THE RIGHT TO PROTECTION OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT: NATIONAL AND INTERNATIONAL ASPECTS

Serhii Budarnyi,
Postgraduate student at West
Ukrainian National University
ORCID:
E-mail: Sbudarnui@gmail.com

Abstract. The article is devoted to a comprehensive analysis of the right to personal data protection in the digital environment, taking into account national and international legal standards, which is particularly relevant in the context of intensive digitalization, the growing influence of online platforms, and the spread of artificial intelligence technologies. The paper highlights the theoretical foundations and evolution of the institution of privacy and identifies the key principles of personal data processing, including legality, proportionality, purpose limitation, minimization, accuracy, and transparency. It analyzes Ukrainian legislation in the field of data protection, outlines its gaps, and assesses its compliance with international regulations. Particular attention is paid to the risks arising from the use of big data, AI algorithms, automated profiling, and the activities of global digital platforms, which pose new challenges to privacy and information security. The article formulates recommendations for improving the national personal data protection system and further aligning Ukrainian legislation with European standards.

Key words: personal data, digital environment, privacy, information technology, legislation, personal information protection.

INTRODUCTION

In the current context of digital transformation of society, the issue of ensuring the right to personal data protection is becoming particularly important. The intensive expansion of digital infrastructure, including the use of cloud services, mobile applications, artificial intelligence technologies, and big data, leads to a significant increase in the amount of information collected, processed, and stored in the private and public sectors. This dynamism contributes to the improvement of management processes, the development of e-commerce, and the improvement of public services, creating new opportunities for information processing, but at the same time generating increased risks to privacy, in particular those related to unauthorized access, mass data leaks, algorithmic profiling, transnational transfers, and commercial use of personal information.

Personal data has become a strategic resource used for both commercial purposes and public administration. However, its uncontrolled dissemination, lack of adequate security guarantees, use of algorithmic analysis and automated decision-making without users understanding the consequences of such processes lead to an increase in threats to fundamental rights and freedoms. The most common problems include massive data leaks, abuse of digital surveillance technologies, profiling without proper legal grounds, and transnational transfers of information without sufficient safeguards.

In Ukraine, despite the existence of basic legislation in the field of personal data protection, numerous problems arise in practice because it does not correspond to the realities of the digital age. It is not sufficiently adapted to the requirements of the digital economy and European Union standards. In the context of Ukraine's European integration course, the harmonization of national regulations with the provisions of the GDPR, which establish a high level of transparency, accountability, and legal protection for data subjects, is particularly relevant.

Ukraine's European integration course and the need to harmonize legislation with European Union law are placing new demands on the modernization of the regulatory framework. In view of this, there is a need to rethink approaches to ensuring the rights of personal data subjects, in particular with regard to the right of access, rectification, restriction of processing, data portability, objection to automated decision-making, and the right to be forgotten. In national law enforcement practice, the relevant instruments are implemented in a fragmented manner or remain declarative.

The international dimension of the problem is further complicated by the fact that the movement of information in the global digital space knows no borders, and therefore the effective protection of the rights of individuals requires coordinated intergovernmental mechanisms, common standards, and proper implementation of international legal obligations. At the same time, both international and national approaches often demonstrate gaps in addressing the latest challenges related to artificial intelligence, digital identification, and cybersecurity.

The international aspect of the problem is due to the transnational nature of digital communications. Personal data is often processed outside the jurisdiction of the subject's country of citizenship, which complicates the mechanisms for its protection and requires international cooperation and unification of approaches.

The use of innovative technologies such as artificial intelligence, facial recognition, biometric systems, and automated law enforcement solutions raises additional ethical and legal questions. Algorithmic data processing often lacks transparency, making it impossible to assess its impact on privacy and potentially leading to discriminatory or biased results.

Thus, the combination of factors – from technological to legal – points to the need for thorough scientific research into the right to personal data protection in the digital environment. It is essential to determine the scope and content of this right, analyze the state of national and international regulation, identify existing gaps and

contradictions, and propose directions for reforming Ukrainian legislation, taking into account European standards and global trends in information technology development.

