

UDC 343.436:004.77]:343.222

DOI <https://doi.org/10.32999/ksu2307-8049/2026-3-9>

CYBERBULLYING: LEGAL REGULATION AND LIABILITY

Timashov Viktor Oleksandrovych,
Doctor of Juridical Sciences, Professor,
Professor at the Department of Administrative,
Financial and Information Law
State University of Trade and Economics
v.timashov@knute.edu.ua
orcid.org/0000-0001-8368-8856

The purpose of the article is to study the legal nature of cyberbullying, analyze the current legislation of Ukraine and international experience in the field of combating cyberbullying, as well as develop recommendations for improving the legal regulation of this phenomenon.

Research methods. The study used the formal-legal method – to analyze the regulatory legal acts of Ukraine; the comparative-legal method – to compare Ukrainian legislation with the legislation of the EU, the USA and Canada; the systemic method – for a comprehensive study of cyberbullying as a socio-legal phenomenon; the method of legal analysis – to determine the legal nature and features of the legal regulation of cyberbullying; the generalization method – to form conclusions and proposals; the modeling method – to develop recommendations for improving the legislation of Ukraine; analysis of judicial and law enforcement practice – to assess the effectiveness of the implementation of current legal norms.

Results. The article examines the legal nature of cyberbullying as one of the most dangerous forms of violence in the digital space, which has become a challenge for national legal systems in the 21st century. With the growth of digital communication, social networks, instant messaging platforms and video content, the number of cases of aggressive behavior aimed at humiliating, harassing, discrediting or intimidating a person in the online environment has significantly increased. Of particular concern is the prevalence of cyberbullying among children, adolescents and young people, who are most vulnerable to negative psychological consequences. The relevance of the chosen topic is due to several factors: first, the increase in the number of appeals to law enforcement agencies and educational institutions regarding cases of online bullying; second, the lack of a clear definition of the concept of «cyberbullying» in the current legislation of Ukraine; third, insufficient legal awareness of users about the mechanisms of protection against this type of violence. In this regard, there is an urgent need not only for a legal understanding of the phenomenon of cyberbullying, but also for finding optimal ways to improve legal regulation in order to prevent, detect and stop such offenses. The study is aimed at a comprehensive analysis of the legislative framework that directly or indirectly relates to cyberbullying, studying foreign experience in the field of preventing cyberbullying and formulating proposals for improving the legal mechanism for combating this phenomenon in Ukraine. The article clarifies the legal nature of cyberbullying, outlines the range of socially dangerous acts that can be qualified as cyberbullying, identifies existing gaps in the current legislation and outlines ways to eliminate them.

Conclusions. The article analyzes the provisions of the Law of Ukraine «On Education», the Criminal Code of Ukraine, the Code of Ukraine on Administrative Offenses, as well as subordinate regulatory legal acts that regulate liability for cyberbullying and related actions. Attention is also paid to the practice of applying these norms in national courts and analyzes which digital platforms are most often used as tools for cyberbullying. The paper conducts a comparative legal analysis of the experience of the European Union, the USA and Canada, where cyberbullying is recognized as a separate crime and special rules for the protection of victims are established. The study substantiates the need to establish at the legislative level the definition of the concept of «cyberbullying» and the introduction of the appropriate composition of an administrative or criminal offense and the possibility of using the proposed recommendations in the activities of law enforcement agencies, in the development of draft laws, educational programs and in the development of preventive measures.

Keywords: cyberbullying, psychological violence, digital environment, legal regulation, information security, legal liability.



