DOI: https://doi.org/10.36059/978-966-397-661-7-5

LEGAL MECHANISMS FOR ENSURING THE DIGITAL SAFETY OF CHILDREN AT EDUCATIONAL INSTITUTIONS UNDER MARTIAL LAW

Bondarenko Viktoriia Anatoliivna,
PhD in Law, Associate Professor,
Professor at the Language Training Department,
Lviv State University of Internal Affairs,
26 Horodotska Street, Lviv, 79007, Ukraine

Introduction

In the current world of rapid digitalisation and the transformation of the education system, ensuring children's safety online is becoming increasingly important[170]. The widespread adoption of information and communication technologies at educational institutions, as well as the use of online platforms, distance and hybrid learning, contribute to expanding access to knowledge; however, they also present new challenges and risks for children[171].

The main threats in the digital environment include cyberbullying, online violence, unauthorised access to personal data, the dissemination of harmful content, and the manipulative influence of information[172]. A particular concern is the low level of digital literacy among those involved in the education system, which makes it difficult to respond effectively to such threats.

The relevance of this research is significantly increasing under martial law in Ukraine[173], where a large part of the educational process is carried out using digital technologies. Under these circumstances, the digital environment becomes the primary space for children's learning, communication, and socialisation, where the risk of their rights and freedoms is being infringed[174].

---

[170] OECD. (2021). *Children in the Digital Environment: Revised Typology of Risks*. Paris: OECD Publishing, DOI: https://doi.org/10.1787/9c8c9c5d-en

[171] European Commission. (2021). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

[172] Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*(6), 22–30. https://doi.org/10.1016/j.jadohealth.2007.08.017

[173] Cabinet of Ministers of Ukraine. (n.d.). *Strategy for the development of digital education in Ukraine*. https://www.kmu.gov.ua

[174] United Nations. (1989). *Convention on the Rights of the Child* (November 20). https://zakon.rada.gov.ua/laws/show/995_021

Legal safeguards for children's digital safety form part of the overall system for protecting children's rights and creating a safe educational environment[175]. The relevant mechanisms should include not only regulatory and legal frameworks, but also effective institutional and organisational tools for implementing legal provisions.

Despite the existence of a significant number of legislative and regulatory acts governing education, data protection, and children's rights, there remains a problem of their fragmentation and insufficient adaptation to modern digital challenges[176]. At the same time, the lack of uniform digital security standards at educational institutions and the inadequate implementation of relevant regulations in practice highlight the need for further academic analysis of this issue.

The purpose of the study is to analyse the legal mechanisms for ensuring children's digital safety at educational institutions and to identify areas for their improvement.

To achieve this aim, the following tasks are set:

– to define the concept of children's digital safety;
– to describe the main threats in the digital environment;
– to analyse the regulatory framework for children's digital safety;
– to identify problems in the implementation of legal mechanisms;
– to justify areas for their improvement.

The methodological framework of the study is based on general scientific and specialised methods of cognition, in particular the formal-legal, systemic-structural, comparative-legal, and analytical methods.

1 Theoretical and legal foundations of children's digital safety at educational institutions

In contemporary legal studies, the issue of ensuring children's digital safety is regarded as part of a broader category – personal safety in the information society[177]. The digitalisation of the educational environment necessitates the development of new approaches to understanding child safety, which take into account the specific nature of information and communication technologies and their impact on personal development.

[175] Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On Education"* (№ 2145-VIII, September 5). https://zakon.rada.gov.ua/laws/show/2145-19

[176] OECD. (2021). *Children in the digital environment: Revised typology of risks*. OECD Publishing. https://www.oecd.org https://doi.org/10.1787/9c8c9c5d-en

[177] Ostroukhov, V. V. (Ed.), Prysiazhniuk, M. M., Farmahei, O. I., Chekhovska, M. M., et al. (2021). *Informatsiina bezpeka [Information security].* Lira-K.

The concept of "digital safety for children" lacks a single, established definition in national legislation, which makes it necessary to examine it from a theoretical perspective. In the academic literature, children's digital safety is regarded as the protection of a child's vital interests in the digital environment from internal and external threats[178]. Other researchers define it as a set of legal, organisational, and technical measures aimed at preventing the negative impact of information technology on a child's physical, mental, and social development[179].

