LEGAL REGULATION OF CYBERSECURITY AND PRIVACY ON THE INTERNET

Volodymyr Polishchuk¹
Vitalii Yurakh²
Olena Kravchenko³
Wolodymyr Warawa⁴
Inna Kulchii⁵

ABSTRACT

Objective: This article examines the conceptual framework for forming and developing legal regulation of cybersecurity and privacy on the Internet.

Theoretical Framework: The article aims to highlight the evolution and future prospects of legal regulation concerning cybersecurity and privacy in both Ukraine and globally.

Method: The methodological principles include impartiality and unbiasedness and a comprehensive study of the legislative framework and its specifics in the context of cybersecurity and privacy.

Results and Discussion: The legislative experiences of international law on cybersecurity and privacy have been summarized. In Ukraine, the legal support process for cybersecurity and privacy continues, with the country ratifying several international documents and developing its own legislative framework.

Research Implications: The term "cybersecurity" has been legislatively defined, encompassing 10 fundamental principles regarding the Internet's development and impact on human life.

Originality/Value: The terms "cybersecurity," "cybercrime," and "privacy in the virtual space" require further refinement. A methodology that facilitates the interaction and coexistence of legal norms and netiquette is needed.

Keywords: Cyber threats, Cybersecurity, Cyberbullying, Netiquette, Privacy, Virtual space, Legal regulation.

REGULAÇÃO LEGAL DE CIBERSEGURANÇA E PRIVACIDADE NA INTERNET

RESUMO

Objetivo: Este artigo examina o quadro conceitual para a formação e desenvolvimento da regulamentação legal da cibersegurança e privacidade na Internet.

Referencial Teórico: O artigo visa destacar a evolução e as perspectivas futuras da regulamentação legal relacionada à cibersegurança e privacidade tanto na Ucrânia quanto globalmente.

Método: Os princípios metodológicos incluem imparcialidade e ausência de preconceitos, além de um estudo abrangente do quadro legislativo e suas especificidades no contexto da cibersegurança e privacidade.

¹ Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: Polishchuk_Volodymyr.20@proton.me Orcid: https://orcid.org/0009-0002-2642-9326
² Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine. E-mail: yuraxandko@gmail.com Orcid: https://orcid.org/0000-0003-1705-389X
³ The National Academy of Security Service of Ukraine, Kyiv, Ukraine. E-mail: elenakrav4enko81@ukr.net Orcid: https://orcid.org/0000-0003-0246-1022
⁴ Dniproptrovsk University of Internal Affairs, Dnipro, Ukraine. E-mail: warawa@ukr.net Orcid: https://orcid.org/0000-0001-7856-1711
⁵ National University, Yuri Kondratyuk Poltava Polytechnic, Poltava, Ukraine. E-mail: nafusial@gmail.com Orcid: https://orcid.org/0000-0002-0063-6493
Resultados e Discussão: As experiências legislativas do direito internacional sobre cibersegurança e privacidade foram resumidas. Na Ucrânia, o processo de suporte legal para cibersegurança e privacidade continua, com o país ratificando vários documentos internacionais e desenvolvendo sua própria estrutura legislativa.

Implicações da Pesquisa: O termo "cibersegurança" foi definido legislativamente, abrangendo 10 princípios fundamentais sobre o desenvolvimento da Internet e seu impacto na vida humana.

Originalidade/Valor: Os termos "cibersegurança," "cibercrime," e "privacidade no espaço virtual" precisam de mais refinamento. Além disso, é necessária uma metodologia que facilite a interação e coexistência das normas legais e da netiqueta.


REGULACIÓN LEGAL DE LA CIBERSEGURIDAD Y LA PRIVACIDAD EN INTERNET

RESUMEN

Objetivo: Este artículo examina el marco conceptual para la formación y desarrollo de la regulación legal de la ciberseguridad y la privacidad en Internet.

Marco Teórico: El artículo tiene como objetivo resaltar la evolución y las perspectivas futuras de la regulación legal sobre ciberseguridad y privacidad tanto en Ucrania como a nivel global.

