PROTECTION OF CHILDREN'S SUBJECTIVE RIGHTS TO PERSONAL DATA IN THE DIGITAL AGE: ADMINISTRATIVE AND LEGAL FOUNDATIONS AND SOCIO-CULTURAL CONTEXT

Iryna Ihnatchenko[1]
Yaroslava Ryabchenko[2]

DOI: https://doi.org/10.30525/978-9934-26-631-7-20

Abstract. This study provides an in-depth and comprehensive analysis of the administrative and legal foundations for protecting children's subjective rights to personal data in the rapidly developing digital age. The research explores the essence of a child's right to privacy through the lens of key international legal instruments, including the UN Convention on the Rights of the Child, General Comment No. 25 of the UN Committee on the Rights of the Child, and the EU General Data Protection Regulation (GDPR), as well as their reflection in Ukrainian national legislation.

Purpose. The paper aims to examine the administrative–legal and socio-cultural aspects of protecting children's subjective rights to personal data in the digital era. It identifies the main problems linked to the collection, storage, processing and dissemination of minors' personal data and proposes theoretical and practical approaches to improving protection mechanisms, including under martial law in Ukraine.

Methodology. The study applies the normative–legal method combined with a legislative approach consistent with the research goal. Qualitative content analysis is used to identify, interpret and evaluate legal provisions and determine their relevance to the protection of children's personal data in digital environments. The analytical model involves a systematic examination of legal norms to identify key principles and

[1] Candidate of Legal Sciences, Candidate of Art Studies,
Associate Professor of the Department of Administrative Law,
Yaroslav Mudryi National Law University, Ukraine
[2] Candidate of Legal Sciences,
Associate Professor of the Department of Administrative Law,
Yaroslav Mudryi National Law University, Ukraine

compare international and national approaches from the standpoint of administrative law.

Results. The findings highlight that the total digitalisation of society creates unprecedented opportunities for children's education, socialisation and development but also entails underestimated risks associated with the unlawful processing and commercial exploitation of children's data and unauthorised interference with minors' privacy. The research identifies educational technology (EdTech) platforms as particularly risky, as they often perform large-scale profiling of minors without adequate parental consent or effective state oversight. The paper substantiates the urgent need for effective mechanisms of public and governmental supervision in the sphere of children's data circulation and for introducing administrative liability for abuse.

Practical implications. The authors propose concrete measures for improving national digital policy in protecting children's rights: adopting a dedicated law on the digital rights of the child, establishing a Digital Ombudsman institution, strengthening control over digital service providers, and implementing wide digital-literacy programmes for parents and educators.

Value/originality. The originality of this study lies in its integrated administrative-legal and socio-cultural approach to the protection of children's data privacy in both national and international contexts. The work stresses the need for cross-sectoral cooperation, the consistent implementation of international standards, and the cultivation of digital responsibility. The study offers specific mechanisms to balance innovation and the protection of children's fundamental rights in the modern digital world, thus contributing to the formation of Ukraine's national policy in this field.

1. Introduction

The rapid development of information and communication technologies (ICTs) has opened unprecedented opportunities for children to explore their rights, receive education, and engage in social interaction. Yet it has also created significant challenges for the protection of minors' privacy and personal data (hereinafter PD). According to Ukraine's Ministry of Digital Transformation, more than 67% of children aged 9–17 have regular

Internet access, with nearly 45% using social media without parental control. Seventeen percent of children have encountered cyberbullying, while 28% have been exposed to unwanted content or communication with strangers [1].

The expanding digital space produces potential risks – commercial exploitation of children's data, invasion of privacy, dissemination of harmful content and automated profiling. Particularly hazardous are educational platforms (EdTech) that collect analytical data without clear explanations of processing terms. Consequently, there are serious challenges to ensuring children's ability to form safe social connections and exercise their subjective rights, particularly the right to the protection of personal data. The latter has evolved from an ethical to a legal issue directly related to human rights – specifically the child's right to privacy guaranteed by both national law and international instruments.

As noted by the Ukrainian Parliament Commissioner for Human Rights, the national system for protecting children's rights in Ukraine often faces internal coordination problems, especially between central and local levels. Three key central executive bodies play an essential role: the Ministry of Social Policy, the National Social Service, and the State Service for Children's Affairs. Despite their shared aim – ensuring the rights and interests of children – these institutions experience duplication of functions, poor coordination, and inadequate interaction [2, p. 104].

The issue's urgency is compounded by the transboundary nature of the digital environment, which complicates the enforcement of effective protection measures. One critical factor remains the lack of specialised international and national regulatory frameworks, strategic plans, adequate resources – including financial ones – and institutional capacity needed for the comprehensive protection of children's rights online. Thus, the development and implementation of an inclusive, multidimensional strategy for safeguarding children's subjective rights in the digital sphere is required. Such a strategy must include effective and targeted measures, backed by sufficient staffing and funding. Only a coordinated, cross-sectoral approach involving a wide range of stakeholders can ensure adequate protection for children and young people and create conditions for empowering them – forming a foundation for their full development in a digitalised society.

Hence, this research contributes to a deeper understanding of challenges and possible solutions necessary to protect children from privacy breaches. It also promotes the creation of stricter regulations and raises public awareness of the importance of safeguarding children's privacy in the digital age.

Studies dedicated to issues of information security have been conducted by many domestic and foreign scholars, such as J. M. Balkin, V. Bohush, L. Brown, Z. Brzezinski, A. Zhovnir, N. Wiener, H. Kissinger, N. Karr, V. Lipkan, V. Muntiyan, M. Palmer, H. Pocheptsov, J. Stein, T. Thomas, J. Thunders, H. French, K. Hambly, B. Schneier, and others.