At the same time, digital safety should be viewed not merely as a state of security, but as a process involving the continuous improvement of mechanisms for protecting children's rights in the context of the rapid development of digital technologies. This approach allows for the changing nature of threats and the need to adapt legal mechanisms to new challenges.

An important category closely linked to digital security is the "safe learning environment"[180]. According to current academic approaches, a safe educational environment comprises a set of conditions that ensure the physical, psychological, informational, and digital safety of those involved in the educational process. Digital safety is therefore an integral part of the overall safety system at educational institutions.

In the context of this study, it is worth highlighting the key characteristics of children's digital safety:

- Comprehensiveness (covering various aspects of a child's life).
- Dynamism (dependence on technological developments).
- Interdisciplinarity (combining legal, educational, and technical aspects).
- Preventive nature (focus on averting threats).

The classification of threats to the digital environment is particularly important[181]. It enables a systematic approach to developing legal mechanisms to overcome them.

The main types of threats include:

1. Socio-psychological threats

This group comprises:

– cyberbullying (systematic harassment in an online environment)[182];

[178] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657–670. https://doi.org/10.1177/1461444816686318

[179] Staksrud, E. (2013). *Children in the online world: Risk, regulation, rights.* Routledge. https://doi.org/10.4324/9781315887136

[180] Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On Education"* (№ 2145-VIII, September 5). https://zakon.rada.gov.ua/laws/show/2145-19

[181] OECD. (2021). *Children in the Digital Environment: Revised Typology of Risks.* Paris: OECD Publishing, DOI: https://doi.org/10.1787/9c8c9c5d-en

[182] Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*(6), 22–30. https://doi.org/10.1016/j.jadohealth.2007.08.017

– online violence;
– psychological pressure via social media;
– digital addiction.

These threats have a significant impact on a child's mental and emotional well-being and can lead to long-term negative consequences.

2. Information-related threats

These threats include:

– access to harmful or prohibited content;
– the spread of misinformation[183];
– manipulative use of information;
– propaganda content.

Under martial law, information campaigns designed to create a distorted perception of reality are particularly dangerous.

3. Technical and cyber threats

These threats include:

– phishing;
– account hacking;
– malware;
– personal data breaches[184].

These threats are directly linked to the level of cybersecurity of the digital platforms used in the educational process.

4. Legal risks[185]

These risks include:

– insufficient regulation of digital relations;
– the lack of clear security standards;
– the difficulty of bringing offenders to justice for online offences;
– gaps in the protection of children's personal data.

The existence of such risks highlights the need to improve the legal regulation of the digital environment.

An important aspect of the theoretical understanding of digital safety is determining its place within the framework of children's rights. Digital safety is directly linked to the realisation of rights such as the right to privacy, the right to protection from violence, the right to information, and the right to a safe

[183] UNICEF. (2017). *The State of the World's Children 2017: Children in a Digital World.* https://www.unicef.org

[184] European Parliament & Council of the European Union. (2016*). Regulation (EU) 2016/679 (General Data Protection Regulation).* https://eur-lex.europa.eu https://doi.org/10.2860/108933

[185] Kovaliv, M. V., Yesimov, S. S., Yarema, O. H. (2022). Informatsiine pravo Ukrainy : navchalnyi posibnyk [Information Law of Ukraine: a textbook]. Lvivskyi derzhavnyi universytet vnutrishnikh sprav.

learning environment[186]. A violation of digital security actually means a restriction or infringement of these rights. Furthermore, contemporary academic approaches emphasise the need to establish a "digital safety culture"[187], which involves developing safe digital behaviour skills among children and educators. This approach allows legal mechanisms to be combined with educational and upbringing measures.

Consequently, the digital safety of children at educational institutions is a complicated, multi-dimensional phenomenon that requires comprehensive legal regulation. It can only be effectively ensured through a combination of theoretical approaches, appropriate normative support, and the practical implementation of relevant mechanisms.

2. Normative and legal provisions for the digital safety of children at educational institutions

The normative and legal basis for children's digital safety at educational institutions comprises a set of interrelated national and international legal acts governing relations in the fields of education, the protection of children's rights, information security, and the processing of personal data[188]. The effectiveness of legal mechanisms in this area depends largely on the coherence of these acts and their adaptability to modern digital challenges.