КІБЕРБУЛІНГ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ВІДПОВІДАЛЬНІСТЬ

Тімашов Віктор Олександрович,
доктор юридичних наук, професор,
професор кафедри адміністративного,
фінансового та інформаційного права
Державного торговельно-економічного університету
v.timashov@knute.edu.ua
orcid.org/0000-0001-8368-8856

***Метою** статті є дослідження правової природи кібербулінгу, аналіз чинного законодавства України та міжнародного досвіду у сфері протидії кібербулінгу, а також розроблення рекомендацій щодо вдосконалення правового регулювання цього явища.*

***Методи дослідження.** Під час дослідження використано формально-юридичний метод – для аналізу нормативно-правових актів України; порівняльно-правовий метод – для зіставлення українського законодавства із законодавством ЄС, США та Канади; системний метод – для комплексного дослідження кібербулінгу як соціально-правового явища; метод правового аналізу – для визначення правової природи та особливостей правового регулювання кібербулінгу; метод узагальнення – для формування висновків і пропозицій; метод моделювання – для розроблення рекомендацій щодо вдосконалення законодавства України; аналіз судової та правозастосовної практики – для оцінки ефективності реалізації чинних правових норм.*

***Результати.** У статті досліджується правова природа кібербулінгу як однієї з найнебезпечніших форм насильства в цифровому просторі, що стала викликом для національних правових систем у XXI столітті. Зі зростанням цифрової комунікації, соціальних мереж, платформ обміну миттєвими повідомленнями та відеоконтенту значно збільшилися кількість випадків агресивної поведінки, спрямованої на приниження, переслідування, дискредитацію або залякування особи в онлайн-середовищі. Особливе занепокоєння викликає поширеність кібербулінгу серед дітей, підлітків та молоді, які є найбільш вразливими до негативних психологічних наслідків.*

Актуальність обраної теми зумовлена кількома факторами: по-перше, збільшенням кількості звернень до правоохоронних органів та навчальних закладів щодо випадків булінгу в мережі; по-друге, відсутністю чіткого визначення поняття «кібербулінг» у чинному законодавстві України; по-третє, недостатньою правовою обізнаністю користувачів про механізми захисту від цього виду насильства. У зв'язку з цим існує нагальна потреба не лише у правовому осмисленні явища кібербулінгу, а й у пошуку оптимальних шляхів удосконалення правового регулювання з метою попередження, виявлення та припинення таких правопорушень.

Дослідження направлено на комплексний аналіз законодавчої бази, яка прямо чи опосередковано стосується кібербулінгу, вивчення зарубіжного досвіду у сфері запобігання кібернасильству та формулювання пропозицій щодо вдосконалення правового механізму протидії цьому явищу в Україні. В статті з'ясується правова природа кібербулінгу, окреслення кола суспільно небезпечних діянь, які можуть бути кваліфіковані як кібербулінг, виявлення існуючих прогалин у чинному законодавстві та окреслення шляхів їх усунення.

***Висновки.** У статті проаналізовані положення Закону України «Про освіту», Кримінального кодексу України, Кодексу України про адміністративні правопорушення, а також підзаконні нормативно-правові акти, що регулюють відповідальність за кібербулінг та пов'язані з ним дії. Також приділено увагу практиці застосування цих норм у національних судах та проаналізовано, які цифрові платформи найчастіше використовуються як інструменти для кібербулінгу. В роботі проведений порівняльно-правовий аналіз досвіду Європейського Союзу, США та Канади, де кібербулінг визнано окремим злочином та встановлено спеціальні правила захисту жертв.*

Дослідження обґрунтовує необхідність закріплення на законодавчому рівні визначення поняття «кібербулінг» та введення відповідного складу адміністративного або кримінального правопорушення та у можливості використання запропонованих рекомендацій у діяльності правоохоронних органів, при розробці законопроектів, освітніх програм та при розробці превентивних заходів.

***Ключові слова:** кібербулінг, психологічне насильство, цифрове середовище, правове регулювання, інформаційна безпека, юридична відповідальність.*

Introduction. In today's digital society, the widespread use of Internet technologies, social media platforms, messaging applications, and online games has become an integral part of everyday life, particularly among young people. Alongside the numerous benefits of digitalization, new threats have also emerged, one of the most significant being cyberbullying – a form of psychological violence perpetrated through information

and communication technologies (ICT). The relevance of this study is driven by the substantial increase in the number of cyberbullying incidents in Ukraine, as well as the lack of effective legal and regulatory mechanisms for its prevention and counteraction.

