pornography (development of child pornography for distribution through computer systems; offering or providing access to child pornography through computer systems; distribution or transmission of child pornography through computer systems; obtaining child pornography using computer systems for oneself or another person; possession of child pornography in a computer system or on a computer medium).

At the same time, the Convention on Cybercrime explicitly states that the criminalization of these actions is aimed at protecting the rights of children in accordance with the UN Convention of 20.11.1989 (New York). Under Article 34 of this Convention, States Parties have an obligation to protect the child from all forms of sexual exploitation and sexual abuse. To this end, States Parties shall, in particular, take all appropriate measures at the national, bilateral and multilateral levels to prevent: (a) The incitement or coercion of a child to engage in any unlawful sexual activity; (b) The use of children for the purpose of exploitation in prostitution or other unlawful sexual practices; (c) The use of children for the purpose of exploitation in pornography and pornographic materials;— offenses related to copyright and related rights infringement.

This requirement is aimed at protecting the intellectual property rights of the copyright and related rights in accordance with the Paris Act of 24.07.1971 on the Berne Convention for the Protection of Literary and Artistic Works, the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), The Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Agreement.

Internet piracy is the illegal distribution of intellectual property on the Internet. The essence of Internet piracy is the reproduction and distribution on the Internet of films, musical works, computer programs, other intellectual property, without the permission of the author or another person who has copyright and / or related rights, or without payment of remuneration for use of works in the manner prescribed by law. In the legislation of Ukraine, the definition of Internet piracy is given in Article 50 "Infringement of copyright and related rights" of the Law of Ukraine "On Copyright and Related Rights": Internet piracy is the commission of any actions recognized as copyright infringement and (or) related rights using the Internet (paragraph b of Article 50). Internet piracy is global, it cannot be defeated in a single country. But the world community and each country are trying to develop an effective mechanism for simplified and accelerated copyright protection on the Internet. The following international acts are aimed at this: the EU Directive "On e-Commerce" № 2000/31 / EU of 08.06.2000; EU Directive "On Copyright in the Digital Single Market" № 2019/790 / EU of 17.04.2019.

In terms of international cooperation, we should agree with the opinion of Yu.S. Razmetaeva, who believes that the prevention of cyber threats is possible through a combination of national and international cyber defense strategies (Razmietaieva, 2015). Therefore, the combination of national and international cybersecurity strategies, dynamism is the way that leads to cyber security, including the prevention of conflicts in the information sphere. One can fully agree with the thesis that both hardware protection and software protection are the main tasks of cybersecurity. However, both types of protection must be implemented and integrated into national and international strategy (regulation) in order to achieve their goals" (Maskun, 2013).

CONCLUSIONS

Legal regulation of cybersecurity in Ukraine is based on the requirements of striking a balance between information protection and freedom of expression, the position of the United Nations and the case law of the European Court of Human Rights. The balance is based on a reasonable combination of restrictions on access to information or its distortion, distortion in the process of "information warfare" and ensuring constitutional rights and freedoms to collect, store, use and disseminate information, access to reliable and objective information, personal data protection, public morality and counteraction to infringements of intellectual property.

REFERENCES

Cherevatiuk, V.B., Bielkin, L.M., Sopilko, I.M., & Yurynets, Yu.L. (2022). The question of the balance between information protection and ensuring the rights of individuals in the regulation of cyber security under the legislation of Ukraine. Modern Aspects of Science: XX. Part of the international collective monograph / International Economic Institute. Czech Republic: International Economic Institute, 601-609. Retrieved from: http://perspectives.pp.ua/public/site/mono/monography-20.pdf

Cyber security and/or human rights. (2018, June 6). ALL-UKRAINIAN ASSOCIATION INFORMATION SECURITY AND INFORMATION TECHNOLOGIES. Retrieved from: https://cutt.ly/21cp8VP

Dziundziuk, V.B., & Kotukh, Ye.V (2020).Cyber security as one of the priorities of national policy. State Construction, 2.

Foros H.V.,& Zhohov V.S. (2019). Peculiarities of the interpretation of the concept of «cyber security» in modern legal science. *Constitutional State, 33*, 128-134.

Khobbi, Yu. (2020). The human right to cyber security: problems of definition and guarantee. *Legal Bulletin*, 2, 37-43

Khudolii, A. (2019). Cyber security: modern challenges for Ukraine. *Acta de history & politics: saeculum XXI,* 1, 138-146.

Losses of banks from cybercrime (2022). TADVISER. Retrieved from: https://www.tadviser.ru/index.php/Statia:Potery_bankov_ot_kyberprestupnosty

Maltseva, I.R., Chernysh, Yu.O., & Cherednychenko, O.Iu. (2020). Cyber security is one of the most important components of the entire defense system in the Armed Forces of Ukraine. *Cyber Security: Education, Science, Technology,* 1. 85-92.

Maskun, S.H. (2013). Cyber Security: Rule of Use Internet Safely. *Journal of Law, Policy and Globalization*, 15, 22.

Razmietaieva, Yu.S. (2015). The international security system in the light of cyber threats: legal problems and prospects. *Actual Problems Of Modern International Law:, Kharkiv*. 1, 175-177.

Russian hackers have launched almost 240 cyberattacks against Ukraine since the beginning of the war— Microsoft. (2022). Retrieved from: https://www.slovoidilo.ua/2022/04/28/novyna/bezpeka/rosijski-xakery-pochatku-vijny-skoyily-majzhe-240-kiberatak-proty-ukrayiny-microsoft.

Sopilko, I.M. (2021). Information security and cyber security: a comparative legal aspect. *Scientific Works Of NAU. Series: Legal Bulletin Air And Space Law, 2*(59), 110-115.

Sopilko, I.M. (2021). Peculiarities of combating cyberthreats with legal methods and means. *Scientific Works Of NAU. Series: Legal Bulletin Air And Space Law, 4*(61), 105-110.

Yushchuk, O. (2009). Information security of Internet users. *Scientific notes of the National University «Ostroh Academy». Series: Culture and social communications,* 1, 224-231