In particular, some of them addressed the use of personal data and possible legal consequences related to its processing, including problems with the application of artificial intelligence (hereinafter – AI) in the educational sphere in accordance with the requirements of domestic legislation and EU law (GDPR, White Paper on AI): M. Bielova, Yu. Zhornokui, O. Zozulia, V. Machuskyi, D. Orziantseva, V. Piddubna, O. Punda, O. Ruban, D. Sadovska, V. Titova, V. Tkachenko, B. Shcherbina, Shch. Yavor, O. Yavorska, O. Yatsenko, and others.

Problems related to the functions and principles of administrative and legal regulation in the era of the digital economy interested scholars such as M. Babik, O. Vinnik, T. Yehorova-Lutsenko, V. Dobrovolskyi, A. Krakovska, and others.

Scholars such as I. Boiko, Yu. Mekh, O. Solovyova, V. Syomina, Ya. Riabchenko, O. Chervyakova, T. Slinko dedicated their works to the study of subjective human rights, and also analyzed the principle of the rule of law and its components [3; 4; 5]. Another group of scholars, including Yu. Mekh, Yu. Heorhiyevskyi, I. Ihnatchenko, I. Maslova, I. Kostenko, I. Verkhovod, R. Oleksenko, O. Ratsul, N. Kushnir, and others, focused their attention on the development of public-private partnership in various fields of public administration in crisis situations in Ukraine, as well as explored the role of social communications, including digital ones, in the development of the social sphere [5; 6; 7].

Despite the significant contribution of previous researchers, the growing interest of digital platforms in personalized information indicates that the protection of children's digital privacy remains both a priority of state policy and a subject for further scientific consideration. This study

is intended to provide a comprehensive understanding of the challenges and potential solutions necessary to ensure the protection of children from violations of the right to privacy in the digital environment. Furthermore, the work aims to stimulate the improvement of legal regulation and raise public awareness of the importance of protecting children's personal data (PD) in the information society.

2. Genesis of Personal Data Protection Views

In Silicon Valley, there is a well-known saying: “Data is the new oil of the 21st century.” This expression, attributed to British mathematician and data scientist Clive Humby, was coined in 2006 when he remarked: “Data is the new oil. It’s valuable, but if unrefined, it cannot really be used. It must be broken down, analysed, and turned into something useful.” [8].

This idea underscores the increasing importance of fostering “digital hygiene” among children – beginning as early as preschool age [9]. Every child should understand that, as J. Tunders observed, much like oil, for those who recognise the fundamental value of data and master its extraction and utilisation, immense opportunities arise. We live in an era of the digital economy, where data has acquired unprecedented value. It is a cornerstone of modern society’s continuous functioning [10].

If big data is indeed the “new oil,” then questions about its “life” and “death” become serious technological, social, and epistemological challenges. J. M. Balkin aptly points out that algorithmic development and artificial intelligence are the driving forces behind these challenges, for the “algorithmic society” relies on vast datasets that can be cheaply and easily collected, organised, and analysed. The digital age enables this because digital communication inherently produces, replicates, and transmits data. Increasingly, human expressions and actions leave digital traces that can be gathered, copied, systematised, and analysed [11] – and, crucially, used against an individual, particularly a child.

As Bruce Schneier aptly put it: “You can’t make digital files uncopyable, any more than you can make water not wet.” [12]. This statement reflects the very essence of digital information and reveals the limitations of purely technological protection measures. Within the context of children’s data protection, Schneier’s observation gains special importance: even if children’s data are safeguarded by state-of-the-art security or access

restrictions, they remain inherently vulnerable to duplication or leakage due to flaws in storage or transmission systems.

Therefore, effective protection cannot rely solely on technical measures. A comprehensive approach is required – one that integrates legal mechanisms, organisational safeguards, and educational initiatives targeting all participants in the digital ecosystem who interact with children's data.

Schneier's thesis emphasises the need for realism in protecting children's personal data: since absolute data inaccessibility is impossible, effective strategies must consider actual threats and technological limitations.

In conclusion, the modern protection of children's personal data in the digital era must rest on the integration of technological, legal, and educational measures that maintain a balance between security, privacy, and a child's personal development within the information society. Such a comprehensive approach promotes digital responsibility, enhances awareness among all participants of the digital environment, and creates conditions for safe and meaningful data use without losing the benefits of technological innovation.

3. The National Digital Ecosystem (NDE) and the Protection of Children's Personal Data

In the digital age, personal data have become a new type of resource. Every person, including every child, forms part of a vast national digital ecosystem (NDE) – a term first introduced by N. Carr with respect to IT technologies [13]. Although not yet formally defined in Ukrainian law or academic tradition, the concept is widely used in national and international digital transformation strategies.

These include:

(1) Strategic documents of the Cabinet of Ministers of Ukraine and the Ministry of Digital Transformation [14; 15];

(2) Reports of international organisations such as the OECD [16], the World Bank, UNDP, and the International Telecommunication Union (ITU), which employ the term in their analyses of national digital development;

(3) National digitalisation strategies of countries like Estonia, Singapore, Indonesia, and the UAE.

Within this research, the NDE is understood as a complex socio-technical system comprising:

(1) digital infrastructure (communication networks, computing power, electronic service platforms);

(2) legal frameworks (including specific data protection acts);

(3) institutional architecture (government agencies, regulators, and independent supervisory authorities);

(4) digital users (citizens, businesses, educational institutions, and minors).

These components interact to ensure children's safety, privacy, and rights in the digital environment.

The NDE thus serves as the foundation for national policy on protecting children's rights in the digital domain, ensuring effective regulation of data processing, oversight of digital platforms (especially EdTech), and the implementation of privacy-by-design and digital inclusion principles. Building such an ecosystem requires inter-agency cooperation, transparent governance, cybersecurity, parental and child digital literacy, and accountability among digital service providers.

The rapid growth of digital technologies offers new opportunities for children's learning, communication, and self-expression, while simultaneously generating significant security and privacy risks. Digital and cyber hygiene encompass behavioural, technical, and educational measures designed to protect children from online harms, minimise risks, and ensure their well-being in the networked environment.

