УДК 342.9:004.7

Natalia DIDYK
Lviv Polytechnic National University,
Associate Professor, Department of administrative and information law,
Institute of law, psychology and innovative education
candidate of legal sciences, Associate Professor,
e-mail: nataliia.i.didyk@lpnu.ua,
ORCID ID: https://orcid.org/0000-0002-6347-5092

Yaryna PAVLOVYCH-SENETA
Lviv State University of Internal Affairs,
Institute of Law
Associate Professor of the Department of administrative and legal disciplines,
candidate of legal sciences, associate professor,
e-mail: pyarp@ukr.net,
ORCID ID: https://orcid.org /0000-0002-3491-8878

ONLINE RISKS IN MODERN CONDITIONS: PROBLEMS AND WAYS TO OVERCOME

http://doi.org/10.23939/law2024.41.085

It was emphasized that ensuring the safety of children is one of the priority tasks of the state. Today, in the conditions of rapid digital development, new challenges and threats to the well-being of children appear, which require the search for effective tools to overcome them and provide a comprehensive approach to ensuring the safety of children in cyberspace.

Attention is focused on the fact that a comprehensive approach includes, among other things, the appropriate level of training of specialists of entities whose competence includes prevention and response to threats to the safety of children in cyberspace. Timely detection of threats to the safety of children in cyberspace depends on their professionalism, care, and impartiality.

It has been proven that information security is more relevant than ever. Growing cyber attacks on public and private enterprises only increase this trend. A separate category of threats concerns citizens, who are increasingly becoming the object of close attention of criminals, therefore, a relatively new concept of the need for users to independently observe basic safety rules is gradually spreading. This approach makes it possible to significantly strengthen the system of collective security of society and the state as a whole.

It is noted that cyber hygiene should be treated in the same way as personal hygiene, and when properly integrated into the organization, become a simple daily procedure that will ensure the state of cyber health of the organization in an optimal state.

It became clear that violation of the rules of cyber hygiene can lead to harmful consequences not only for an individual person. Quite often, the victim's employer also suffers from the actions of criminals. Even great powers can suffer enormous damage from a careless attitude towards the security requirements of one person. Violators often use an individual to

penetrate critical infrastructure facilities, steal government data, and create conditions for coordinated full-scale attacks.

Key words: cyber security; media literacy; grooming; cyberbullying; cyber violence; online space; cyber hygiene.

Formulation of the problem. As a result of the rapid integration of information technologies in modern society, a situation has developed that about 80 % of children start using the Internet from the age of 5–11, and this trend continues to spread.

Modern gadgets: mobile phones, smart watches, tablets, laptops, computers give children the opportunity to be "online" almost all the time, which children use to communicate, build and develop social relationships, play various games, exchange information with peers. The points listed above are a positive asset, but these processes also have the reverse side of the coin and often acquire a negative color, which affects the mental and physical health and safety of the child.

Such negative processes can be risks related to the nature of the content (forbidden, violent, destructive, racist, discriminatory actions); risks related to contact by adults or peers: harassment, exclusion, discrimination, defamation and damage to reputation, as well as sexual abuse and sexual exploitation, including extortion, grooming for sexual purposes; risks related to contracts: inappropriate contractual relationships, children's consent issues in the online environment, hidden marketing, online gambling.

Given the above, as well as many other reasons that testify to the negative impact of unlimited harmful content, the relevance of the chosen topic is more important than ever. It is necessary to look for ways to solve problematic aspects, in particular, to raise the level of awareness of children and teenagers about the rules of reasonable use of the Internet, to cultivate a sense of justice, and the ability to distinguish between "black and white".

Analysis of the study of the problem. Among the wide range of works in the field of cybercrimes in Ukraine and the online risks associated with it, we should highlight the following scientific works: A. A. Barikova, A. O. Vedernikova, O. Horodetska, O. O. Zolotar, V. G. Krement, I. Lubenets, O. Mikheeva, M. M. Novikova, A. V. Pazyuka, A. V. Pyvovarova, O. G. Radzievska, V. Rufanova, V. M. Steshenka, T. Yu. Tkachuka and others.

The purpose of the article is to study the concept of cyber-violence in the online space, as well as the factors causing online risks in this area.