It is precisely the need for a comprehensive study of these aspects that determines the relevance of the chosen topic and defines its practical and theoretical significance.

The issue of personal data protection in the digital environment is the subject of active scientific discourse in both Ukrainian and international legal doctrine, but the development of digital technologies is constantly transforming its content and bringing new aspects to the fore. In Ukrainian doctrine, the nature of personal data, the mechanisms for its processing, and legal guarantees have been studied by O. opylenko, I. Aristova, O. okhanovskaya, and I. Gorodnenko, who focused on the conceptual definition of the right to privacy and its application to digital information flows. Scientists emphasize the growing role of information security as a component of national security, which necessitates the creation of an effective mechanism for the protection of personal data. The works of foreign scientists focus on assessing the impact of global digital platforms, Big Data, and artificial intelligence on the protection of personal information. The works of H. Baker, . Bennett, and M. Brunnen shape the modern view of the risks of digital interaction. At the same time, a number of authors, including P. Gustavo and E. Seligman, analyze the challenges of transnational data transfers and issues of jurisdictional responsibility. Despite the availability of a significant body of scientific literature, comprehensive research on the right to personal data protection in the context of the modern challenges of the digital environment, including analysis of technological risks, international standards, and the state of national legislation, remains underdeveloped. Existing works mostly focus on individual practical or conceptual aspects, which necessitates a more systematic scientific approach.

The purpose of the study is to provide an in-depth scientific and legal understanding of the state and prospects of the development of mechanisms for ensuring the right to personal data protection in the digital environment, taking into account international standards, technological trends, and the peculiarities of the Ukrainian legal space. The fulfillment of these objectives creates the basis for forming a holistic vision of the mechanisms for ensuring the right to personal data protection in the digital age and determining the optimal model for its implementation in Ukraine.

RESEARCH METHODOLOGY

The methodological basis of the study is a set of general scientific and special legal methods, the use of which ensured a comprehensive analysis of the mechanism for ensuring the right to personal data protection in the digital environment.

The dialectical method allowed us to consider the right to personal data protection in connection with the dynamics of digital transformations, the development of information technologies, and changes in social communications.

The systemic-structural method was used to determine the interaction between national and international norms, institutional control mechanisms, and technical and ethical components of privacy protection, which made it possible to form a comprehensive model of legal regulation.

The formal-legal method was used to analyze the provisions of Ukrainian national legislation, in particular the Law "On the Protection of Personal Data" and subordinate acts, as well as to compare them with European Union standards and GDPR norms.

The comparative legal method made it possible to study international approaches to personal data protection, including the practices of the EU, the Council of Europe, and individual states, to identify differences, gaps, and opportunities for implementing effective models into domestic legislation.

The analysis and synthesis method was used to assess current technological risks—algorithmic profiling, digital identification, Big Data processing, transnational data transfers, etc.

The sociological approach is based on the use of survey results on the level of digital literacy of citizens, which made it possible to take into account the practical aspect of the problem.

The comprehensive combination of these methods ensured the scientific validity of the conclusions and formed a complete picture of the legal, technological, and institutional mechanisms for protecting personal data in the digital environment.

The scientific novelty of the study lies in the systematic scientific and legal understanding of the mechanisms for ensuring the right to personal data protection in the digital environment, combining the analysis of national and international approaches, taking into account modern technological transformations. The author has developed a comprehensive concept for studying the legal protection of personal data in the digital age, which allows for a comprehensive assessment of the current state of the problem, identification of technological and legal risks, and proposal of effective ways to improve national legislation.

RESULTS

The right to protect personal data in the digital environment is becoming particularly important in the context of the transformation of social relations, which covers virtually all areas—public administration, the economy, education, healthcare, and communications. The growth in the number of digital services, the use of information and communication technologies in everyday activities, and the formation of a global cyberspace have led to an unprecedented spread of personal information. In the context of the rapid development of digital technologies, this position has taken on a new dimension. Data that was previously considered secondary — such as log files, geolocation information, search history, and behavioral markers — is now used for comprehensive digital profiling of individuals. This creates risks of interference with human autonomy, the imposition of behavioral patterns, manipulation, and discrimination based on algorithmic decisions.

In this regard, personal data is considered not only

as an element of private life, but as a resource inextricably linked to freedom, human dignity, and autonomy of will. That is why the legal systems of states are moving from declarative protection mechanisms to the implementation of risk-oriented tools that respond to modern technological challenges.

As scientists note, "Actions in the digital space leave traces that can be used to analyze personality, behavior, social status, i.e., potentially threaten privacy" [6]. In such conditions, ensuring the right to privacy becomes not only a legal but also a social, technological, and ethical problem that requires a comprehensive approach.

As researchers O. V. Zaderayko, O. G. Trofimenko, Y. V. Prokop, and others, analyzing information systems with stationary and mobile devices oriented toward interaction with digital space, "IT corporations collect and process user data, primarily through traffic redirection (e.g., DNS queries) and subsequent encryption, which makes it impossible for government agencies to control this process. This study directly points to the increased mobility and dynamism of information flows in the digital environment, as well as the associated risks to privacy and the need for appropriate legal and technical mechanisms to control and protect them" [8]. In this context, the national legal model must evolve in line with technological and social changes, ensuring the preservation of fundamental human rights.

The Law of Ukraine "On Personal Data Protection" defines the basic principles of information processing: "legality, purpose, proportionality, reliability, accuracy, and data minimization" [4]. Ukraine also seeks to implement the provisions of the GDPR (General Data Protection Regulation) – the European data protection regulation. As O. Gomaniuk points out, "the GDPR is a pan-European data protection law that sets high standards of confidentiality" [3, p. 71]. We would add that the GDPR defines the rights of data subjects, in particular the right to access, correct, delete, and restrict the processing of personal information. In addition, the regulation obliges organizations to ensure the transparency of data processing, implement security measures, and be accountable for violations of these requirements. Harmonizing Ukrainian legislation with the GDPR is critical to ensuring a high level of personal data protection, increasing citizens' trust in digital services, and integrating Ukraine into a single European information space. This allows for the creation of transparent and effective control mechanisms, the protection of data subjects' rights, and compliance with international standards in the field of confidentiality.

It should be noted that information relations in the digital environment are improving against the backdrop of the development of such state services as "Diya," the registers of the Ministry of Justice, the electronic medical system, e-learning, and e-government services. Each of these services involves massive processing of personal data, which increases the importance of legal control mechanisms.

Michèle Finck and Asia J. Biega, considering whether the principles of "purpose limitation" and "data minimization" can be "meaningfully implemented" in modern systems that process large amounts of data — in particular, algorithmic systems, machine learning, personalisation, profiling, etc., conclude that "yes, it is theoretically possible, but in practice there is a 'significant limit' to implementation, with 'restrictions' that make such compliance difficult" [5, p. 45]. In other words, the practical application of these principles is complicated by the vagueness of risk assessment methods and the insufficient level of responsibility of data operators. "To improve the protection of personal data, it is important to raise the awareness of individuals who often 'ignore issues related to the protection of personal data' due to a lack of understanding of legislative standards and requirements" [9].

European law, primarily the EU General Data Protection Regulation (GDPR), has a significant influence on the formation of national standards. Its provisions have become a benchmark for Ukrainian legislative reforms aimed at modernizing the legal regime for data, increasing the transparency and accountability of data controllers, and improving mechanisms for informing and obtaining consent from data subjects [7].

Global experience shows that the most effective model for personal data protection is the European Union standards set out in the General Data Protection Regulation (GDPR). The Regulation grants data subjects broad rights, including: the right of access; the right to be forgotten; the right to data portability; the right to restrict processing; and the right to object to profiling [7].

Ukraine, moving towards European integration, is gradually harmonizing its legislation with the GDPR standards, but full implementation requires:

- rethinking the principles of processing;
- introducing new procedures (Data Protection Impact Assessment, Data Protection Officer);
- creating an independent body with sufficient resources and powers;
- updating the sanction mechanism.

As scientists who studied how companies adapted their security and privacy policies after the introduction of the GDPR rightly note, "harmonization of regulations has forced a change in approaches to security and privacy—which is an indicator of how regulatory changes shape practice" [10].

Issues of cybersecurity and information system resilience are becoming particularly relevant. In the context of the ongoing armed aggression against Ukraine, cyberattacks on state registries, the banking sector, and critical infrastructure have increased the need to implement comprehensive technical and legal data protection mechanisms. CERT-UA analytical materials demonstrate an increase in the scale of attacks aimed at stealing, encrypting, and manipulating personal data, which requires the modernization of state digital security policies and the enhancement of the capabilities of relevant authorities [2].

Effective protection of personal data is only possible with the support of capable institutional structures. In Ukraine, the Ukrainian Parliament Commissioner for Human Rights is responsible for monitoring compliance

with the rights of data subjects. However, researchers emphasize the limited resources of this body, particularly in terms of personnel and finances. Unlike European Data Protection Authorities, the Ukrainian ombudsman does not have the necessary infrastructure to carry out systematic monitoring of digital services.

Important areas for reforming the institutional model include:

- creating a separate state service or agency for personal data protection;
- strengthening the powers of the supervisory authority;
- improving mechanisms for cooperation with the private sector;
- increasing the transparency of data processing in state registers;
- developing benchmark cyber security policies.

These measures are aimed at creating a robust system capable of responding quickly to technological changes and new types of threats.

One of the key non-legal factors for effective data protection is the level of digital literacy among citizens. According to surveys conducted by government and public initiatives, only about a third of Ukrainians fully understand what data mobile applications and internet platforms collect. A similar situation can be observed in the field of electronic services. Lack of adequate awareness increases the risks of manipulation, social engineering, and illegal data collection.

International corporations, including Google, Facebook, and Amazon, possess significant amounts of personal data belonging to billions of users around the world, creating potential risks of misuse, leakage, or commercialization without the proper consent of the data subjects. In response to these challenges, many countries are implementing national legislative mechanisms to regulate the processing of personal data. As mentioned above, the European Union has introduced a set of rules and principles known as the GDPR [7], which define standards of legality, proportionality, and transparency in data collection and processing. However, the global nature of the internet complicates the unification of privacy requirements across different jurisdictions, creating additional risks for the protection of user rights on an international scale.

Organizations that collect personal data must be guided by ethical principles, including ensuring transparency of processes and obtaining voluntary, informed consent from users for the processing of their data. In international communications, the application of these principles is complicated by cultural, legal, and social differences between countries: what is considered ethically acceptable in one country may be considered unacceptable in another. In this regard, there is an urgent need to develop universal ethical standards that would harmonize approaches to the protection of privacy and personal information in the global digital environment, ensuring a balance between the rights of users, the commercial interests of organizations, and international norms.

A separate aspect concerns the ethics of digital interaction. Artificial intelligence technologies, facial recognition systems, and other tools pose potential threats to human autonomy. As noted by the Council of Europe, an ethical approach should be based on the principles of gender equality, non-discrimination, transparency, and respect for dignity. Therefore, legal regulation should be combined with ethical standards that define the limits of acceptable use of algorithms and artificial intelligence.

Thus, an effective mechanism for ensuring the protection of personal data in the digital environment must be based on a balanced combination of national and international standards, institutional development of supervisory bodies, improving the digital competence of citizens, and the implementation of modern technical solutions. The complexity of the issue necessitates an interdisciplinary approach that combines the legal, organizational, technical, and ethical aspects of the functioning of digital systems.

CONCLUSION

The study showed that the right to personal data protection in the digital environment is one of the key components of human rights in the information society. An analysis of national and international legislation shows that the effective implementation of this right requires a comprehensive approach that takes into account both regulatory and technological aspects of information protection.

An analysis of national legislation has shown that, although Ukraine has established basic guarantees for the protection of personal data, there are significant gaps in practice. In particular, the legislation does not sufficiently take into account modern technological challenges, the problems of algorithmic profiling, automated decision-making, and transnational processing of personal data. The inconsistency of certain provisions of the national protection system with the requirements of the GDPR and international standards complicates the implementation of the rights of data subjects and creates potential threats to their privacy [1].

International experience, in particular the practice of the European Union and the Council of Europe, demonstrates the effectiveness of a comprehensive approach to ensuring the right to personal data protection, which combines clear standards for information processing, control and accountability mechanisms, and guarantees of data subjects' rights. Taking these approaches into account when harmonizing Ukrainian legislation will increase the level of legal protection and ensure the integration of the national system into the global digital space.

Thus, the analysis of national and international approaches to ensuring the protection of personal data in the digital environment shows some progress in legal regulation, while revealing current gaps and potential risks associated with the rapid development of digital technologies and insufficient legal and digital awareness of data subjects. Taking these circumstances into account necessitates the formulation of targeted proposals, including: improving the national regulatory framework to take into account the current challenges of the digital environment; harmonizing

Ukrainian legislation with international standards, in particular the GDPR; introducing effective technical and organizational measures to protect personal data in public and private institutions; raising citizens' legal and digital awareness of their rights and the safe use of digital services; and introducing a system of control and accountability for violations in the field of personal data processing.

The implementation of these proposals will contribute to improving the effectiveness of personal data protection in Ukraine, ensuring an adequate level of digital security, strengthening trust in electronic services, and integrating the national system into the international legal space.

REFERENCE:

1. Asmita Dalela, Saverio Giallorenzo, Oksana Kulyk, Jacopo Mauro, Elda Paja (2021). A Mixed-method Study on Security and Privacy Practices in Danish Companies. https://doi.org/10.48550/arXiv.2104.04030.
2. First annual report on the results of the vulnerability detection system and response to cyber incidents and cyber attacks. Retrieved from: https://cert.gov.ua/article/17696
3. Gomanyuk O.(2024) Issues of ethics and confidentiality in digital international communications. Scientific journal of the Mykhailo Dragomanov National University. Issue 36. https://doi.org/10.31392/UDU-nc.series22.2024.36.08
4. Law of Ukraine "On the Protection of Personal Data" dated 01.06.2010 No. 2297-VI. Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. Michèle Finck, Asia J. Biega (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. Technology and Regulation : pp. 44-61. https://doi.org/10.48550/arXiv.2101.06203
6. OLINDER, N., TSVETKOV, A., FEDYAKIN, K., & ZABURDAEVA, K. (2020). Using Digital Footprints in Social Research: an Interdisciplinary Approach. WISDOM, 16(3), 124–135. https://doi.org/10.24234/wisdom.v16i3.403
7. 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, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
8. Research on potential data leaks in information and communication systems / O. V. Zaderayko, O. G. Trofimenko, Yu. V. Prokop, N. I. Loginova, A. I. Dika, S. V. Kukharenko. Radioelectronic and Computer Systems: Scientific and Technical Journal. Kharkiv: "HAI", 2022. - No. 4 (104). - P. 64-84. - Access mode: https://doi.org/10.32620/reks.2022.4.05.
9. Shabatura, M. M., & Salashnyk, R. O. (2021). Analysis of personal data protection methods according to ukrainian legislation and the GDPR. Ukrainian Journal of Information Technology, 3(2), 51–57. https://doi.org/10.23939/ujit2021.02.051
10. Voigt P., Von dem Bussche A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer. https://doi.org/10.1007/978-3-319-57959-7