Effective child cyber hygiene in the NDE requires a multi-level approach:

1. Technical dimension – secure platforms, data encryption, access control, and regular software updates.

2. Educational dimension – critical thinking, risk awareness, and responsible data behavior.

3. Legal and organisational dimension – legislation for data protection, oversight institutions, and monitoring of digital safety.

Children's cyber hygiene includes:

– Technical hygiene: managing accounts and devices, using strong unique passwords, updating software, avoiding malware, and understanding privacy settings;

– Behavioural hygiene (digital ethics): responsible data sharing, recognising and countering cyberbullying, verifying information, and preventing fake content dissemination;

– Emotional–psychological hygiene: balancing screen time, maintaining mental health, preventing digital addiction, and rejecting harmful content.

Special attention must be paid to children's interactions with digital services at both national and commercial levels, where vast datasets are accumulated, analysed, and reused. Thus, children's cyber hygiene becomes part of state policy on creating a safe digital environment rather than merely an individual practice.

The child's vulnerability within the NDE is heightened by specific online threats that transcend traditional cybercrime, including grooming, phishing, social engineering, harmful content exposure, malware, insecure networks, fraudulent websites, and account hijacking. These risks often lead to data breaches or the uncontrolled disclosure of information about a child's identity, location, school, or parents' financial details through unsecured educational or gaming platforms.

To address these issues, it is imperative to integrate digital and cyber hygiene into formal and informal education systems. This requires:

(a) Standardised programmes – embedding cybersecurity and digital ethics modules into curricula from primary school;

(b) Teacher training – educators must be prepared not only technically but psychologically to guide children's digital conduct;

(c) Parent–school–state partnerships – joint educational and accountability initiatives fostering children's "digital immunity."

In summary, fostering sustainable digital and cyber hygiene among children is a strategic imperative for national security and child rights protection in the context of the NDE. Solving this challenge demands interdisciplinary collaboration and investment in educational and technological safeguards.

4. International Standards for the Protection of Children's Privacy and Cybersecurity

At the global level, the principal approaches to safeguarding children in the digital space are enshrined in a series of international legal instruments, including:

1. The Universal Declaration of Human Rights (1948) [17].
2. The UN Convention on the Rights of the Child (1989) [18].

3. General Comment No. 25 of the UN Committee on the Rights of the Child on children's rights in the digital environment (2021) [19].

4. The General Data Protection Regulation (GDPR) of the European Union (2016) [20].

Article 12 of the Universal Declaration of Human Rights provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [17].

This provision, echoed in the Law of Ukraine on Personal Data Protection [21], represents a cornerstone of human rights protection.

UNICEF's Policy Guidance on AI for Children (2021) [22] emphasises that the protection of children and youth is a shared responsibility among state regulators, digital industry actors, parents, educators and all other stakeholders. They must ensure a sustainable environment in which children can fully realise their potential both online and offline. The digital space should embed safety-by-design principles that empower children and secure their rights.

The UN Convention on the Rights of the Child (1989) [18] recognises children as a particularly vulnerable group and reaffirms their fundamental rights: protection from exploitation, the right to privacy, freedom of expression and participation in public life.

General Comment No. 25 (2021) [19] extends these guarantees to the digital environment and stresses that all rights must be applied in accordance with a child's evolving capacities. Digital technologies and platforms may not limit children's privacy, data protection, freedom of expression or access to information. States and digital-service providers are obliged to ensure safe and responsible use of technology, taking into account minors' vulnerability.

Particular attention is paid to children's personal data. The Comment requires that the collection, storage and processing of children's information comply with the principles of lawfulness, data minimisation, transparency and protection from unauthorised access. It also stresses the need to balance access to digital opportunities with adequate protection.

The GDPR [20] establishes unified rules for collecting, processing, storing and protecting personal data across the EU, ensuring individuals' rights to privacy and control. Article 8 of the Regulation specifies:

– a child is defined as an individual under 16 years old (Member States may lower this to 13);

– online services aimed at children require verifiable parental consent;

– privacy notices must be concise and age-appropriate;

– processing children's data is considered high-risk, requiring enhanced safeguards and encryption.

Collectively, these documents show that while data-driven innovation brings social and economic benefits, it also necessitates pragmatic state policy that maximises benefits and minimises threats to data subjects. Such policy should rest on the principles of:

(a) Human-centricity, (b) Inclusivity, (c) Accountability, (d) Transparency, (e) Robustness, and (f) Privacy & Security.

Current priorities for regulating relations within the national digital ecosystem include:

1. Defining guiding principles for governance in the digital environment.

2. Determining responsible authorities for "digital control" and "digital security".

3. Establishing mechanisms for sustainable digital infrastructure development.

4. Setting standards for data availability, confidentiality, and integrity.

5. Creating a framework for the ethical use of digital technologies and services.

In Ukraine, the Law on Digital Content and Digital Services (No. 3321-IX of 10 August 2023) [23] represents a first step toward implementing these principles.

Thus, international standards collectively form a human-centred foundation for protecting children's rights amid global digitalisation. They affirm that fundamental rights – including privacy and data protection – extend to online life, requiring transparency, accountability and built-in security by design.

5. Legal Regulation of the Protection of Children's Personal Data in Ukraine

Article 32 of the Constitution of Ukraine guarantees the right to privacy and the protection of personal and family life [24]. Ukraine currently has a number of legislative acts regulating the protection of children's personal

data and their safety in the digital environment. Although there is still no dedicated law that exclusively governs the protection of children's digital personal data, the existing legal framework provides several important guarantees. In the national context, a set of legal acts directly or indirectly regulate the protection of children's personal data (PD). These include the following laws of Ukraine:

(1) On Personal Data Protection [21];

(2) On the Protection of Childhood [25];

(3) On Education [26];

(4) On the Basic Principles of Ensuring Cybersecurity in Ukraine [27];

(5) On Electronic Trust Services [28];

(6) The Code of Ukraine on Administrative Offences (CUAO) [29]; and

(7) The Criminal Code of Ukraine (CCU) [30].