Cyberbullying manifests itself in the form of insults, humiliation, blackmail, and the dissemination of false or compromising information

about an individual through digital platforms. Particular attention should be paid to cyberbullying among minors, as it has a detrimental impact on their mental health, socialization, and educational process. The proliferation of this phenomenon is accompanied by significant challenges for law enforcement practice, including the absence of specific legislative provisions, difficulties in identifying perpetrators, and obstacles to collecting and preserving digital evidence (Ministry of Digital Transformation of Ukraine, 2021).

1. Theoretical and Legal Foundations of Cyberbullying and Its Legal Regulation in Ukraine

Cyberbullying is a form of aggressive behavior carried out through information and communication technologies (ICT) with the purpose of humiliating, intimidating, or inflicting psychological harm on another individual (Hidenko, 2021: 26). This phenomenon has become increasingly widespread in the context of the rapid digitalization of society, particularly among children and young people. A distinctive feature of cyberbullying is its continuous nature: unlike traditional bullying, it can persist around the clock regardless of the victim's location, affecting virtually every aspect of their personal life.

At present, Ukrainian legislation does not provide a separate legal definition of cyberbullying. However, Article 30-1 of the Law of Ukraine On Education defines bullying as a form of psychological violence, including acts committed through electronic means of communication (Law of Ukraine «On Education», 2017). Accordingly, cyberbullying may be regarded as a distinct form of bullying that occurs exclusively within the digital environment (Law of Ukraine «On Education», 2017).

This form of violence is perpetrated through social media platforms, messaging applications, online forums, email services, video-sharing platforms, online games, and other digital communication channels. Common manifestations of cyberbullying include the dissemination of abusive messages, the publication of false or compromising information, threats, blackmail, social exclusion or deliberate ostracism from online groups, and the creation of fake accounts intended to discredit the victim. The anonymity of perpetrators, the rapid dissemination of online content, and the technical challenges associated with identifying those responsible create additional obstacles to the effective prevention and counteraction of this phenomenon.

Cyberbullying causes significant harm not only to an individual's emotional well-being but may also result in violations of the rights to honor, dignity, and privacy. In some cases, it can lead to severe mental health disorders, social isolation, and even suicide attempts. Particularly concerning is the fact that victims often do not seek assistance, either because they perceive doing so as a sign of weakness or because they are unaware of the legal nature of the offense committed against them (Korniychenko, 2021).

Moreover, cyberbullying may be perpetrated either by an individual or collectively, where

abusive conduct is carried out by a group of individuals. As a result, the informational pressure exerted on the victim intensifies, leading to even more severe consequences. In practice, negative content targeting an individual is often not only created but also disseminated by other users within digital communities, making the problem multidimensional and considerably more difficult to address through legal mechanisms (Korniychenko, 2021).

Thus, cyberbullying constitutes a complex socio-legal phenomenon that requires a comprehensive approach to its study, prevention, and effective legal response (Korniychenko, 2021). The distinctive characteristics of this form of misconduct lie in the interplay of technical, psychological, and legal dimensions, which complicates its identification, investigation, and proof under the existing legislative framework. Consequently, cyberbullying requires not only comprehensive legal conceptualization but also legislative reform aimed at providing a precise legal definition and establishing clear mechanisms for holding perpetrators accountable.

At present, Ukrainian legislation does not contain a separate legislative act that comprehensively regulates the prevention and counteraction of cyberbullying (Chumak, Tsebinoha, 2018). Nevertheless, a number of legislative acts include provisions that directly or indirectly address this phenomenon. The principal legal instrument is the Law of Ukraine On Education, which, in 2019, formally introduced the term bullying and established its legal definition. Pursuant to Article 30-1 of this Law, bullying is defined as systematic conduct aimed at humiliating an individual's dignity or inflicting psychological or physical violence, including acts committed through electronic means of communication (Law of Ukraine «On Education», 2017).