Presenting main material. There are many types of cyberbullying: the use of personal data, anonymous threats, silent phone calls, harassment (as one of the elements of physical harassment, sending messages by email or phone, collecting information about the victim, tracking the victim's communications and other forms of harassment), trolling (posting provocative messages messages on the Internet), "fun slaps" (violence for entertainment, for example, filming violence for further distribution on the Internet) and sexual violence [1, p. 43]

In 2018, special reporter on violence against women, its causes and consequences at the 14th session of the UN Human Rights Council noted that online violence against women and girls from a human rights perspective is an increasingly common form of violence committed under with the help of information and communication technologies. The report notes that in the modern digital era, the Internet and ICT have created a social digital space, transforming the ways people meet, communicate and interact, thereby transforming society as a whole [7].

V. M. Rufanova classifies cyber violence into the following 9 categories:

1) transmission of e-mails or messages for the purpose of intimidation or blackmail;
2) dissemination of false information about a person;
3) hacking of e-mail or accounts in social networks;
4) changing or using someone else's password to change or use another person's profile;

5) posting or sending photos of other people for the purpose of ridicule or discussion;

6) posting intimate photos of people with the aim of stigmatizing them or persecuting them;

7) requesting personal information using electronic means of communication for the purpose of distributing personal information;

8) copying and using personal information by hacking into another person's profile in a social network

9) discussion in social networks or chat rooms "for the purpose of slander or discredit", or transmission of messages for the purpose of intimidation or blackmail [6, p. 222].

Regarding the cyber safety of children and the existence of risks of violence against children on the Internet, most experts agreed that before the start of the war, the COVID-19 pandemic had a great impact on the general situation concerning the safety of children in the Internet space and forced many children to study and spend more time in social networks and the Internet. There have been rare cases of child grooming and cyberbullying; the problem of attracting teenagers to "destructive groups" was relevant. Since the start of full-scale hostilities in Ukraine, the situation regarding the safety of children has worsened due to the large-scale violence that war brings to people, evacuation, resettlement, hostilities, deaths, new violent content on the Internet with constant profanity and gruesome photos of deaths, including sexual ones.

Features of prevention of cyberbullying of young people in the school environment are family support, creation of a friendly and trusting atmosphere, contact and problem solving when cyberbullying occurs, as well as coordinated work at school, educational activities of cyber security specialists. Social workers and psychologists, providing support to young people, should be based on the following principles: systematicity, subjectivity, confidentiality, inclusiveness and humanity. Today, preventive work takes place in two directions. The first concerns the development of technical tools (filters, censorship) to limit unwanted content, including "complain" buttons on social networks and websites, privacy settings in personal accounts, etc. This direction also includes the development of systems that allow content and service providers, law enforcement agencies and moderators to quickly respond to illegal activities on the Internet. The second direction of cyberbullying prevention involves teaching Internet users the basic rules of safety and correct behavior in relation to other users of the community. Abroad, there are special web resources dedicated to increasing the level of media literacy and teaching correct, non-offensive and harmless behavior on the Internet [3, p. 5].

Therefore, it should be noted that the main problems of children's Internet safety, which are relevant during military operations in Ukraine, can be attributed to:

– access to text, video and audio information about physical violence, rape, death, destruction, with profanity, etc., causes aggression, sleep disorders, somatic pain, depression, mental and psychological disorders, etc. in children;

– involvement of children in military operations through recruitment through Internet channels or social networks to provide information, logistics and other services for the armed forces of the Russian Federation, which violates the rights of the child according to the UN Convention;

– involvement of children in destructive and suicidal groups with the aim of inflicting physical injuries, performing dangerous tasks, and the final goal is to commit suicide;

– human trafficking with a focus on sexual exploitation, especially among women and teenage girls who are forced to flee from Ukraine [2, pp. 30–31].

In order to prevent the main problems of children's Internet safety, it is necessary to carry out preventive work both with the children themselves and with their parents and teachers and educators. The experience of Canada in this case is important, their preventive work is based on provincial youth programs aimed at preventing violence and cyberbullying as a component of violence. The Administrator of the National Violence Prevention Program provides recommendations to the Government of Canada regarding measures that may affect the prevalence of violence in the country's population. The government has also launched ongoing comprehensive educational programs and initiatives related to gender-based violence and reconciliation in educational institutions. In addition, the theory of "digital citizenship" is being developed among Canadian volunteers and non-governmental organizations working to protect against cyber-violence.