The primary legislation setting out the general principles governing the functioning of the education system is the Law of Ukraine "On Education"[189]. It enshrines the right of learners to safe and healthy learning conditions, which also encompasses safety in the digital environment. At the same time, the Law sets out the obligations of educational institutions to create a safe educational environment, including the prevention of all forms of violence and discrimination.

The Law of Ukraine "On the Protection of Children"[190] is of great importance, as it sets out the fundamental guarantees for the protection of children's rights.

[186] United Nations. (1989). *Convention on the Rights of the Child* (November 20). https://zakon.rada.gov.ua/laws/show/995_021

[187] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657–670. https://doi.org/10.1177/1461444816686318

[188] Council of Europe. (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*. https://rm.coe.int

[189] Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On Education"* (№ 2145-VIII, September 5). https://zakon.rada.gov.ua/laws/show/2145-19

[190] Verkhovna Rada of Ukraine. (2001). *Law of Ukraine "On Child Protection"* (№ 2402-III, April 26). https://zakon.rada.gov.ua/laws/show/2402-14

In the context of digital safety, this Law enshrines a child's right to protection from all forms of violence, exploitation, and abuse, which may also occur in the digital environment.

However, it should be noted that the provisions of this Law do not provide sufficient detail regarding digital risks, so they need to be further developed.

The Law of Ukraine "On the Protection of Personal Data"[191] plays a key role in ensuring digital security, as it regulates matters relating to the collection, storage, and use of information about individuals. At educational institutions, this applies to the processing of pupils' data, the use of electronic registers, educational platforms, and other digital resources. The Law establishes requirements regarding the lawfulness of data processing, the protection of data against unauthorised access, and the obligation to obtain the consent of the subjects of personal data or their legal representatives.

At the same time, experience shows that a significant number of educational institutions use foreign digital platforms[192]; this creates additional risks regarding the transfer of personal data outside Ukraine. This issue requires clearer legal regulation and the introduction of uniform security standards for digital services used in the educational process.

Subordinate normative and legal acts, in particular the concepts and strategies for the digital transformation of education[193], are also of significant importance. They define the directions for the development of the digital educational environment; however, they are largely declaratory in nature and do not establish clear mechanisms for ensuring children's safety.

International legal regulation is a key component in the development of national legal frameworks. The foundational instrument is the UN Convention on the Rights of the Child[194], which enshrines the child's right to protection from all forms of violence, the right to privacy, and the right to access information. In the current context, these provisions also apply to the digital environment.

Furthermore, within the European legal framework, European Union legislation on the protection of personal data and digital rights, in particular the General Data Protection Regulation (GDPR)[195], has a significant influence. Its provisions set high

[191] Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection"* (№ 2297-VI, June 1). https://zakon.rada.gov.ua/laws/show/2297-17

[192] European Commission. (2021). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

[193] Cabinet of Ministers of Ukraine. (n.d.). *Strategy for the development of digital education in Ukraine*. https://www.kmu.gov.ua

[194] United Nations. (1989). *Convention on the Rights of the Child* (November 20). https://zakon.rada.gov.ua/laws/show/995_021

[195] European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu ; https://doi.org/10.2860/108933

standards for the processing of personal data, including specific safeguards for children, which can serve as a guideline for improving national legislation.

An analysis of the normative and legal provisions allows us to conclude that there are certain issues that undermine the effectiveness of legal mechanisms for ensuring the digital safety of children at educational institutions.

Firstly, there is a lack of coherence in the legal framework[196], as the provisions relating to digital safety are contained in various legislative acts and do not form a unified system.

Secondly, there is a lack of specific normative acts that comprehensively regulate the issue of children's digital safety within the educational environment.

Thirdly, there is an insufficient level of implementation of international standards into national legislation, particularly regarding the protection of children's personal data.

Fourthly, there are no clear requirements for digital platforms used in the educational process, creating risks of violations of children's rights.

Thus, the normative and legal framework for digital safety of children at educational institutions is characterised by the existence of basic guarantees, but requires further systematic improvement. It is necessary to develop a comprehensive approach to the legal regulation of the digital educational environment, taking into account contemporary challenges and ensuring the effective protection of children's rights.

3 Challenges and directions for improving legal mechanisms to ensure the digital safety of children at educational institutions

Despite the existence of a regulatory framework governing the protection of children's rights, digital safety at educational institutions remains insufficiently effective. This is due both to shortcomings in the legal framework and to difficulties in implementing the relevant mechanisms in practice.