Under this Law, liability for bullying may be imposed on students, their parents or legal guardians, teaching staff, and the administration of educational institutions. The legislation provides for administrative fines as a sanction for such misconduct, as well as the possibility of entering relevant information into the Unified Register of Pre-Trial Investigations in cases where the conduct exhibits the elements of a criminal offense.

The Code of Ukraine on Administrative Offenses has also been supplemented by Article 173-4 (Code of Ukraine on Administrative Offenses, 1984), which establishes administrative liability for bullying. The sanctions include the imposition of a fine or community service, with more severe penalties applicable in cases of repeated offenses. However, the legislation does not recognize cyberbullying as a distinct form of bullying, which creates significant challenges in law enforcement practice. In practice, identifying, proving, and holding accountable individuals who engage in online harassment is considerably more difficult than in cases involving offline violence.

Ukrainian criminal legislation may also be applied in cases of cyberbullying where



the perpetrator's conduct constitutes a criminal offense. For example, Article 129 of the Criminal Code of Ukraine may be invoked in cases involving threats of murder or threats to cause harm to a person's health or property. Article 182 of the Criminal Code of Ukraine applies to the unlawful collection, storage, or dissemination of confidential information. Where an individual's conduct amounts to incitement to suicide, Article 120 of the Criminal Code of Ukraine may be applicable (Criminal Code of Ukraine, 2001). It should be noted, however, that these provisions are invoked only in the most serious cases, where the consequences are clearly criminal in nature.

Judicial practice concerning cyberbullying in Ukraine remains limited. In most cases, incidents are classified under the general legal provisions governing bullying without distinguishing their digital dimension. This highlights the need to improve the legal approaches to the classification of such offenses, as well as to provide a more detailed specification of the defining characteristics of cyberbullying within the relevant legal framework. Furthermore, the existing legislative framework fails to adequately account for the technical characteristics of the digital environment, including perpetrator anonymity, the use of virtual private networks (VPNs), and temporary user accounts, all of which complicate both the collection of evidence and the identification of offenders (Criminal Code of Ukraine, 2001).

Overall, the Ukrainian legal and regulatory framework governing cyberbullying remains at an early stage of development and does not yet provide an adequate level of protection for victims of online bullying. There is an urgent need for a clear legislative definition of cyberbullying, effective mechanisms for identifying perpetrators, and well-defined legal sanctions. It would be appropriate to amend the existing legislation by introducing specific provisions that take into account the distinctive characteristics of offenses committed within the digital environment, while also strengthening cooperation between public authorities and digital platforms to ensure a prompt and effective response to such incidents.

2. Foreign Experience in the Legal Regulation of Cyberbullying and Challenges in Counteracting it

Cyberbullying is a global phenomenon, and many countries have already introduced appropriate legal mechanisms to address it. The experience of foreign jurisdictions may serve as a valuable reference for developing an effective strategy to prevent and counteract cyberbullying in Ukraine, as it encompasses not only legislative measures but also educational and preventive approaches.

The United States was among the first countries to recognize cyberbullying as a distinct legal offense (US State Laws on Cyberbullying. StopBullying.gov., 2023). In the United States, the regulation of cyberbullying is primarily governed at the state level. For example, California, New York, Florida, and several other states have

enacted specific legislation defining cyberbullying as unlawful online conduct, including acts committed against minors in educational settings. These laws require educational institutions to document and respond to incidents of online bullying, as well as to implement preventive educational programs for students. In many cases, perpetrators may be held criminally or administratively liable, and their access to certain digital resources may be restricted as part of the legal response (US State Laws on Cyberbullying. StopBullying.gov., 2023).

In Canada, the Protecting Canadians from Online Crime Act was enacted in 2014 to directly address cyber-enabled violence and related online offenses (NetzDG – Network Enforcement Act, 2014). The Act establishes criminal liability for the non-consensual distribution of intimate images, a measure introduced in response to the growing prevalence of so-called «revenge pornography». Canadian legislation also provides for close cooperation with online service providers and digital platforms, enabling the prompt removal of harmful online content (Protecting Canadians from Online Crime Act, 2014).