This involves social media users understanding their rights to safe and inclusive online communities. These "digital citizens" can act as implementers of the "Neighborhood Watch" online project, which signals social networks when their platforms are used for acts of violence or abuse [5, p. 63].

The causes of cyberbullying are complex and various. They should be divided into personal (subjective) and social (objective). The most common personal factors affecting aggressive (bullying) behavior in general and the use of information and communication tools in particular are:

– aggressive tendencies and the misconception that aggressive behavior towards others is acceptable;

– striving for superiority and priority, which increases the reliability of friends and peers. During teenage years, the "distance" between parents and children increases, and the authority of parents (teachers) is often inversely proportional to the authority of close friends. At this stage of the child's socialization, one of the main desires is to gain authority among classmates (peers);

– the inferiority complex leads to envy, and sometimes to revenge for insults;

– boredom, when aggression serves as entertainment;

– compensation for failures at school or in relationships (state of frustration);

– lack of conflict resolution or avoidance skills (due to young age);

– the space of children's social interaction is rapidly narrowing. The problem of the modern information society is that people in general, and teenagers in particular, have very few opportunities for direct communication without using electronic means of communication or the Internet;

– features of the personality of minors, such as low self-esteem, secretiveness and low level of empathy [4, p. 171].

Conditions contributing to the proliferation of children's online safety concerns during the war:

– threats to physical security due to military actions take distract from threats in the Internet space;

– children began to devote less time to study, sports and leisure activities;

– parents do not have the resources to pay enough attention to education, leisure time, psychological state of the child due to household problems and often need psychological or humanitarian help themselves;

– law enforcement agencies are focused on maintaining the physical safety of the population and providing humanitarian aid;

– most children, parents and teachers do not perceive risks, threats, bullying or abusive actions in the digital space as a crime;

– most children and parents do not know where to turn for help to prevent or respond to crimes on the Internet;

– the current mechanism for contacting the police is not perceived as accessible, transparent, confidential and effective;

– the lack of coordination and monitoring of the security situation on the Internet by state institutions during the active phase of the war leads to a delay in solving the problem, its concealment from adults and specialists, and an increase in the risks of cyber-violence [8, p. 31].

Conclusions. Consequently, taking into account the information mentioned above, we can see that the list of factors contributing to the development of cyber-violence among children and adolescents is endless and constantly increases in the conditions of the war. Some reasons depend on the children themselves, while others arise with the help of the influence of adults.

Overcoming cyber-violence in Ukraine requires comprehensive measures not only from the Ukrainian state, but also law enforcement and judicial authorities. This includes the creation of an appropriate legal framework for combating cyberviolence, which clearly defines the legal status and jurisdiction of pre-trial investigation authorities and judicial institutions implementing measures to combat cyberviolence. The state, law enforcement agencies, social network companies, experts from various fields and users must work together to combat cyberbullying. However, in order to develop successful programs at the state level, foreign experience must be explored and adapted according to needs.

REFERENCES

1. Vedernikova A. O. (2019*). **Neobkhidnist' kryminal'no-pravovoho rehulyuvannya kiberbulinhu**.* [Necessity of criminal law regulation of cyberbullying]. *Protydiya kiberzahrozam ta torhivli lyud'my* (26 lyst. 2019 r., m. Kharkiv) / MVS Ukrayiny, Kharkiv. nats. un-t vnutr. sprav; Koordynator proektiv OBSYE v Ukrayini. Kharkiv: KHNUVS. P. 42–46 [in Ukrainian].

2. Zvit doslidzhennya (2022). ***Shvydka otsinka sytuatsiyi shchodo kiberbezpeky ditey 10–18 rokiv***. [Rapid assessment of the cyber security situation of children aged 10–18]. Kyyiv. 48 p. [in Ukrainian].

3. Kremen′ V. H., Sysoyeva S. O., Bekh I. D. (2022). *Kontseptsiya vykhovannya ditey ta molodi v tsyfrovomu prostori.* [The concept of raising children and youth in the digital space]. *Visnyk Natsional'noyi akademiyi pedahohichnykh nauk Ukrayiny. 4 (2).* 30 p. [in Ukrainian].