Método: Los principios metodológicos incluyen imparcialidad y objetividad, además de un estudio exhaustivo del marco legislativo y sus especificidades en el contexto de la ciberseguridad y la privacidad.

Resultados y Discusión: Se han resumido las experiencias legislativas del derecho internacional sobre ciberseguridad y privacidad. En Ucrania, el proceso de apoyo legal para la ciberseguridad y la privacidad continúa, con el país ratificando varios documentos internacionales y desarrollando su propio marco legislativo.

Implicaciones de la investigación: El término "ciberseguridad" ha sido definido legislativamente, abarcando 10 principios fundamentales sobre el desarrollo de Internet y su impacto en la vida humana.

Originalidad/Valor: Los términos "ciberseguridad," "cibercrime," y "privacidad en el espacio virtual" requieren mayor refinamiento. Además, se necesita una metodología que facilite la interacción y coexistencia de las normas legales y la netiqueta.

Palabras clave: cónyuges, matrimonio, derechos personales no patrimoniales, ECHR, formas de proteger los derechos familiares.

1 INTRODUCTION

Besides its apparent advantages, the modern digital world also carries many threats. The data revolution (Schmidt & Cohen, 2015, pp. 40-54), i.e., the incredible accumulation and generation of information, reveals unprecedented possibilities for humanity. The extent and vectors of these possibilities are yet to be fully understood. However, at the same time, the data revolution deprives individuals of control over their personal information on the internet. On a
personal level, cyber-attacks and security breaches can have various unpleasant and dangerous consequences, such as the theft of personal data for financial and property manipulations or the extortion of family photos.

Cybersecurity is also crucial to ensuring the proper functioning of critical infrastructure (power plants, hospitals, banks, etc.) and the government administrative apparatus. Today, the military-industrial complex is only possible with the technical support and maintenance of cyber protection infrastructure. With the increasing role of ideas and concepts in the modern world, protecting intellectual property in cyberspace has become of particular importance.

The IT industry and the information space are snowballing, and neither ordinary citizens, business corporations, nor the legal system can keep up with the rapid response to the challenges and threats arising from this. Cybercriminals, armed with technical equipment and skills and exploiting the imperfections of legal regulation in the virtual world, actively contribute to the problem.

Efforts to restrain societal surveillance through new laws will likely increase. Consumers will pay more for services that guarantee confidentiality, and the market for privacy protection technologies will grow. In April 1999, The Economist published an article titled "The End of Privacy," discussing the impossibility of restraining the wave of electronic intrusion into confidentiality and privacy, which became one of the biggest social changes of modern times.

Considering that digital information can likely be stored indefinitely, careful legislative approaches and guarantees for solving privacy and virtual security issues should be thoroughly considered. Of course, this will not provide a 100% guarantee the practical implementation of such rights and freedoms. However, this will at least create the necessary legislative basis for some civilized control over the virtual space and its use (Schmidt & Cohen, 2015, p. 66). In addition to the legal regulation of cybersecurity and privacy on the Internet, essential conditions for developing a stable society include monetary and fiscal policy components. Among them, free competition guaranteed by law, loyal trade, and capital flows deserve special attention. Political stability and progressive development are also critical factors (Nikonenko et al., 2022, p. 504). Also, for comprehensive coverage of the research topic (a global issue), constant monitoring and comparative analysis of the obtained data are necessary. This applies primarily to countries with developed economic systems (Zayed et al., 2022, p. 9).

Cybersecurity and privacy protection in the virtual space as service sector components are relevant components of the modern economy. This is especially true for countries like the United States, Germany, and China (Kovalko et al., 2022). Speaking of business development,
cybersecurity, its legal aspects, and practical implementation are necessary conditions for its functioning. Enterprise management also involves monitoring and diagnosing the cybersecurity system (Lelyk et al., 2022, p. 306). In particular, cyberattacks are the greatest danger for business companies. Their leaders consider cyberattacks more dangerous than brand reputation loss, legal regulation, and economic uncertainty (Dovgan, 2019, p. 15).