Within the European Union, cyberbullying is addressed primarily in the context of child protection and digital safety. The European Union supports the implementation of the Better Internet for Kids (BIK+) initiative, which aims to create a safer online environment for children (European Commission, 2025). Many EU Member States, including Poland, France, and Germany, have enacted specific legislation or introduced amendments to their criminal codes to criminalize online harassment, insults, defamation, and other forms of cyberbullying.

For example, in Poland, Article 190a of the Criminal Code establishes criminal liability for stalking, including conduct carried out through online means (NetzDG – Network Enforcement Act, 2017). The law also authorizes courts to prohibit offenders from contacting victims in any manner, including via the Internet. In Germany, the Network Enforcement Act (NetzDG), which entered into force in 2018, requires social media platforms to respond promptly to complaints regarding unlawful content by removing manifestly illegal material within 24 hours of receiving a complaint (NetzDG – Network Enforcement Act, 2017). Failure to comply with these obligations may result in substantial financial penalties.

International practice demonstrates that effective prevention and counteraction of cyberbullying require not only robust legislative measures but also educational initiatives and the active involvement of digital platforms in responding to users' complaints. Many countries have also established national helplines, informational websites, and online counseling services for children, parents, and educators to provide guidance, support, and assistance in addressing incidents of cyberbullying (UN Committee on the Rights of the Child, 2021).

Thus, foreign experience demonstrates that the legal regulation of cyberbullying should

adopt a multi-level approach encompassing criminal, administrative, and educational measures. Ukraine may draw upon the best practices of the European Union Member States and North American countries while adapting them to its national legal and social context. The introduction of a clear legal definition of cyberbullying, the establishment of liability for digital platforms, and the implementation of specialized preventive measures constitute essential steps toward creating a safe and secure digital environment in Ukraine.

3. Directions for Improving the Legal Regulation of Cyberbullying in Ukraine

Despite the existence of certain legislative provisions addressing bullying, including its manifestations in the digital environment, the practical implementation of measures to prevent and counteract cyberbullying in Ukraine continues to face a number of significant challenges. These difficulties arise from both legal and organizational-technical factors, which complicate the identification of perpetrators, the collection and documentation of evidence, and the imposition of legal liability on individuals who engage in cyberbullying.

One of the key challenges is the absence of a clear legal definition of cyberbullying in Ukrainian legislation (Law of Ukraine «On Education», 2017). This legal uncertainty gives rise to difficulties in the classification of relevant offenses, as cyberbullying is often conflated with other forms of digital aggression, such as defamation, stalking, hacking, or the unauthorized disclosure of personal information. As a result, law enforcement authorities generally classify such conduct under broader legal provisions without taking into account the distinctive characteristics of the digital environment.

Another significant challenge lies in the technical complexity of investigating cyberbullying, particularly the anonymity of perpetrators (Law of Ukraine «On Education», 2017). Individuals who engage in cyberbullying may use fake profiles, temporary email addresses, virtual private networks (VPNs), and other tools designed to conceal their identities. Identifying such individuals often requires the involvement of cybersecurity specialists, as well as cooperation with the administrators of social media platforms, messaging services, and other online platforms, many of which are based outside Ukraine. Consequently, law enforcement authorities face substantial obstacles in collecting evidence and establishing the perpetrator's guilt.

An equally significant challenge is the low level of legal awareness among victims, as well as among representatives of educational institutions, parents, and law enforcement officers. Many individuals are unaware that they have become victims of cyberbullying or do not know where to seek legal or psychological assistance (Hidenko, 2021). Consequently, incidents of cyberbullying often fail to receive an appropriate response, particularly in cases involving minors who are reluctant to report abusive behavior. In turn, school administrations frequently limit their response to

formal procedures or disregard incidents occurring outside the physical premises of the educational institution, despite their potential impact on students' well-being (Law of Ukraine «On Education», 2017).

