STATE POLICY OF CHILD PROTECTION IN CYBERSPACE AS A PRIORITY OF HUMAN SECURITY: A RETROSPECTIVE OF FORMATION

Dymytriieva Oksana Ihorivna [1]

Received: 2024-09-01
Accepted: 2024-10-02
DOI: https://doi.org/10.5281/zenodo.17012172

Annotation. The article is devoted to researching the retrospective of the formation of state policy for the protection of children in cyberspace as a key component of Ukraine's humanitarian security. The author proceeds from the assumption that it is the humanitarian paradigm that allows us to see the long-term socio-psychological consequences of digital threats and to form proactive management decisions capable of ensuring a safe digital childhood in a situation of war, mass migration and saturation of the information space with manipulative content.

The author examines the international legal and European standards that have formed the methodological framework of contemporary policy: the UN Convention on the Rights of the Child with General Comment No. 25, the Lanzarote and Budapest Conventions, and the BIK+ Strategy, which enshrines the principle of 'safety by default' and combines preventive, educational and restorative mechanisms. It shows how the evolution of these documents has shifted the focus from combating child pornography to comprehensive protection of personal data, algorithmic discrimination and digital well-being.

National dynamics are analysed: from isolated campaigns in the early 2000s to the integrated system established by the Law 'On the Basic Principles of Ensuring Cybersecurity' and the Cybersecurity Strategy 2021. Achievements are highlighted - the creation of a cyber police force, the launch of the Safer Internet UA platform, school courses on cyber hygiene, and a network of CERT units - and challenges are identified, such as lack of funding, fragmentation of services, and delays in the adoption of a special law on the protection of children online.

The experience of Germany, France, the Netherlands, Lithuania, and the United Kingdom has been summarised, confirming the advantages of models with an independent regulator, age verification, and algorithm auditing. Guidelines for Ukraine have been formulated: codification of the 'digital childhood' doctrine, launch of a strong regulator, development of a psychological support network, use of artificial intelligence for early risk detection, and introduction of clear performance indicators that will allow for flexible policy adjustments in line with technological changes.

Keywords: public policy, public administration, human security, national security, protection of children's interests, combating domestic violence, criminal enforcement, cybersecurity, cyberspace.

[1] researcher at the National University of Civil Defence of Ukraine, Kharkiv,
ORCID ID: 0009-0005-2776-5999
E-mail: oidimitr5@gmail.com

Relevance of the research topic

In the context of military aggression and the forced transition of a significant part of the school process to an online format, the digital space has actually become the main socialisation environment for Ukrainian children, where both educational opportunities and multiple risks are concentrated. According to UNICEF, more than 80 per cent of 15- to 16-year-olds spend between two and seven hours on social media every day, which correlates with an increase in cases of cyberbullying, sexual harassment and online recruitment in the period 2022-2024. The National Strategy for the Protection of Children in the Digital Environment until 2025 explicitly points to a wide range of threats - from grooming to the involvement of minors in extremist networks and the commercial exploitation of personal data - emphasising the need for state coordination of efforts between law enforcement, educational and social institutions.

The relevance of the topic is further enhanced by the European trend towards the introduction of mandatory "safety by default"standards, as reflected in the BIK+ Strategy (2022), as well as the emergence of the draft law "On the Protection of Children in the Digital Environment"in Ukraine, which provides for age verification and fines for offending platforms. Given that human security determines the priority of state policy in times of war, the formation of a holistic, cross-sectoral system for the protection of digital childhood is not only a requirement of international obligations, but also a critical factor in preserving the mental health and social potential of the future generation.

Analysis of recent research and publications

The current academic discourse on child protection in cyberspace is determined by a reorientation from a narrow criminal law field to an interdisciplinary study of humanitarian risks, which is confirmed by the works of Smahel, Livingstone and Mascheroni, who substantiate the need for a comprehensive "protect-empower"approach. Studies by UNICEF and Innocenti have shown that in countries with a military or crisis situation, digital threats to minors increase in proportion to online time and lack of psychosocial support, which is especially relevant for Ukraine. European think tanks Brookings and EU Kids Online in their 2024-2025 reviews emphasise the effectiveness of independent regulators and algorithmic audit of platforms, while researchers Taylor and Sprague highlight the importance of age verification as a safeguard against grooming and manipulative targeting. In Ukrainian scholarship, the topic is most consistently developed by Gulich, Dubovyk, and Potiy, who analyse the national specifics of implementing the requirements of the BIK+ Strategy and the problem of institutional fragmentation. Together, these publications demonstrate a gradual shift from reactive punitive practices to a proactive humanitarian policy that integrates legal, technical, social and educational tools.