One of the key issues is the fragmentation of legal regulation[197]. Provisions relating to children's digital safety are contained in various legislative acts and do not form a coherent system. The lack of a unified approach to regulating the digital educational environment complicates their application in practice and reduces the effectiveness of legal protection.

[196] OECD. (2021). *Children in the digital environment: Revised typology of risks*. OECD Publishing. https://www.oecd.org https://doi.org/10.1787/9c8c9c5d-en

[197] Ibid.

Another problem is the lack of a specialised normative act that would comprehensively define the legal mechanisms for ensuring children's digital safety at educational institutions. Existing normative acts only partially cover certain aspects of this issue, which makes it impossible to apply a systematic approach to resolving it.

Another significant shortcoming is the lack of regulation governing the use of digital platforms[198] in the educational process. Many educational institutions use commercial or foreign services without properly assessing their compliance with data protection requirements. This creates risks of unauthorised access to information about children, data leaks, or misuse.

A serious problem is the low level of digital literacy among those involved in the education system. Pupils, teachers, and parents often do not have sufficient knowledge of how to behave safely in the digital environment, which makes it difficult to prevent cyber threats and respond to them quickly.

Furthermore, there is a problem with the insufficient effectiveness of mechanisms for bringing offenders to justice for offences in the digital environment, particularly cyberbullying[199]. The difficulty of identifying offenders, as well as the specific nature of proving such offences, makes it difficult to prosecute those who are guilty.

Particular attention should be paid to the lack of adequate mechanisms for monitoring digital risks at educational institutions[200]. At present, such mechanisms are fragmented and do not provide for a systematic analysis of threats or their timely detection.

Under the current circumstances, special attention should be paid to the impact of martial law on protecting children's digital security at educational institutions. Military operations have significantly transformed the educational process, transferring a significant part of it to an online format, which, in turn, has greatly increased the educational environment's dependence on digital technologies. This transformation has led not only to expanded access to education but also to a sharp increase in cyber threats[201].

During the period of martial law, there has been an increase in information and psychological influence aimed at children and young people[202]. Disinformation, propaganda, and manipulative content can be disseminated via social media,

[198] European Commission. (2021). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

[199] Henson, B. (2012). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. *Security Journal, 25,* 88–89. https://doi.org/10.1057/sj.2011.25

[200] European Union Agency for Cybersecurity (ENISA). (2021). *Cybersecurity in education*. https://www.enisa.europa.eu

[201] Staksrud, E. (2013). *Children in the online world: Risk, regulation, rights.* Routledge. https://doi.org/10.4324/9781315887136

[202] UNICEF. (2021). *Policy guidance on AI for children*. https://www.unicef.org

messaging services, and educational platforms[203]. Children, as the most vulnerable group of digital users, often lack the critical thinking skills needed to recognise such threats, increasing the risk of being negatively affected[204].

Furthermore, under martial law, there is an increased risk of children's personal data being used for unlawful purposes. Cyberattacks on government and educational resources, data leaks, and unauthorised access to electronic systems may lead to a breach of a child's right to privacy and security[205]. In this context, the issue of strengthening the cybersecurity of educational institutions' information systems and introducing additional safeguards for the protection of personal data is of particular urgency[206].

Another important aspect is the need for normative regulation of the use of foreign digital platforms in the educational process[207]. In most cases, such platforms are subject to the jurisdiction of other countries, which makes it difficult to monitor the processing of personal data and ensure its protection[208]. The absence of clear requirements regarding their use creates legal uncertainty and increases the risks to children.

In the context of improving legal mechanisms, it is also worth noting the need for inter-agency coordination in ensuring children's digital safety[209]. For such a system to function effectively, cooperation is required among government bodies, educational institutions, law enforcement agencies, and international organisations[210]. Only a comprehensive approach will ensure an adequate level of protection for children's rights in the digital environment.

The implementation of institutional mechanisms for responding to digital incidents at educational institutions is also important. It is advisable to establish internal cybersecurity policies, appoint individuals responsible for information security, and develop protocols for dealing with

[203] OECD. (2021). *Children in the digital environment: Revised typology of risks*. OECD Publishing. https://www.oecd.org https://doi.org/10.1787/9c8c9c5d-en

[204] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657–670. https://doi.org/10.1177/1461444816686318

[205] European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu https://doi.org/10.2860/108933

[206] Ostroukhov, V. V. (Ed.), Prysiazhniuk, M. M., Farmahei, O. I., Chekhovska, M. M., et al. (2021). *Informatsiina bezpeka [Information security]*. Lira-K.