In practice, another significant challenge is the insufficient coordination among the public authorities and institutions responsible for responding to cyberbullying, including law enforcement agencies, education authorities, child protection services, psychologists, and the courts. The absence of clearly defined response protocols, specialized response units, and standardized procedural guidelines often results in delays in the handling of cases and leaves victims without effective legal protection (Korniychenko, 2021).

An additional challenge is the rapid dissemination of harmful content on the Internet. Even when a timely response is provided, such content often cannot be completely removed because it may already have been saved by other users or redistributed across third-party platforms. This significantly hinders the full restoration of the victim's reputation and further intensifies the psychological harm caused by cyberbullying (Cyberbullying – legal response mechanisms, 2021).

Overall, the effective implementation of the existing legal framework for preventing and counteracting cyberbullying in Ukraine is hindered by a range of factors, including ambiguous legal provisions as well as technical and organizational barriers. Addressing these challenges requires a comprehensive and systematic approach, including legislative reform, the establishment of specialized support and response services, the enhancement of public legal awareness, and strengthened cooperation between public authorities and digital platforms (Cyberbullying – legal response mechanisms, 2021).

In light of the existing shortcomings in the current legislative framework and its practical implementation, there is a clear need to improve the legal regulation of cyberbullying in Ukraine. The proposed reforms should be aimed at establishing a clear legal framework for the protection of victims while also enhancing the effectiveness of responses to incidents of cyberbullying (Ministry of Digital Transformation of Ukraine, 2021).

First and foremost, it is advisable to introduce a statutory definition of «cyberbullying» as a distinct legal offense. Such a provision should reflect the specific characteristics of the digital environment and encompass the principal forms of cyberbullying, including online insults, blackmail, the dissemination of false or confidential information, threats, and other forms of online intimidation and harassment. A clear legal definition would not only promote greater consistency in judicial practice but also facilitate the uniform application of the law throughout the country (Cyberbullying – legal response mechanisms, 2021).

A further step could involve amending the Code of Ukraine on Administrative Offenses and the Criminal Code of Ukraine by introducing specific provisions establishing liability for



cyberbullying. The sanctions should be proportionate to the gravity of the offense and may range from administrative fines and restrictive measures (such as prohibiting access to certain Internet resources) to imprisonment in particularly serious cases where cyberbullying has resulted in severe psychological or physical harm to the victim (Code of Ukraine on Administrative Offenses, 1984).

The active involvement of digital platforms, including social media networks, messaging services, and online forums, is of particular importance within the system for preventing and counteracting cyberbullying. The State should establish partnership agreements with major online service providers to facilitate cooperation in combating digital violence. Such cooperation would enable the prompt detection and removal of harmful content, the preservation of digital evidence for investigative purposes, and the restriction or suspension of perpetrators' accounts where appropriate (European Commission, 2025).

Furthermore, it is necessary to establish a unified online reporting system for individuals who have become victims of cyberbullying. Such a mechanism should provide users with a simple and accessible means of reporting incidents, uploading screenshots and other forms of digital evidence, facilitating the automated processing of complaints, and enabling direct communication with law enforcement authorities. The implementation of this system would promote a more rapid and effective response to cyberbullying incidents, strengthen public confidence in legal protection mechanisms, and contribute to reducing the incidence of repeated online harassment (US State Laws on Cyberbullying. StopBullying.gov., 2023).

Preventive measures also play a crucial role in combating cyberbullying. It is essential to implement systematic public awareness campaigns and educational programs for children, parents, teachers, and law enforcement officers focusing on safe Internet use, the identification of cyberbullying, and the available mechanisms for obtaining legal protection (Law of Ukraine «On Education», 2017). In addition, digital ethics should be incorporated into school and university curricula as an integral component of digital citizenship education (UN Committee on the Rights of the Child, 2021).

The mechanisms for collecting statistical data and monitoring incidents of cyberbullying also require further improvement. The availability of comprehensive and reliable official data would enable a more accurate assessment of the scale of the problem, facilitate the identification of the most vulnerable groups, and support the development of targeted public policies and evidence-based preventive measures (Chumak, Tsebinoha, 2018).

In conclusion, a comprehensive improvement of the legislative framework, technical monitoring mechanisms, international cooperation, and public awareness initiatives constitutes a fundamental prerequisite for the effective prevention and counteraction of cyberbullying in Ukraine. The implementation of the proposed

reforms will contribute to strengthening information security, enhancing the protection of citizens' rights, and fostering a safe and secure digital environment (NetzDG – Network Enforcement Act., 2017).

Conclusions. The study has demonstrated that cyberbullying is a complex and multifaceted phenomenon that has emerged as a consequence of the rapid development of digital technologies and the globalization of the communication environment. It poses a significant threat not only to the psychological well-being of victims but also to their information security, right to privacy, and personal honor and dignity. Cyberbullying is particularly dangerous for children and young people, who constitute the most vulnerable group within the digital environment.

The analysis of Ukrainian legislation demonstrates that the current legal framework contains only fragmented provisions governing bullying in general, without distinguishing its digital form. The absence of a clear legal definition of cyberbullying, the fragmented nature of the relevant legal provisions, the limited body of judicial practice, the technical difficulties associated with identifying perpetrators, and the low level of public awareness constitute the principal factors hindering the effective prevention and counteraction of this phenomenon.

International experience demonstrates that the effective prevention and counteraction of cyberviolence requires not only legislative reform but also the active involvement of digital platforms, the implementation of preventive measures, and the development of comprehensive support systems for victims. Ukraine has significant potential to draw upon the best practices of the European Union, the United States, and Canada and to adapt them to its national legal and institutional context.

Thus, the effective prevention and counteraction of cyberbullying requires a comprehensive and systematic approach that integrates legal, technical, and educational measures. The implementation of the proposed reforms will contribute to strengthening digital security, enhancing the protection of citizens' rights in the online environment, and increasing public trust in digital technologies as an integral component of contemporary society.

Conflict of Interest. The author declares no conflict of interest.

BIBLIOGRAPHY:

1. Міністерство цифрової трансформації України. Національна стратегія захисту дітей в цифровому середовищі на 2021–2026 роки. URL: <https://thedigital.gov.ua/regulations/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomu-seredovishchi-na-2021-2026-roki>
2. Гіденко Є. С. Кібербулінг: насильство в соціальній мережі // *Вісник МГУ. Серія: Право*. 2021. Вип. 50. С. 26–29. <https://doi.org/10.32841/2307-1745.2021.50.6>
3. Закон України «Про освіту» від 05.09.2017 № 2145-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>
4. Корнійченко А.О. Адміністративно-правовий механізм запобігання булінгу в Україні: дис. ... д-ра філософії: 081

«Право» / Центральноукраїнський державний педагогічний університет імені Володимира Винниченка. Кропивницький, 2021. URL: https://cusu.edu.ua/images/autoreferats/2021/Kornijchenko/dis_KornijchenkoA.pdf

5. Чумак В.В., Цебінога В.Ю. Правове регулювання протидії кібербулінгу в Україні // *Матеріали науково-практичної конференції Харківського національного університету внутрішніх справ (30 листопада 2018 р.)*. Харків, 2018. С. 202–204. URL: https://univd.edu.ua/general/publishing/konf/30_11_2018/pdf/99.pdf

6. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073 X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>

7. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

8. US State Laws on Cyberbullying. StopBullying.gov. URL: <https://www.stopbullying.gov/resources/laws>

9. Protecting Canadians from Online Crime Act, 2014. Government of Canada. URL: <https://www.parl.ca/DocumentViewer/en/41-2/bill/C-13/royal-assent>

10. European Commission. Better Internet for Kids Programme. URL: <https://www.betterinternetforkids.eu/>

11. NetzDG – Network Enforcement Act. Federal Ministry of Justice (Germany). URL: https://www.bmj.de/EN/Topics/Fokus/TheNetworkEnforcementAct/NetzDG_node.html

12. UN Committee on the Rights of the Child. General Comment No. 25 on children's rights in relation to the digital environment. 2021. URL: <https://digitallibrary.un.org/record/3925923>