(1) The Law of Ukraine "On Personal Data Protection" [21] establishes the main principles for processing, storing, and protecting personal information, including children's data. However, it lacks special provisions specifically addressing minors. By contrast, the draft Law of Ukraine "On Personal Data Protection" No. 8153 of 25 October 2022 (currently under revision in the Verkhovna Rada as of September 2025, included in the agenda by Resolution No. 4586-IX of 3 September 2025) aims to harmonise Ukrainian legislation with the GDPR. The draft strengthens the role of the Parliament Commissioner for Human Rights in the sphere of digital rights, expanding its powers to monitor parental or legal-guardian consent for processing children's personal data and to ensure their right to access, rectify, or erase such data [31].

(2) The Law of Ukraine "On the Protection of Childhood" is the core legislative act concerning children's rights protection. It:

(a) guarantees protection of the child from all forms of violence, exploitation, intimidation, and discrimination;

(b) explicitly provides the right of the child to privacy and to personal and family secrecy (Article 10); and

(c) imposes duties on parents or guardians, as well as on state and local authorities, to safeguard the child's personal rights, including those to personal data [25].

(3) The Law of Ukraine "On Education" contains provisions on students' digital safety but does not specifically elaborate on personal-data protection in the digital environment [26].

(4) The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" indirectly concerns the protection of children's personal data, especially in cases of cyberattacks. It:

(a) aims to protect the national information space, including children's data;

(b) defines the rights and obligations of cybersecurity entities;

(c) explicitly stresses the need to safeguard personal data in cyberspace; and

(d) recommends that public authorities take measures to prevent data leaks [27].

(5) The Law of Ukraine "On Electronic Trust Services":

(a) regulates the protection of electronic information, particularly during identification and authentication of individuals;

(b) ensures secure transmission and storage of digital data;

(c) guarantees the confidentiality and integrity of electronic information; and

(d) provides mechanisms to protect children's digital rights through electronic services [29].

(6) The Code of Ukraine on Administrative Offences establishes administrative liability for violations of personal-data legislation, including Article 188-39, which concerns the unlawful processing of personal data [29].

(7) The Criminal Code of Ukraine defines criminal liability for breaches of privacy and misuse of personal data, including:

(a) unlawful collection, storage, use, or dissemination of confidential information about an individual (Article 182 CCU); and

(b) the distribution of child pornography (Article 301-1) [30].

Some provisions on the protection of personal data are also contained in strategic and conceptual policy documents (or their drafts), such as:

(1) the Digital Strategy of Ukraine for 2021–2030 [14]; and

(2) the National Strategy for the Protection of Children in the Digital Environment for 2021–2026 [15].

The Digital Strategy of Ukraine for 2021–2030 [14] sets out objectives for creating a unified digital-education platform and forming a national digital ecosystem; however, it insufficiently addresses children's data security. The National Strategy for the Protection of Children in the Digital

Environment for 2021–2026 [15], by contrast, focuses on building a safe online space for minors, fostering cooperation among parents, educators, and IT specialists, and promoting initiatives that enhance children's and youth's digital literacy.

Therefore, it must be acknowledged that Ukraine currently lacks a specific legislative act comprehensively regulating the protection of children's personal data. This gap underscores the need for a dedicated normative document aligned with the provisions of the GDPR and the forthcoming European AI Act.

6. National Frameworks for Children's AI Safety

International organisations – the United Nations, the Council of Europe and the European Union – attach particular importance to the ethical and safe use of artificial intelligence (AI). The central idea behind these initiatives is the human-centric development of technology: digital solutions must serve human welfare rather than replace human will or autonomy. The widespread introduction of AI, automated decision-making and profiling systems significantly transforms traditional privacy safeguards, requiring new legal standards to ensure that the best interests of the child remain paramount.

At the EU level, these principles were formalised in the White Paper on Artificial Intelligence: A European Approach to Excellence and Trust (2020) [32], which underpins the forthcoming EU AI Act. It articulates the principles of trust, safety and respect for fundamental rights, identifying children as a particularly vulnerable category requiring stronger legal protection. The European Commission proposed key safeguards, including:

1. Limiting automated profiling of minors.
2. Banning manipulative algorithms targeting children's behavior.
3. Ensuring transparency of algorithms that process children's data; and
4. Prioritising human-centric AI in education, health and entertainment.

Ukraine has begun to integrate similar principles through national strategic documents, most notably the White Paper on Artificial Intelligence in Ukraine (2023) [33], prepared with the support of USAID and UK Dev. Though not a binding legal act, this policy paper outlines a roadmap for aligning national regulation with EU standards. It highlights the need for

ethical oversight, risk assessment mechanisms for minors and transparency in algorithmic systems, particularly within education.

The Ministry of Digital Transformation of Ukraine has also developed sector-specific guidelines, including:

1. Methodological Recommendations for the Introduction and Use of AI Technologies in Secondary Education (2024) [34]; and

2. Human Rights in the Age of Artificial Intelligence: Challenges and Legal Regulation (2024) [35].

The first document stresses the principles of confidentiality and security, requiring educational institutions to verify compliance with personal-data legislation, inform parents and obtain parental consent for processing students' data. It also recommends internal AI-use policies, attention to privacy statements of external AI tools, and prohibiting teachers and students from entering confidential information into AI systems without authorisation.

The second document [34] outlines broader human-rights guarantees:

– recognising children's heightened vulnerability;

– mandating parental consent for data processing;

– requiring transparency and accessible information on data handling;

– introducing effective remedies for rights violations;

– recommending the adoption of clear privacy policies, educational campaigns for parents and children, and cooperation between authorities and civil society.