The purpose of the study is to systematically analyse the evolution of the state policy of child protection in cyberspace through the prism of human security, to identify its key stages and factors, and to formulate scientifically based directions for further institutional and regulatory modernisation.

The main content of the study.

In the humanitarian paradigm, child safety is not seen as a side dimension of national defence capability, but as an autonomous value that requires the state to guarantee conditions for the comprehensive development of minors, including safe access to the digital environment. The normative axis of this approach is set by the UN Convention on the Rights of the Child, as specified in General Comment 25, which emphasises that any public policy in the field of digital technologies must "respect, protect and fulfil"the rights of the child regardless of the platform or business model, and therefore combine preventive, educational and regulatory mechanisms [1]. This threefold logic formed the basis of the European BIK+ Strategy (2022), which puts forward the criterion of "safety by default"and at the same time

guides states to develop digital competence and the active participation of children themselves in shaping safe online spaces, making the document a key methodological reference point for EU candidate countries.

The expansion of digital threats to a transnational scale has highlighted the need for specialised criminal law instruments. The Lanzarote Convention of the Council of Europe (2007) was the first international treaty to criminalise sexual abuse of children using information and communication technologies and imposes a positive obligation on states to ensure the removal of illegal content and support for victims. At the same time, the Budapest Convention on Cybercrime (2001) proposed a procedural framework for extradition and joint investigations, and its Additional Protocol focused on countering the dissemination of sexual exploitation of minors on the darknet, which currently accounts for up to a third of all requests for mutual assistance from European law enforcement agencies [2]. The synergy of these two conventions forms the basic legal framework within which national strategies combine administrative, criminal and socio-pedagogical measures.

Methodologically, the study relies on an interdisciplinary analysis that combines comparative jurisprudence, security policy and human rights theory to reconstruct the evolution of international and European standards and then extrapolate them to the Ukrainian context. A comprehensive study of the texts of conventions, policy documents, and academic works allows us to trace the transformation of emphasis - from the isolated regulation of "child pornography"in the 2000s to the modern concept of protecting digital childhood, which includes issues of data commercialisation, algorithmic discrimination, and psychological well-being [3]. Such a historical and legal "cut"allows us to clearly outline the factors that determined the transition from purely punitive to comprehensive policies and to prepare the ground for the analysis of national practice in the following sections.

The first stage of development of Ukraine's online child protection policy dates back to the early 2000s, when the Internet was just beginning to move beyond the computer labs of Kyiv's lyceums. The state responded mainly with educational initiatives: electives on the basics of safe online work and individual information campaigns such as "Children Online", implemented jointly with private providers under the auspices of the Ministry of Education and Science. The programmes lacked consistency, and the issue of cyber threats remained outside the regulatory framework, limited to the general provisions of the Law on Childhood Protection. At the same time, Ukraine's accession to the global Safer Internet Day movement in 2008 launched a regular public dialogue on safe digital environments, which led to the first methodological guides for teachers and parents. In 2013, the Ministry of Education and Science approved the concept of introducing media literacy into the educational process, but did not provide any real financial support, so the programme remained a one-off [4]. The year 2015 was a turning point, when, in response to the growth of cyberbullying in schools, a government hotline on child safety on the Internet was launched, and a separate cyberpolice unit was created under the Ministry of Internal Affairs, which was given the competence to investigate crimes against the sexual freedom of minors in the virtual environment. Despite this, the lack of an integrated strategy and specific legislation left prevention and awareness-raising efforts fragmented, and the mechanisms for removing prohibited content uncoordinated between providers, law enforcement and educational institutions.

The second phase began with the adoption of the Law on the Basic Principles of Ensuring Cybersecurity of Ukraine in 2017, which for the first time defined child protection as a component of national security. The document mobilised interagency cooperation: The National Commission for the Protection of Children's Rights was given a mandate to regulate secure Internet access, and the National Coordination Centre for Cybersecurity was given a strategic planning function to protect vulnerable groups. In 2018, the Ukrainian Safer Internet Centre was opened under the Osvitoria NGO and with the support of the European Commission, which launched an online complaint platform and the Stop Sexting educational