13. Кібербулінг – правові механізми реагування // *Громадський Простір*. 12.02.2021. URL: <https://www.prostir.ua/?news=kiberbulinh-pravovi-mehanizmy-reahuvannya>

REFERENCES:

1. Ministerstvo tsyfrovyi transformatsiyi Ukrainy. Natsional'na stratehiya zakhystu ditey v tsyfrovomu seredovyshchi na 2021–2026 roky [Ministry of Digital Transformation of Ukraine. National Strategy for the Protection of Children in the Digital Environment for 2021–2026]. URL: <https://thedigital.gov.ua/regulations/natsionalna-strategiya-zakhystu-ditey-v-tsifrovomu-seredovyshchi-na-2021-2026-roki>

2. Hidenko YE. S. (2021). Kiberbulinh: nasyt'stvo v sotsial'niy merezhi [Cyberbullying: violence on social media]. *Visnyk MHU. Seriya: Pravo – Scientific Bulletin of the International Humanitarian University*. Series: «Jurisprudence» Issue. 50. P. 26–29. <https://doi.org/10.32841/2307-1745.2021.50.6>

3. Zakon Ukrainy «Pro osvitu» vid 05.09.2017 № 2145-VIII [Law of Ukraine «On Education» dated 05.09.2017 No. 2145-VIII]. URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>

4. Kornijchenko A.O. (2021). Administratyvno-pravovyy mekhanizm zapobihannya bulinhu v Ukraini [Administrative and legal mechanism for preventing bullying in Ukraine]: dys. ... d-ra filosofiyi: 081 «Pravo» / Tsentral'noukrayins'kyy derzhavnyy pedahohichnyy universytet imeni Volodymyra Vynnychenka. Kropyvnyts'ky – Volodymyr Vynnychenko Central Ukrainian State Pedagogical University. URL: https://cusu.edu.ua/images/autoreferats/2021/Kornijchenko/dis_KornijchenkoA.pdf

5. Chumak V.V., Tsebinoha V.YU. (2018). Pravove rehulyuvannya protydyi kiberbulinhu v Ukraini [Legal regulation of countering cyberbullying in Ukraine] // *Materialy nauково-praktychnoyi konferentsiyi Kharkivs'koho natsional'noho universytetu vnutrishnikh sprav (30 lystopada 2018 r.)*. Kharkiv P. 202–204. URL: https://univd.edu.ua/general/publishing/konf/30_11_2018/pdf/99.pdf

6. Kodeks Ukrainy pro administratyvni pravoporushennya vid 07.12.1984 № 8073 X. [Code of Ukraine on Administrative Offenses]. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>

7. Kryminal'nyy kodeks Ukrainy vid 05.04.2001 № 2341-III. [Criminal Code of Ukraine]. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

8. US State Laws on Cyberbullying. StopBullying.gov. URL: <https://www.stopbullying.gov/resources/laws>

9. Protecting Canadians from Online Crime Act, 2014. Government of Canada. URL: <https://www.parl.ca/DocumentViewer/en/41-2/bill/C-13/royal-assent>

10. European Commission. Better Internet for Kids Programme. URL: <https://www.betterinternetforkids.eu/>

11. NetzDG – Network Enforcement Act. Federal Ministry of Justice (Germany). https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/NetzDG_engl.pdf?__blob=publicationFile&v=4&utm

12. UN Committee on the Rights of the Child. General Comment No. 25 on children's rights in relation to the digital environment. 2021. URL: <https://digitallibrary.un.org/record/3925923>

13. Kiberbulinh – pravovi mekhanizmy reahuvannya (2021) [Cyberbullying – legal response mechanisms] // *Hromads'kyi Prostir*. 12.02.2021. URL: <https://www.prostir.ua/?news=kiberbulinh-pravovi-mehanizmy-reahuvannya>

Дата першого надходження статті до видання: 17.07.2026

Дата прийняття статті до друку після рецензування: 04.08.2026

Дата публікації (оприлюднення) статті: 01.09.2026