Between 2026 and 2027, Ukraine plans to draft a Law on Artificial Intelligence, serving as a national analogue to the EU AI Act. In preparation, several policy documents have already been adopted: the Concept for AI Development in Ukraine [36], the Action Plan for its Implementation [37] and the AI Regulatory Roadmap [38]. These emphasise the need for adequate legal regulation of AI in education and cybersecurity and the protection of personal data.

Additionally, the Concept of Digital Hygiene for Preschool Children [39] defines digital hygiene as a system of knowledge and skills ensuring safe, healthy and ethical technology use by children during learning, play and communication. It seeks to protect children's mental, physical and informational well-being, foster resilience to manipulation and harmful content, and harmonise traditional and digital forms of learning.

In summary, Ukraine's evolving AI governance framework reflects a gradual shift towards a human-centred and child-sensitive digital policy aligned with European standards. Digital hygiene education and ethical AI regulation are key instruments for safeguarding children's personal data and psychological welfare in the information society.

7. Ukraine's Child Digital Rights Governance

Ukraine's public-administration system for safeguarding children's subjective rights – including personal data protection – is multilayered, encompassing both general and specialised institutions. The principal state bodies with mandates in this domain include:

1. The Ukrainian Parliament Commissioner for Human Rights (Ombudsman) – exercises parliamentary oversight of constitutional rights and freedoms, including privacy and data protection. The Ombudsman reviews citizen complaints, conducts inspections of data controllers, and issues recommendations to eliminate violations [40].

2. The National Police of Ukraine – investigates cybercrimes and unlawful collection, use or dissemination of personal data, including data relating to minors [41].

3. The Ministry of Education and Science of Ukraine (MoES) – develops policies for digital literacy, cybersecurity education and ethical technology use in schools [43].

4. The Ministry of Digital Transformation of Ukraine (MinDigital) – formulates national policy on digitalisation, artificial intelligence and cybersecurity, including regulations on personal data use in educational and technological services [43].

5. The Ministry of Social Policy and the State Service for Children's Affairs – coordinate child-protection policy, including responses to information-security violations or misuse of children's data [44; 45].

6. Regional and Local Child-Protection Services – operate under regional and municipal administrations, implementing national policies at the community level and intervening when a child's data or privacy are compromised [46; 47; 48].

At the local level, child-protection services handle tasks such as monitoring online abuse, coordinating with educational institutions and

law-enforcement bodies, and raising community awareness about safe digital behaviour.

Despite this institutional diversity, fragmentation persists. Responsibilities often overlap, and coordination mechanisms remain weak. Therefore, an integrated administrative architecture is required – one that unites governmental, educational, social and technological actors in a coherent system of digital child-rights governance.

Such an architecture should rest on four pillars:

1. Legality and accountability – clear delineation of institutional powers and transparent oversight mechanisms.

2. Inter-agency coordination – joint information platforms and shared databases between ministries and regulators.

3. Digital literacy and capacity building – continuous training for officials, educators and parents.

4. Monitoring and evaluation – regular assessment of digital-safety policies and incident response mechanisms.

Creating a Digital Ombudsman for Children could become a crucial innovation. This specialised office would focus exclusively on minors' digital rights, bridging the gap between families, schools and the state and ensuring compliance with GDPR-aligned standards.

8. Institutionalizing Data Protection for "Children of War"

In the context of the ongoing armed aggression of the Russian Federation against Ukraine, the issue of protecting the rights of children living in temporarily occupied territories has become particularly acute. The occupying authorities systematically resort to enforced disappearances, forced deportations, militarisation, and ideological "re-education" of children, aiming to reshape their national identity.

According to the National Portal "Children of War", between 22 February 2022 and 24 October 2025, Ukrainian state agencies, in cooperation with civil-society organisations and international partners, succeeded in returning 1,713 of 19,546 deported and/or forcibly displaced children from the territory of the Russian Federation and the temporarily occupied areas of Ukraine [49]. These figures illustrate the scale of the problem and the urgent need for a systematic state policy ensuring both legal and digital protection of these children.

Instances of forced displacement are accompanied by the unlawful collection, transfer, and use of children's personal information – including biographical, medical, educational, and social data. Such data are often employed to create databases of individual profiles, to monitor children's locations, and to facilitate their further assimilation into the aggressor state's socio-political environment. This practice violates fundamental principles of international law that guarantee the preservation of personal identity, respect for privacy, and the prohibition of any form of child abduction or trafficking. It also contravenes key international instruments on the protection of minors' personal data, notably the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) [50] and the principles outlined in General Comment No. 25 of the UN Committee on the Rights of the Child (2021) [19].

Within Ukraine's national legal framework, these issues are regulated by the Law of Ukraine "On Personal Data Protection" [21] and a number of related legislative acts analysed earlier. However, under martial law and conditions of occupation, these mechanisms are insufficient to ensure effective protection of children's rights, especially against the unlawful use of their personal data by occupation authorities.

The protection of children's personal data requires a systematic solution through the creation of a Commissioner for the Protection of Children's Personal Rights – a specialised, independent body authorised to monitor, respond to, and coordinate state policy in the sphere of minors' digital rights. The key responsibilities of such an institution should include:

1. Supervising compliance with children's privacy rights in the digital environment.

2. Developing state standards for secure processing of personal data in educational, healthcare, and social institutions.

3. Cooperating with international organisations such as UNICEF, the International Organization for Migration (IOM), and the Council of Europe on the return and reintegration of deported children.

4. Shaping national digital-security policy and implementing educational programmes for parents, teachers, civil servants, and local-government officials.

The protection of children's personal data constitutes an integral component of ensuring their fundamental rights and freedoms. During war and occupation, this issue gains strategic importance, as interference with a child's digital identity becomes a tool of information-psychological manipulation and erasure of national self-awareness.