[207] European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu https://doi.org/10.2860/108933

[208] European Commission. (2021). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

[209] Cabinet of Ministers of Ukraine. (n.d.). *Strategy for the development of digital education in Ukraine*. https://www.kmu.gov.ua

[210] United Nations. (1989). *Convention on the Rights of the Child* (November 20). https://zakon.rada.gov.ua/laws/show/995_021

cyberthreats[211]. Such measures will help to improve the readiness of educational institutions to respond to contemporary challenges.

Consequently, the conditions of martial law complicate efforts to ensure children's digital safety, making it necessary to review existing legal mechanisms and adapt them to the new realities[212]. Considering these factors is essential for establishing an effective system to protect children's rights in the digital educational environment.

To enhance the effectiveness of legal mechanisms for ensuring children's digital safety, it is advisable to propose the following steps for their improvement.

Firstly, it is necessary to draft and adopt a special normative legal act that would comprehensively regulate issues relating to children's digital safety at educational institutions. Such an act should define the key concepts, principles, subjects, and mechanisms for ensuring digital safety.

Secondly, it is advisable to introduce uniform national digital security standards for educational institutions. These should include requirements regarding the use of digital platforms, the protection of personal data, cybersecurity, and incident response.

Thirdly, it is necessary to strengthen the legal regulation of the processing of children's personal data, in particular by establishing additional safeguards for their protection within the educational process. It is also important to introduce mandatory security assessments of digital services before their use by educational institutions.

Fourthly, the level of digital literacy among those involved in the education process should be improved. This can be achieved by introducing special educational programmes, training sessions, and courses on digital security for pupils and teachers.

Fifthly, it is advisable to improve the mechanisms for bringing offenders to justice in the digital environment, in particular by clarifying the elements of offences and simplifying the procedures for investigating them.

Sixthly, an important priority is the creation of an effective system for monitoring digital risks at educational institutions. Such a system should ensure the identification of threats, the analysis of their causes, and the development of measures to eliminate them.

Furthermore, it is necessary to provide for implementing international standards in the field of children's digital safety, which

[211] Kovaliv, M. V., Yesimov, S. S., Yarema, O. H. (2022). Informatsiine pravo Ukrainy : navchalnyi posibnyk [Information Law of Ukraine : a textbook]. Lvivskyi derzhavnyi universytet vnutrishnikh sprav.

[212] OECD. (2021). *Children in the digital environment: Revised typology of risks.* OECD Publishing. https://www.oecd.org https://doi.org/10.1787/9c8c9c5d-en

will contribute to the harmonisation of national legislation with European requirements[213].

Therefore, improving the legal mechanisms for ensuring children's digital safety at educational institutions requires a comprehensive approach, including both improving normative and legal regulation and enhancing the effectiveness of its practical implementation. Only under such conditions, it is possible to create a safe digital educational environment that meets contemporary challenges and ensures an adequate level of protection for children's rights.

Conclusions

The study has established that children's digital safety at educational institutions is an integral part of the overall system for safeguarding children's rights and creating a safe educational environment. Given the rapid digitalisation[214] and the increasing use of information and communication technologies in the learning process, the issue of protecting children in the digital environment is becoming particularly urgent[215].

It has been established that children's digital safety is a multifaceted concept comprising protection against socio-psychological, informational, technical, and legal threats. It is closely linked to the implementation of children's fundamental rights, in particular the right to privacy, safety, protection from violence, and access to a safe educational environment.

It has been proven that the current normative and legal provisions for digital safety of children in Ukraine are fragmented and do not form a coherent system of legal regulation. Despite the existence of basic legislative guarantees, the absence of a specialised normative act that would comprehensively regulate this area reduces the effectiveness of legal mechanisms.

It has been found that key problems include insufficient regulation of the use of digital platforms at educational institutions, the risks of children's personal data leaks, the low level of digital literacy among those involved in the educational process and the difficulty of bringing offenders to justice for offences committed in the digital environment.