4. Lubenets' I. (2016). ***Kibernasyl'stvo (kiberbulinh) sered uchniv zahal'noosvitnikh navchal'nykh zakladiv***. [Cyber violence (cyberbullying) among students of general educational institutions]. *Natsional'nyy yurydychnyy zhurnal: teoriya i praktyka.* Kyyiv. P. 178–182. [in Ukrainian].

5. Novikov M. M. (2021). ***Teoretyko-pravovyy aspekt kibernasyl'stva: ponyattya ta zmist.*[**]**Theoretical and legal aspect of cyber violence: concept and content]. *Yurydychnyy visnyk, 1 (58).* P. 61–67 [in Ukrainian].

6. Rufanova V. (2021). ***Genderno zumovlene kibernasyl'stvo v svitli praktyky Yevropeys'koho sudu z prav lyudyny***. [Gender-based cyber-violence in the light of the practice of the European Court of Human Rights]. *Knowledge, Education, Law, Management, No. 6. (42).* P. 209–213 [in Ukrainian].

7. ***Dopovid′ Spetsial'noho dopovidacha z pytan′ nasyl'stva shchodo zhinok, yoho prychyn i naslidkiv shchodo nasyl'stva shchodo zhinok i divchat v Interneti z tochky zoru prav lyudyny.*** [Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective]. (A/HRC/38/47, 18 chervnya 2018 r.). Oryhinal: anhl. URL: https://documentsdds-ny.un.org/doc/UNDOC/GEN/G18/184/58/ PDF/G1818458.pdf (data zvernennya 20.11.2023) [in Ukrainian].

Дата надходження: 19.01.2024 р.

Наталія ДІДИК
Національний університет "Львівська політехніка" ,
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права,
психології та інноваційної освіти,
кандидат юридичних наук, доцент,
e-mail: nataliia.i.didyk@lpnu.ua,
ORCID ID: https://orcid.org/0000-0002-6347-5092

Ярина ПАВЛОВИЧ-СЕНЕТА
Львівський державний університет внутрішніх справ
Інститут права,
доцент кафедри адміністративно-правових дисциплін
кандидат юридичних наук, доцент,
e-mail: pyarp@ukr.net,
ORCID ID: https://orcid.org/0000-0002-3491-8878

ОНЛАЙН-РИЗИКИ В УМОВАХ СУЧАСНОСТІ: ПРОБЛЕМИ ТА ШЛЯХИ ПОДОЛАННЯ

Наголошено, що забезпечення безпеки дітей є одним із пріоритетним завдань держави. Сьогодні в умовах стрімкого цифрового розвитку з'являються нові виклики та загрози благополуччю дітей, які спонукають до пошуку дієвих інструментів їх подолання та вироблення комплексного підходу до убезпечення дітей у кіберпросторі.

Акцентовано на тому, що комплексний підхід передбачає зокрема належний рівень підготовки фахівців – суб'єктів, до компетенції яких належить запобігання та реагування на загрози

безпеці дітей у кіберпросторі. Від їхньої професійності, небайдужості, неупередженості залежить своєчасне виявлення загроз для безпеки дітей в кіберпросторі.

Доведено, що безпека роботи з інформацією актуальна як ніколи. Почастішання кібератак на державні та приватні підприємства тільки посилює цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об'єктом прискіпливої уваги правопорушників, тому поступово набуває поширення порівняно нова концепція необхідності для користувачів самостійно дотримуватись елементарних правил безпеки. Такий підхід дає змогу істотно посилити систему колективної безпеки суспільства та держави загалом.

Зазначено, що кібергігієна повинна розглядатися, як особиста гігієна, і після належної інтеграції в організацію стати простою повсякденною процедурою, яка забезпечить оптимальний стан кіберздоров'я організації.

З'ясовано, що порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Нерідко від дій зловмисників страждає і роботодавець жертви. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу для проникнення на об'єкти критичної інфраструктури, викрадення державних даних, створення умов для скоординованих повномасштабних атак.

Ключові слова: кібербезпека; медіаграмотність; грумінг; кібербулінг; кібернасильство; онлайн-простір; кібергігієна.