The creation of the Commissioner for the Protection of Children's Personal Rights would strengthen the state system for safeguarding minors' rights, improve responsiveness to digital threats, and promote international cooperation in protecting Ukrainian children. This would mark an important step toward affirming the humanistic and legal foundations of Ukraine's digital sovereignty.

Thus, the introduction of a Digital Ombudsman institution and the development of a comprehensive state policy on children's digital rights are strategic directions for building a safe, lawful, and ethically balanced digital space in Ukraine.

7. Conclusions

The challenge of digital transformation lies in managing the paradox: unlocking educational opportunities while mitigating intensified risks like privacy violations and personal-data abuse. The proposed strategy for Ukraine is a comprehensive, multi-pillar effort anchored by legal, technical, and educational initiatives.

(1) Foundational Pillars of Protection

Effective protection of children's rights in the digital sphere must be built upon two core, internationally recognized principles, serving as the benchmark for regulatory evolution (e.g., aligning with GDPR standards).

a) Legal and Ethical Grounding:

– Protection must be based on Lawfulness and Proportionality. Data processing must adhere strictly to established legal bases, be necessary, and be proportionate to a legitimate purpose. Over-collection and unnecessary data retention must be eliminated.

– The core principle is Human-Centrism (Child-Centric Design), meaning that the best interests of the child must mandate that all digital services, applications, and legal standards are designed by default to prioritize the young user's safety, privacy, and well-being.

b) Technological Integration and Systemic Safeguards:

– The National Digital Ecosystem must integrate child-specific safeguards beyond general data protection, acting as a protector rather than a vulnerability.

– This is crucial in:

- EdTech Applications: Enforcing strict measures to prevent the profiling of students for commercial or behavioral purposes.

- Artificial Intelligence (AI): Mandating AI ethics and audit standards to ensure transparency and prevent algorithmic discrimination in services impacting a child's educational path or opportunities.

- The digital environment must be shielded from Commercial Exploitation, with clear prohibitions on targeted advertising based on personal data collected from children.

(2) Strategic Measures and Institutional Coordination

Legal and technological frameworks require activation through dedicated educational efforts and an interconnected governance structure to ensure enforcement and prevent policy gaps.

a) Education and Awareness (The Cross-Cutting Component):

– Digital literacy and hygiene must be woven into formal and informal learning to build a collective culture of cyber-resilience.

– For Children: The curriculum must teach practical digital hygiene, including privacy settings, recognizing scams, and managing their digital footprint.

– For Parents: Awareness programs must equip them to supervise digital activity, understand privacy implications, and provide informed consent.

– For Teachers: Educators require specific training to integrate digital tools safely and serve as frontline mentors on responsible online behavior.

b) Multi-Institutional Coordination for Coherent Governance:

– Protecting digital rights demands a unified front linking policy, technology, and enforcement to ensure rapid, effective responses.

- The coordination model must link:

- The Ombudsman (Human Rights Commissioner): For independent oversight and redress.

- MinDigital (Ministry of Digital Transformation): Ensuring privacy-by-design in digital infrastructure.

– MoES (Ministry of Education and Science): Integrating digital safety into the national education system.

- Law Enforcement: Addressing serious cybercrimes and data breaches.
- Local Child-Protection Services: Providing ground-level support and intervention.

(3) Legislative Reform and Independent Oversight

To solidify this comprehensive strategy, dedicated legislative and institutional changes are imperative to ensure accountability and long-term advocacy for children's digital interests.

a) Legislative Reform: Ukraine should adopt a Special Law on the Digital Rights of the Child to explicitly define and protect rights (like digital access, identity, and the right to be forgotten) beyond general data protection law.

b) Independent Oversight: The Establishment of a Digital Ombudsman or a child-focused digital rights commission is crucial. This independent body would have the mandate and resources to audit digital services, enforce compliance, and advocate for children's interests against both state and private actors.

In essence, the strategy requires a human-centred, interdisciplinary approach that delicately balances innovation with security, and transforms the digital environment from a potential threat into a catalyst for children's full and safe development.

References:

1. Ministry of Digital Transformation of Ukraine. (2024). *Results of digital transformation in the regions of Ukraine for 2023*. URL: https://www.kmu.gov.ua/news/rezultaty-tsyfrovoi-transformatsii-v-rehionakh-ukrainy-za-2023-rik

2. Verkhovna Rada of Ukraine Commissioner for Human Rights. (2024). *Annual report on the state of observance and protection of human and civil rights and freedoms in Ukraine in 2024*. URL: https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/Щорічна_доповідь_Уповноваженого_у_2024_році.pdf

3. Boiko, I. V., Mekh, Y. V., Soloviova, O. M., Somina, V. A., & Cherviakova, O. B. (2020). Universal human rights and state sovereignty. *International Journal of Criminology and Sociology*, (9), 3014–3022. https://doi.org/10.6000/1929-4409.2020.09.367

4. Slinko, T. (2022). The rule of law principle in the legal positions of the Constitutional Court of Ukraine. *Access to Justice in Eastern Europe*, *5*(1(13)), 165–177.

5. Ihnatchenko, I. H., & Riabchenko, Ya. S. (2024). *Teoretychni ta pravovi aspekty motyvatsii do viiskovoi sluzhby cherez pryzmu zakhystu sub'iektyvnykh prav liudyny* [Theoretical and legal aspects of motivation for military service

through the prism of protecting subjective human rights]. In *Theoretical and Applied Foundations of Innovation in Modern Science: Scientific Multidisciplinary Monograph* (pp. 6–12). International Center for Science and Social Transformation (isst.co.ua). URL: https://drive.google.com/file/d/1v6Gh5ZAPLJ698jR8KEfHa-FyAdyES-

6. Mekh, Y., Georgiievskyi, I., Ignatchenko, I., Maslova, I., & Kostenko, I. (2021). Public-Private Partnership in the Security Sector: Updating in the Conditions of Counteracting the COVID-19 and Armed Aggression in Eastern Ukraine. *Revista de la Universidad del Zulia*, *13*(37), 347–361. URL: https://www.academia.edu/80865781/Public_Private_Partnership_in_the_Security_Sector_Updating_in_the_Conditions_of_Counteracting_the_COVID_19_and_Armed_Aggression_in_Eastern_Ukraine

7. Verkhovod, I., Oleksenko, R., Ratsul, O., Kushnir, N., & Ihnatchenko, I. (2023). Social Communications and Their Role in the Development of the Social Sphere. *Review of Economics and Finance*, *21*(1), 836–843. URL: https://refpress.org/ref-vol21-a91/

8. Humby, C., & Palmer, M. (2006, November 3). Data Is the New Oil. *ANA Marketing Maestros*. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

9. Cabinet of Ministers of Ukraine. (2025, May 2). *Rozporiadzhennia No. 432-r, Pro skhvalennia Kontseptsii tsyfrovoi hihiieny ditei doshkilnoho viku* [Resolution No. 432-r, On Approval of the Concept of Digital Hygiene for Preschool Children]. Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/432-2025-p#Text

10. Toonders, J. (2014, July). Data Is the New Oil of the Digital Economy. *Wired*. URL: https://www.wired.com/insights/2014/07/data-is-the-new-oil-of-the-digital-economy/

11. Balkin, J. M. (2018). *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation* (Yale Law School, Public Law Research Paper No. 615). SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939

12. Schneier, B. (2001, May 15). The Futility of Digital Copy Prevention. *Crypto-Gram Newsletter*. URL: http://www.counterpane.com/crypto-gram-0105.html#3

13. Carr, N. (2010). *The shallows: What the internet is doing to our brains*. W. W. Norton & Company. URL: https://wwnorton.com/books/9780393357820

14. Cabinet of Ministers of Ukraine. (2024, December 31). *Rozporiadzhennia No. 1351-r, Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025–2027 rokakh* [Resolution No. 1351-r, On Approval of the Strategy for Digital Development of Innovation Activity of Ukraine for the period up to 2030 and approval of the operational plan for its implementation in 2025–2027]. Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/go/1351-2024-%D1%80

15. Ministry of Digital Transformation of Ukraine. (2020). *Natsionalna stratehiia z zakhystu ditei v tsyfrovomu seredovyshch na 2021–2026 roky* [National

Strategy for the Protection of Children in the Digital Environment for 2021–2026]. URL: https://thedigital.gov.ua/documents/legislation/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomu-seredovishchi-na-2021-2026-roki

16. OECD. (2021). *Development Co-operation Report 2021: Shaping a Just Digital Transformation*. OECD Publishing. https://www.oecd-ilibrary.org/development/development-co-operation-report-2021_e

17. United Nations. (1948, December 10). *Universal Declaration of Human Rights* (U.N. General Assembly Resolution 217 A (III)). URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights

18. United Nations. (1989, November 20). *Convention on the Rights of the Child* (U.N. General Assembly Resolution 44/25). UNICEF. URL: https://www.unicef.org/child-rights-convention/convention-text

19. Committee on the Rights of the Child. (2021, March 2). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (U.N. Document No. CRC/C/GC/25). United Nations. URL: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

20. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

21. Verkhovna Rada of Ukraine. (2010). *Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI* [On Personal Data Protection: Law of Ukraine No. 2297-VI]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

22. UNICEF. (2021). *Policy guidance on AI for children*. United Nations Children's Fund (UNICEF). URL: https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children

23. Verkhovna Rada of Ukraine. (2023). *Pro tsyfrovi kontent ta tsyfrovi posluhy: Zakon Ukrainy vid 10.08.2023 No. 3321-IX* [On Digital Content and Digital Services: Law of Ukraine No. 3321-IX]. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text

24. Verkhovna Rada of Ukraine. (1996). *Konstytutsiia Ukrainy: Zakon Ukrainy vid 28.06.1996 No. 254k/96-VR* [Constitution of Ukraine: Law of Ukraine No. 254k/96-VR]. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

25. Verkhovna Rada of Ukraine. (2001). *Pro okhoronu dytynstva: Zakon Ukrainy vid 26.04.2001 No. 2402-III* [On Childhood Protection: Law of Ukraine No. 2402-III]. URL: https://zakon.rada.gov.ua/laws/show/2402-14

26. Verkhovna Rada of Ukraine. (2017). *Pro osvitu: Zakon Ukrainy vid 05.09.2017 No. 2145-VIII* [On Education: Law of Ukraine No. 2145-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2145-19

27. Verkhovna Rada of Ukraine. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 No. 2163-VIII* [On the Main Principles of Cybersecurity Assurance in Ukraine: Law of Ukraine No. 2163-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2163-19

28. Verkhovna Rada of Ukraine. (2017). *Pro elektronni dovirchi posluhy: Zakon Ukrainy vid 05.10.2017 No. 2155-VIII* [On Electronic Trust Services: Law of Ukraine No. 2155-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2155-19

29. Verkhovna Rada of the Ukrainian SSR. (1984). *Kodeks Ukrainy pro administratyvni pravoporushennia (KUAP)* [Code of Ukraine on Administrative Offenses]. URL: https://zakon.rada.gov.ua/laws/show/80731-10

30. Verkhovna Rada of Ukraine. (2001). *Kryminalnyi kodeks Ukrainy (KKU)* [Criminal Code of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/2341-14

31. Verkhovna Rada of Ukraine. (2022). *Pro zakhyst personalnykh danykh: Proiekt Zakonu No. 8153 vid 25.10.2022 r.* [On Personal Data Protection: Draft Law No. 8153]. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

32. European Commission. (2020). *White Paper on Artificial Intelligence – A European approach to excellence and trust* (COM(2020) 65 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065

33. Ministry of Digital Transformation of Ukraine. (2023). *Bila knyha z pytan rozvytku shtuchnoho intelektu v Ukraini* [White Paper on the Development of Artificial Intelligence in Ukraine]. Ministry of Digital Transformation of Ukraine. URL: https://thedigital.gov.ua/projects/ai-white-paper-ukraine

34. Ministry of Digital Transformation of Ukraine, & Ministry of Education and Science of Ukraine. (2024). *Instruktyvno-metodychni rekomendatsii shchodo zaprovadzhennia ta vykorystannia shtuchnoho intelektu v zakladakh serednoi osvity* [Instructional and Methodological Recommendations on the Implementation and Use of Artificial Intelligence in Secondary Education Institutions]. URL: https://storage.thedigital.gov.ua/files/f/9f/960585ee1e964dc6f50ed3492f66a9fb.pdf

35. EU4DigitalUA, Office of the Ombudsman, & Ministry of Digital Transformation of Ukraine. (2024). *Prava liudyny v epokhu shtuchnoho intelektu: vyklyky i rekomendatsii* [Human Rights in the Era of Artificial Intelligence: Challenges and Recommendations]. URL: https://drive.google.com/file/d/1YLb1X8wCMQi3g8LjPsERa2b58GM1fRS2/view

36. Cabinet of Ministers of Ukraine. (2020, December 2). *Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia No. 1556-r* [On Approval of the Concept for the Development of Artificial Intelligence in Ukraine: Resolution No. 1556-r]. Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

37. Cabinet of Ministers of Ukraine. (2021, May 12). *Pro zatverdzhennia planu zakhodiv z realizatsii Kontseptsii rozvytku shtuchnoho intelektu v Ukraini na 2021-2024 roky: Rozporiadzhennia No. 438-r* [On Approval of the Action Plan for the Implementation of the Concept for the Development of Artificial Intelligence in Ukraine for 2021-2024: Resolution No. 438-r]. Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/438-2021-p#Text

38. Ministry of Digital Transformation of Ukraine. (2023). *Dorozhnia karta z rehuliuvannia shtuchnoho intelektu v Ukraini: Bottom-Up Pidkhid* [Roadmap for the Regulation of Artificial Intelligence in Ukraine: Bottom-Up Approach]. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf

39. Cabinet of Ministers of Ukraine. (2025, May 2). *Pro skhvalennia Kontseptsii tsyfrovoi hihiieny ditei doshkilnoho viku: Rozporiadzhennia No. 432-r* [On Approval of the Concept of Digital Hygiene for Preschool Children: Resolution No. 432-r]. Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/432-2025-p#Text

40. Verkhovna Rada of Ukraine. (1997). *Pro Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny: Zakon Ukrainy vid 23.12.1997 No. 776/97-VR* [On the Verkhovna Rada of Ukraine Commissioner for Human Rights: Law of Ukraine No. 776/97-VR]. URL: https://zakon.rada.gov.ua/laws/show/776/97-вр#Text

41. Verkhovna Rada of Ukraine. (2015). *Pro Natsionalnu politsiiu: Zakon Ukrainy vid 02.07.2015 No. 580-VIII* [On National Police: Law of Ukraine No. 580-VIII]. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

42. Cabinet of Ministers of Ukraine. (2014). *Pro zatverdzhennia Polozhennia pro Ministerstvo osvity i nauky Ukrainy: Postanova No. 630 vid 16.10.2014 r.* [On Approval of the Regulation on the Ministry of Education and Science of Ukraine: Resolution No. 630]. URL: https://zakon.rada.gov.ua/laws/show/630-2014-п#Text

43. Cabinet of Ministers of Ukraine. (2019). *Pytannia Ministerstva tsyfrovoi transformatsii: Postanova No. 856 vid 18.09.2019 r.* [Issues of the Ministry of Digital Transformation: Resolution No. 856]. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text

44. Cabinet of Ministers of Ukraine. (2025). *Pytannia Ministerstva sotsialnoi polityky simi ta yednosti Ukrainy: Postanova No. 904-p* [Issues of the Ministry of Social Policy, Family, and Unity of Ukraine: Resolution No. 904-p]. URL: https://zakon.rada.gov.ua/laws/show/904-2025-п#Text

45. Cabinet of Ministers of Ukraine. (2023). *Pytannia Derzhavnoi sluzhby Ukrainy u spravakh ditei: Postanova No. 1048-p* [Issues of the State Service of Ukraine for Children's Affairs: Resolution No. 1048-p]. URL: https://zakon.rada.gov.ua/laws/show/1048-2023-п#Text

46. Cabinet of Ministers of Ukraine. (2007). *Pro zatverdzhennia typovykh polozhen pro sluzhbu u spravakh ditei: Postanova No. 1068 vid 17.10.2007 r.* [On Approval of Standard Regulations on the Service for Children's Affairs: Resolution No. 1068]. URL: https://zakon.rada.gov.ua/laws/show/1068-2007-п#n13

47. Ministry of Social Policy of Ukraine. (2021). *Pro zatverdzhennia prymirnykh polozhen pro sluzhbu u spravakh ditei: Nakaz No. 533 vid 03.11.2021 r.* [On Approval of Standard Regulations on the Service for Children's Affairs: Order No. 533]. URL: https://zakon.rada.gov.ua/laws/show/z1383-21#Text

48. Verkhovna Rada of Ukraine. (1997). *Pro mistseve samovriaduvannia v Ukraini: Zakon Ukrainy vid 21.05.1997 No. 280/97-VR* [On Local Self-Government in Ukraine: Law of Ukraine No. 280/97-VR]. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр#Text

49. National Portal "Children of War". (n.d.). *Dity viiny 24 liutoho 2022 – 24 zhovtnia 2025* [Children of War February 24, 2022 – October 24, 2025]. URL: https://childrenofwar.gov.ua/?utm_source=https://www.google.com/search?q=chatgpt.com

50. Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108). URL: https://rm.coe.int/1680078b37