[213] Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection"* (№ 2297-VI, June 1). https://zakon.rada.gov.ua/laws/show/2297-17

[214] European Commission. (2022). *A European strategy for a better internet for kids (BIK+).* https://digital-strategy.ec.europa.eu

[215] Council of Europe. (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment.* https://rm.coe.int

It has been confirmed that there is a need to improve the legal mechanisms for ensuring children's digital safety by adopting a comprehensive approach that combines regulatory, organisational and educational measures.

The following main directions for improvement have been outlined:

– drafting and adopting a specialised regulatory act in the field of children's digital safety;

– introducing uniform national standards for digital safety at educational institutions;

– strengthening the protection of children's personal data in the digital environment;

– raising the level of digital literacy among those involved in the educational process;

– improving mechanisms for liability for online offences;

– creating an effective system for monitoring digital risks.

It has been concluded that effective digital safety for children at educational institutions can only be ensured through systematic improvements to legislation, its alignment with international standards[216], and the proper practical implementation of the relevant legal mechanisms.

Summary

This study deals with the legal mechanisms for ensuring the digital safety of children at educational institutions. The current challenges related to the digitalisation of the educational process, in particular the risks of cyberbullying, personal data leakage, and the impact of harmful content, are analysed. National and international legislation concerning child rights protection in the digital environment is examined. The main issues in implementing legal mechanisms to ensure digital safety are identified. The need to improve normative and legal regulation is substantiated. Directions for enhancing the effectiveness of legal protection for children in the digital educational environment are proposed. A conclusion is drawn regarding the need for a comprehensive approach to ensuring digital safety of children at educational institutions.

References

1. Cabinet of Ministers of Ukraine. (n.d.). *Strategy for the development of digital education in Ukraine*. https://www.kmu.gov.ua

[216] ITU. (2020). *Guidelines for child online protection. International Telecommunication Union.* https://www.itu.int

2. Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. https://rm.coe.int
3. European Commission. (2021). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu
4. European Commission. (2022). A European strategy for a better internet for kids (BIK+). https://digital-strategy.ec.europa.eu
5. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu https://doi.org/10.2860/108933
6. European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity in education. https://www.enisa.europa.eu
7. Henson, B. (2012). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. *Security Journal, 25*, 88–89. https://doi.org/10.1057/sj.2011.25
8. ITU. (2020). Guidelines for child online protection. International Telecommunication Union. https://www.itu.int
9. Kovaliv, M. V., Yesimov, S. S., Yarema, O. H. (2022). *Informatsiine pravo Ukrainy : navchalnyi posibnyk [Information Law of Ukraine : a textbook]*. Lvivskyi derzhavnyi universytet vnutrishnikh sprav.
10. Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*(6), 22–30. https://doi.org/10.1016/j.jadohealth.2007.08.017
11. Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications*, 39(3), 283–303. https://doi.org/10.1515/commun-2014-0113
12. Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657–670. https://doi.org/10.1177/1461444816686318
13. OECD. (2021). *Children in the digital environment: Revised typology of risks*. OECD Publishing. https://www.oecd.org https://doi.org/10.1787/9c8c9c5d-en
14. Ostroukhov, V. V. (Ed.), Prysiazhniuk, M. M., Farmahei, O. I., Chekhovska, M. M., et al. (2021). *Informatsiina bezpeka [Information security]*. Lira-K.
15. Staksrud, E. (2013). *Children in the online world: Risk, regulation, rights*. Routledge. https://doi.org/10.4324/9781315887136
16. UNICEF. (2017). The State of the World's Children 2017: Children in a Digital World. https://www.unicef.org
17. UNICEF. (2021). *Policy guidance on AI for children*. https://www.unicef.org
18. United Nations. (1989). *Convention on the Rights of the Child* (November 20). https://zakon.rada.gov.ua/laws/show/995_021

19. Verkhovna Rada of Ukraine. (1996). *Constitution of Ukraine* (Law No. 254k/96-VR, June 28). https://zakon.rada.gov.ua/laws/show/254k/96-vr
20. Verkhovna Rada of Ukraine. (2001). *Law of Ukraine "On Child Protection"* (№ 2402-III, April 26). https://zakon.rada.gov.ua/laws/show/2402-14
21. Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection"* (№ 2297-VI, June 1). https://zakon.rada.gov.ua/laws/show/2297-17
22. Verkhovna Rada of Ukraine. (2017). *Law of Ukraine "On Education"* (№ 2145-VIII, September 5). https://zakon.rada.gov.ua/laws/show/2145-19