module. The State Digital Literacy Programme "Diia.Digital Education"(2020) provided an additional impetus, creating a course for parents and teachers called "Online Safety for Children". The culmination was the Cybersecurity Strategy 2021, which for the first time set out the task of developing a special law on the protection of children in the digital environment, introducing mandatory cyber hygiene programmes in schools, and deploying a network of CERT units responsible for incidents involving minors. At the same time, educational institutions have begun to introduce content filtering and monitoring systems for undesirable web resources, which are partially funded by subventions from the Ministry of Digital Transformation [5]. Despite the significant progress, the military aggression of 2022 brought new risks to light: a sharp increase in online time, the shift of learning to digital platforms, and the spread of disinformation campaigns aimed at minors. In response, in 2023, the government stepped up work on a draft law that would provide for age verification, mandatory parental control, and fines for services that do not remove harmful content, and engaged industry associations in developing a safe design code. Given the declared course of European integration, the national system is gradually moving from fragmented measures to a comprehensive model where legal, technical and educational components should interact in an integrated manner to ensure humanitarian resilience in the digital age.

The current stage is characterised by a rapidly increasing complexity of the risk models that were in place at the beginning of the decade: distance learning, triggered by the pandemic and military circumstances, has unprecedentedly increased the time children spend online, while equating social media, gaming platforms and video hosting with offline environments in terms of influence. Basic threats such as cyberbullying, grooming, dangerous flash mobs, sexting, and identity theft have been complemented by highly targeted manipulative campaigns aimed at emotional exhaustion or radicalisation of adolescents. The proliferation of artificial intelligence tools has led to the generation of "deepfake"content with strong sexual overtones, which can cause psychological trauma even without physical contact between the perpetrator and the victim [6]. The economic dimension of the problem is also growing: massive leadership platforms collect detailed digital profiles of minors to accurately target advertising or sell game content, which calls into question the child's right to privacy. At the same time, the lack of digital literacy among parents and educators, the limited number of school psychologists with special training, and weak preventive mechanisms in educational institutions create an environment of increased vulnerability, where the negative effects of cyber incidents are exacerbated by socio-economic shocks associated with war and internal displacement.

Against this backdrop, a special law "On the Protection of Children in the Digital Environment"is in its final stages of development, which should institutionalise the comprehensive "protect, empower, respect"model by integrating it into Ukraine's legal system. The draft law proposes three key mechanisms: mandatory age verification on digital platforms, the introduction of the "safety by default"principle for services targeting minors, and increased administrative liability for providers for inadequate protection of children's content. Importantly, the draft law provides for the creation of an independent regulator with the authority to promptly block resources with illegal materials and impose fines, as well as the launch of a state register of malicious domains with automatic synchronisation across telecom operators' networks [7]. At the same time, the Ministry of Education is developing a module on mandatory cyber hygiene in the school curriculum, the Ministry of Digital Transformation is developing technical requirements for parental control systems, and the cyber police are preparing special investigative units to respond quickly to cases of online exploitation. However, the effectiveness of the reform will directly depend on the state's ability to ensure adequate funding for age verification infrastructure, synchronisation of the regulator's powers with law enforcement and judicial systems, and coordination with technology companies to implement safe design. Successful completion of this stage will be a

qualitative transition from a fragmented, mostly reactive policy to a proactive humanitarian strategy that can not only minimise current threats but also proactively build the principles of ethical and safe use of technology by children into the country's digital ecosystem.

A comparative overview of European practices shows that the countries that were the first to recognise digital childhood safety as a strategic priority moved towards integrating legal, technical and educational tools within a single protection-development policy. In Germany, the introduction of accredited age verification systems is combined with the obligation of design-by-default platforms to block algorithmic recommendations of content that could harm underage users; France has focused on criminalising digital grooming and holding providers liable for high fines; and the Netherlands has moved online child protection centres to a public-private partnership model, where tech giants co-fund cloud infrastructure to automatically detect sexual exploitation material [8]. The common denominator of these approaches is the creation of independent regulators with the power to quickly block resources and impose significant financial sanctions, allocation of budgets for digital education for teachers and psychologists, and annual audit reports on the accessibility and safety design of children's content.

Within the post-Soviet space, the closest to a comprehensive model is Lithuania, which has combined school cyber hygiene classes with an institutional network of "trust centres"where specially trained professionals provide psychological assistance to victims of cyberbullying and advise parents on setting up parental controls. Intersectoral coordination has proved to be a key success factor: law enforcement, educators, social welfare agencies, and private telecommunications companies work in a single digital intranet, which allows them to remove or block harmful content within hours and simultaneously launch rehabilitation procedures for children [9]. The experience of the United Kingdom, where the Online Safety Act delegates to the media regulator Ofcom the function of checking recommended content algorithms, clearly proves that an independent supervisory body with technological expertise can effectively balance freedom of speech and protection of vulnerable groups, while stimulating innovation in the field of safe design.