World countries are building up their cyber power and strengthening their cyber borders. For Ukraine, this has become particularly relevant after the full-scale invasion by Russia on February 24, 2022. Much attention, especially in the field of public administration, is given to cyber hygiene (Voytovych et al., 2024). Additionally, decentralization is crucial in our country's context. This reform has "freed the hands" of communities to address the priority and relevance of issues requiring solutions independently. Importantly, budget adoption and allocation remain local (Borodina et al., 2022, p. 12). In other words, financial freedom should contribute to effectively implementing cybersecurity and privacy protection at the local level.

Even though the legal system, especially in the international format, is incredibly bureaucratic and inflexible, legal regulation of cybersecurity and the circulation of personal data in cyberspace is a dynamic legislative activity that requires constant monitoring and the search for effective strategies to counter virtual threats to the safety of citizens and states.

2 THEORETICAL FRAMEWORK

Forming legal foundations for cybersecurity and privacy in the virtual space is integral to the legislative process. This also includes its practical implementation and incorporation into the legislation of different countries, international agreements, treaties, etc. Therefore, when studying this topic, attention must be paid to scientific works that generally discuss the legal mechanisms of states and intergovernmental associations. In particular, in his monograph, Bratsuk I. characterized the theoretical and legal interaction of European Union (EU) law and the national law of member states. The author also examined the mechanisms of legal acts and constitutional-legal features of implementing EU law into the national law of member states (Bratsuk, 2016).

The monograph by Shemchuk V. "Ensuring Information Security as a Function of Modern States: Comparative Legal Analysis," is dedicated to the study of theoretical and practical problems of information security as one of the fundamental functions of states in the modern world (Shemchuk, 2020). Kovacs L. focused on analyzing the cybersecurity strategies of EU and NATO countries (Kovacs, 2018). Klymenko N. considered interpretations of security
in the works of lawyers, sociologists, and philosophers from antiquity to the present (Klymenko, 2019). The state of cybersecurity, main trends in virtual technology, resistance to external cyber aggression, and technical aspects of cybersecurity are discussed in the study "Cybersecurity in the Information Society" (Dovgan, 2019).

The monograph by Pazyuk A. "International Information Law: Theory and Practice," introduces readers to various issues related to the development of international information law. In particular, special research attention is focused on the impact of the Internet on forming legislative initiatives. The latter is related to the emergence of cyberspace and its comprehensive penetration into all spheres of life of citizens, society, and states (Pazyuk, 2015). Voytsikhovkyy A. examined conceptual approaches to cybersecurity in the European legal field, legal and organizational foundations of the EU, and their further perspectives (Voytsikhovkyy, 2018).

Given Ukraine's European integration aspirations and the practical steps taken to realize these aspirations, the study of the EU legal framework and the specifics of its implementation in national legislation will remain relevant in the near future. This includes studies in cybersecurity and scientific and analytical works on the legal aspects of international relations.

In the early 2000s, Pazyuk A. examined the issue of privacy on the Internet through the lens of legal specifics. In particular, the author noted that despite rapid digitization, issues related to cybersecurity would still be addressed (Pazyuk, 2000). Bulavina S. and Davydova T. are engaged in studying the consequences of privacy rights violations. They analyze international practices to bring better experiences into the legal field of Ukraine (Bulavina & Davydova, 2020). As the greatest danger to any organization, cybersecurity and cyberattacks are the focus of Bakalinska O.'s publication (Bakalinska, 2020). Additionally, Bakalinska O. has focused her research on theoretical and practical steps to improve cybersecurity legislation in Ukraine. The author considers modern trends in EU and NATO countries, as well as the impact of full-scale war on the cyber environment in Ukraine and the need for legal regulation at the international level in the Ukrainian context (Bakalinska, 2022).

Currently, the topic of legal regulation of cybersecurity and privacy on the Internet is dynamically evolving. It is the subject of scientific and applied interest for lawyers, media experts, economists, sociologists, public servants, and psychologists.
3 METHODOLOGY

The article is based on general and special methods of studying legal phenomena and processes. Such a systematic approach allowed us to study the issue of legal regulation of cybersecurity and privacy on the Internet in a historical and chronological context. The general formal and logical methods of analysis and synthesis focused the research attention on the main problems of our study of the specifics of legal regulation of virtual space. The methods of induction and deduction were applied to analyze the legislative framework in the field of cybersecurity. This allowed us to systematize and structure the information following the article's logic. The method of analogy helped to trace the specifics of legal regulation of cybersecurity and online privacy in the laws of various countries, including Ukraine. The sociological method helped study the opinions and proposals of lawyers regarding practical legal support for cybersecurity and privacy in the virtual space.

The comparative legal method was used to analyze foreign experience in forming and developing the legislative framework for cyberspace regulation. As a result, we concluded that it is necessary to study the most effective practices of legal regulation of cybersecurity and privacy on the Internet in the Ukrainian legal field and implement them in national legislation. The methods of generalization and forecasting were employed when drawing conclusions and proposals on the legal framework for cybersecurity and privacy in the virtual space in Ukraine. The method of processing and selecting the necessary information (analysis of documents, official communications, and interviews with lawyers) allowed us to systematize the existing legal framework in the field of cybersecurity and privacy in the virtual space.

4 RESULTS AND DISCUSSIONS

Considering the growing role of cybersecurity in people's lives and on an international scale, as well as the increasing challenges in protecting privacy in the virtual world, the evident advantages of virtualization in all aspects of our daily lives have a flip side. Threats to national security due to cybercrime, both at the country level and globally, will continue to rise. In the context of a full-scale war in Ukraine, the factor of life virtualization has acquired specific characteristics. The war extends across all spaces, including the virtual realm. Therefore, state-of-the-art cybersecurity is a legislative priority for our country's national security.

The contemporary development of human civilization depends to a large extent on the progress of the virtual environment. For instance, the term "digitization" became one of the
most popular in Ukraine's online environment in 2019 (Bulavina & Davydova, 2020, p. 8). The word "digitization" is one of the outcomes of the global digital revolution. It is a neologism denoting changes in societal life caused by the emergence, dissemination, and widespread use of digital technologies.

As of today, the virtual world largely replicates interactions in the physical realm. This also applies to legal relationships in digital format. In particular, a system of legal relationships has formed between consumers and internet service providers, electronic payments, communication, the provision of administrative services through digital applications, electronic management, and law enforcement functions. The laws of countries and international agreements somewhat regulate all of this. At the same time, there is netiquette (the concept emerged in the 1980s - from the English "net" and the French "etiquette") - the culture of virtual communication, which involves adhering to several basic categories:

- Emotional contact (smileys, emojis, forms of addressing "you" or "you're," ignoring aggressive incidents, established forms of greeting and farewell in official correspondence, etc.);
- Technical features of virtual communication (rules of quoting, form, size, and font color, specifics of text formatting, design of presentations, etc.);
- Administrative (permissibility or inappropriateness of flame (emotional assertion of one's position), advertising or its prohibition, the group's theme, etc.).

Violations of netiquette include personal attacks, verbal and visual insults, deviating from the topic of conversation, excessive self-promotion, plagiarism, immoral statements, etc.

When forming and improving the legal culture related to the digitalization of society, Ukraine should pay attention to the relevant achievements in the EU countries. Given the ongoing war, the country should consider our internal situation and needs.

In ancient times and up to the XVI century, understanding security was associated with physical protection from various threats. The state was assigned the role of guarantor of such protection. In those specific historical conditions, cooperation and community were crucial for survival. Solitude usually equated to death and sharply reduced the chances of physical survival. Christian philosophers considered security to be linked to God's protection, grace, or the wrath of heavenly forces.

The Renaissance centuries fostered an awareness of security as the benevolence of a wise ruler (monarch). For the XVII and XVIII centuries, a strong state was to act as the guarantor of the natural right of individuals to be secure. In the XIX century, fundamentally
different understandings of security rights emerged. Now, the state itself could threaten citizens, just as they could to the state. Legal aspects of distributing branches of power, protecting the state's territory, and international agreements became increasingly important.

In the XX century, despite two World Wars, a series of revolutions, repression, genocides, and ideologies of hatred, the concept of "security" added an awareness of it in relation to persons, society, and the state. The well-established institution of the state was obliged to protect all rights and freedoms of citizens. This was meant to guarantee free and stable progressive development, progress, and prosperity. The concepts of sovereignty and territorial integrity became relevant. In our present day, humanitarian components have been added to existing interpretations and understandings of security. Religion, language, tradition, and identity are all part of human civilization's modern conception of security. It is primarily about internal (national) security. However, in the conditions of deepening globalization and the increasing role of the virtual world in all international processes, significant attention is beginning to focus on global security (Klymenko, 2019, pp. 6-7).

In countries of the Western cultural circle, there is a widespread belief that the successful, fair, and effective enforcement of judicial decisions, both regarding people in economic operations and regarding state bodies or officials, is crucial for developing legal culture norms and the independence of judges. At the same time, we observe an increase in the volume of various documents and materials of international jurisprudence. This, among other things, requires thoughtful approaches to making maximally objective judicial decisions (Lytvyn, Andrushchenko, Zozulya, Nikanorova & Rusal, 2022, p. 95).

Education is essential to ensure sustainable development, which includes, among other things, cybersecurity and privacy in the digital age. At the same time, education aims to increase humanity's intellectual level. People need to learn to recognize dangerous behavior and be able to correct it or prevent such manifestations. Effective changes must occur at both the individual and societal levels. Realizing one's potential will contribute to societal well-being and the disclosure of better prospects (Mia et al., 2022, p. 3).

Cybersecurity and privacy in the virtual space are crucial economic, political, and military security issues. However, they are currently the most vulnerable regarding protection (including legal), understanding threats and perspectives, vectors of development, and opportunities for influence in various spheres of society's activities. It should be noted that states already have policies in both the physical and digital worlds. Sometimes, they will even contradict each other in the future, no matter how paradoxical it may sound (Schmidt & Cohen, 2015, p. 263). A cybersecurity strategy is a tool for achieving national security goals. Along
with technological development, technical support, and training of qualified personnel, legal regulation is part of this strategy (Kovacs, 2018).

Cyberspace has its specificity, determined by the instant dissemination of information, its accessibility, and the absence of borders (or by its almost absence, depending on the policies of existing states today) (Pazyuk, 2015, p. 229). It significantly complicates its regulation and response to challenges and dangers. The first step in ensuring the security of critical infrastructure is considered to be the establishment in 1996 of the Commission on Critical Infrastructure Protection by the President of the United States. It aimed to develop a national strategy for protecting critical infrastructure from physical and cyber threats (Zvezdova & Vakalyuk, 2021-2022, p. 85). In most countries around the world, it includes:

− Transportation network and energy;
− Logistics;
− Media, communication;
− Interbank settlements;
− Objects of functioning of state authorities;
− Enterprises of national importance;
− Emergency services;
− The life support system of megacities (Biryukov & Kondratov, 2012, p. 3, 5).

As accurately noted by Bakalinska O., cyberspace has become a mighty tunnel for information's emergence, dissemination, and transformation. At the same time, it takes over the functions of the "heart" of the economy and its "engine." It is also a platform for new social links, communications, and communities. We can already talk about the emergence of a new type of state - a virtual one (Bakalinska, 2020).

The "Declaration on Internet Governance Principles" formulates 10 key principles:

1. The rule of law supremacy and democracy development;
2. Multilateral management;
3. Responsibilities of states;
4. Assistance to consumers of digital content;
5. The universality of the Internet;
6. Integrity of the Internet (this principle includes security, stability, reliability, and resilience of the Internet, as well as its ability to evolve, should be key objectives of Internet governance);
7. Decentralized management (the bodies responsible for the technical and managerial aspects of the Internet and the private sector) should retain their leading role in technical and operational matters while ensuring transparency. Also, they should be accountable to the global community for actions affecting public policy;
8. Architectural principles (barrier-free Internet usage);
9. Open network;
10. Cultural and linguistic diversity, promotion of the development of local content (Declaration by the Committee of Ministers on Internet governance principles, 2011).

The EU has or has had several organizations that aim to develop a culture of cybersecurity, including through legal norms and guarantees. They include a series of documents that deal with the following:
- network and information security;
- combating cybercrime;
- regulatory methods, tools, and means (Voytsikhovkyy, 2018, p. 27-28).

The Council of Europe's Strategy for Internet Governance continued legislating the virtual space's activities and development. In particular, it highlights points that focus on cybersecurity and the protection of the privacy of Internet users. These issues are a shared responsibility, consolidation, and concentration of efforts to combat extremism, radicalization, cybercrime, exploitation, harassment, and intimidation of people using virtual technologies. Particular attention is paid to protection against sexual violence, online child exploitation, combating trafficking of organs and human beings, and the sale of counterfeit medicines and drugs. The Council of Europe will focus on promoting countries' accession to a range of international legislative initiatives in this area to ensure the effective implementation of these priorities. Further steps also include establishing a common policy and principles of Internet governance, especially in information and network security. The problems of data interception, protection of personal data, and human rights in the virtual space are still relevant.

On December 16, 2020, the UN General Assembly adopted the "The Right to Privacy in the Digital Age" resolution. This document summarized previous developments in international law in the field of cybersecurity and privacy in the virtual world. The resolution also focuses on artificial intelligence (Danylenko, 2022). As noted above, humanity has yet to realize and experience in practice the benefits and dangers of the virtual world.

However, it has already been noted that artificial intelligence's impact on protecting human rights and transforming public administration and social relations may have far-
reaching, unpredictable consequences, not least related to privacy. This stems primarily from the lack of appropriate safeguards when rapidly learning artificial intelligence can influence decision-making that will affect economic, social, and cultural human rights. It will also affect the principle of non-discrimination. 

The particular danger of such unpredictable results involves:

− The processing of personal and biometric data;
− Unlawful or unconscious data collection, interception, and unauthorized access to personal data;
− The illegal use of biometric technologies.

All these threats and challenges can lead to violations of the right to privacy, freedom of expression, freedom of opinion and belief, freedom of peaceful assembly and association, and the right to religious liberty. Moreover, they contradict society's fundamental democratic principles.

The resolution emphasizes that all people's rights in their daily lives, including the right to privacy, should also apply to virtual space. Another concern is the spread of disinformation and false information, especially on social media. Such disinformation aims to spread racism, xenophobia, negative stereotypes, and stigmatization. It also contains calls for violence, discrimination, hatred, and hostility in all its manifestations. States and commercial entities are responsible for complying with international and national law. They are called upon to respect accepted norms and interpretations of privacy, human health, data protection, etc. The resolution confirms numerous rules and laws on privacy and data protection that have already been developed. This is especially true for the protection of children's rights. It is necessary to harmonize international and national legislative frameworks and regularly monitor and improve practices, procedures, and legislation to ensure the right to privacy in the virtual world. This will require the use of existing and developed resources and mechanisms and the creation of new, impartial, unbiased, and effective courts, parliamentary oversight, and transparent reporting on collecting, disseminating, and storing personal data.

The text of the resolution states the need for further development of effective legislation, both at the international and national levels, related to privacy in the virtual space. Given the rapid development of virtual technologies, artificial intelligence, and their impact on the lives of individuals, societies, and states, the resolution states the need for further development of the legal framework related to cybersecurity and privacy protection in virtual space (The right to privacy in the digital age: Resolution/adopted by the General Assembly, 2020, p. 8-11).
In 2021, the European Commission published the Digital Compass, which sets out the goals and targets for Europe's development until 2020 in digital technologies and forming a sustainable closed-loop economy. In addition, the Digital Compass considers climate change, focusing on human well-being and prosperity in the context of developing a digital culture on a global scale (Bakalinska, 2022, p. 83).

We currently have several relevant legislative decisions concerning the legal regulation of cybersecurity and privacy in the virtual space in Ukraine. On September 7, 2005, Ukraine ratified the 2001 Council of Europe Convention on Cybercrime. In particular, this document defines the measures that fall within the competence of national legislation:

- Unauthorized interference with a computer system;
- Illegal interception of information by technical means;
- Interference with data.

The Convention also defines corporate liability, complicity, sanctions, and measures related to non-compliance with its provisions (Convention on Cybercrime, 2005).

The fundamental basis of Ukraine's cybersecurity is the Constitution of Ukraine and various laws and regulations. On December 28, 2021, the Information Security Strategy (Strategy) was implemented in Ukraine. According to this document, the tasks set out in the Strategy should be implemented by 2025. Their practical solution requires:

- Consolidation of legal developments, technical and technological developments, personnel decisions, and systemic media literacy at all levels of education;
- Stable and systematic interaction with foreign partners, considering the international community's theoretical and practical experience.

This goal's practical realization requires improving the relevant legislation and monitoring the Strategy's objectives.

The formation and development of the legal framework related to cybersecurity and privacy in the virtual space in Ukraine stems from the European integration of our country and the realities of the Russian-Ukrainian war. It is essential to realize that legislative solutions alone are insufficient for the effective legal regulation of cyberspace. In the context of the increasing atomization of society, the consciousness of citizens and their level of media literacy play an essential role in shaping the understanding of cyber threats and countering them.
5 CONCLUSION

Legal regulation of cybersecurity and privacy in the virtual space is a dynamic and multidirectional process. The legislative process in this area requires further development of definitions of "cybersecurity," "cybercrime," "privacy in the virtual space," and the methodology of legal regulation of the virtual world. In addition, it is necessary to keep in mind the unprecedented development of virtual technologies, artificial intelligence, digital culture, the growing level of cybercrime, and the impact of the virtual world on all spheres of human, social, and state life without exception. The legislative process should consider existing international and national legislation and current challenges and forecast the prospects for positive and negative effects of virtual influence on real life.

Legal support for cybersecurity and privacy in the virtual space is an essential factor in developing the Internet economy. This sector of economic growth (primarily virtual commerce) has revived during the quarantine and in Ukraine - due to the full-scale invasion of Russia. Therefore, this area of legislative activity is up-and-coming in terms of relevance and speed of response to the challenges of the times.

The phenomenon of cyberbullying (cyberviolence) as one of the consequences of non-compliance with the right to privacy requires further study, analysis, and development of the legislative framework. Currently, in addition to lawyers, psychologists, sociologists, doctors, and educators are also studying cyberbullying. In other words, this is an interdisciplinary problem that requires constant monitoring and interaction between specialists from different fields.

Today, the virtual world reproduces relationships in physical life. The same applies to legal relations in digital format. In particular, a system of legal relations between consumers and providers of Internet services, electronic payments, communication, provision of administrative services through digital applications, e-governance, and law enforcement functions has been formed. These areas are regulated in one way or another by national laws and international treaties.

At the same time, there is netiquette (a concept that originated in the 1980s - English "net" and French "etiquette") - a culture of virtual communication that involves observance of several main categories:

- Emotional contact (emoticons, emojis, forms of addressing "you" or "you're," ignoring aggressive attacks, established forms of greeting and farewell in official correspondence, etc.);
- Technical features of virtual communication (citation rules, font shape, size and color, specifics of text formatting, presentation design, etc.);
- Administrative (admissibility or inappropriateness of flaming (emotional proof of one's position), advertising or its prohibition, group topics, etc.).

Violations of netiquette include:
- Personalization;
- verbal and visual abuse;
- deviation from the topic of communication;
- excessive self-promotion;
- plagiarism;
- immoral statements, etc.

Thus, we can firmly state that new technological realities, international relations, and geopolitical situations have become serious challenges for the system of legal relations in the modern world. International legal norms and national legislation play a catch-up role in virtual space's cybersecurity and privacy systems. The regulatory framework for the virtual sphere, both in Ukraine and globally, needs to catch up with the development of technology. This further exacerbates the threat of cybercrime. However, legal regulation itself is not enough to solve these problems. Other important factors in cybersecurity and privacy in the virtual world are cyber hygiene, media literacy, and cyber detox. All of these should become part of our lives from childhood.

REFERENCES


Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on September 21, 2011, at the 1121st meeting of the Ministers' Deputies) (2011). *Council of Europe. Committee of Ministers*. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6