For Ukraine, adopting these practices involves several strategic steps. First, the codification of a comprehensive doctrine of "digital childhood"in a special law should be complemented by detailed bylaws on safety by default and auditing-by-design to minimise regulatory gaps. Second, the creation of an independent regulator with a mandate for laboratory audits of algorithms and a flexible tariff mechanism for fines will increase the responsibility of platforms and encourage them to self-regulate. Thirdly, the state should invest in a nationwide network of psychological support services with a focus on cyber incidents, combining them with digital literacy education centres to form a sustainable prevention and response ecosystem [10]. Finally, building an early warning loop based on CERT-UA, which will use machine learning technologies to proactively detect risk patterns in the children's segment of the network, can provide the speed and accuracy needed in the face of hybrid information threats.

Conclusions and prospects for further research

The analysis has shown that the state policy of child protection in cyberspace in Ukraine has evolved from isolated educational initiatives to an awareness of the complex humanitarian nature of the problem, but is still at the stage of institutional consolidation. It is critical to move to a proactive model that combines a special law with default security principles, the creation of an independent regulator with technological expertise, the development of a national monitoring and rapid response system (in close cooperation with CERT-UA and cyber police), and an integrated psychosocial support network for children and parents. Harmonisation with the European BIK+ framework, the introduction of algorithmic auditing and age verification standards, supported by stable funding for digital education of

teachers and school psychologists, should form the basis for long-term humanitarian resilience.

Prospects for further research include the development of verifiable indicators of policy effectiveness (impact and outcome metrics), empirical assessment of the impact of algorithmic recommendations and commercialisation of children's data, audit of age verification systems from the perspective of human rights and non-discrimination, and study of the psychological consequences of new forms of violence, including deepfake exploitation. Particular attention should be paid to long-term (longitudinal) studies of groups of increased vulnerability - children of internally displaced persons, military personnel, bereaved families - to properly target interventions; analysis of court practice regarding the liability of platforms and providers; modelling the optimal architecture of an independent regulator; and the development of ethical protocols for the use of artificial intelligence in early risk detection.

List of references

1. European Commission.European Strategy for a Better Internet for Kids (BIK+). Brussels:European Commission, 2022. 36 c. URL: https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.
2. Council of Europe.Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Strasbourg: CoE, 2007.28 c. URL: https://rm.coe.int/1680084822.
3. European Parliament.The new European strategy for a better internet for kids (BIK+): Briefing 733663. Luxembourg:Publications Office of the EU, 2022. 12 c. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733663/EPRS_BRI(2022)733663_EN.pdf (accessed on:).
4. Better Internet for Kids.Safer Internet Day in Ukraine focused on the local level.Brussels:European Schoolnet, 2024. URL: https://better-internet-for-kids.europa.eu/en/news/safer-internet-day-ukraine-focussed-local-level.
5. Verkhovna Rada of Ukraine.Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"No. 2163-VIII of 05.10.2017. Kyiv: VRU, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
6. UNICEF Ukraine.Situation Analysis of Children in Ukraine 2024. Kyiv: UNICEF, 2024. 24 c. URL : https://www.unicef.org/ukraine/en/media/49211/file/UNICEF_SitAn_Summary_2024_ENG.pdf.
7. Ministry of Digital Transformation of Ukraine.Protection of children in the digital environment: recommendations for public authorities. Kyiv: Ministry of Digital Transformation of Ukraine, 2023. 40 c. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/COP-Guidelines_for_Policy_Makers_UA.pdf.
8. Taylor Wessing.Germany's approach to protecting minors online after JuSchG amendments 2021 [Analytical report]. Berlin: Taylor Wessing, 2025. URL: https://www.taylorwessing.com/en/interface/2025/online-safety-update/germanys-approach-to-protecting-minors-online.
9. Financial Times.Tech giants' age verification tools put to the test as UK Online Safety Act rules kick in. London: Financial Times, 24.07.2025. URL: https://www.ft.com/content/dca34551-4828-4677-9a72-ac8966a380cd
10. Davydiuk O.; Potii V..National Cybersecurity Governance: Ukraine. Tallinn: NATO CCDCOE, 2024. 60 c. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf.