UDK 342.925

Mariana POVALENA
Lviv Polytechnic National University,
Educatinoal and Rasearch Institute of Law,
Psychology and Innovative Education,
Associate Professor of the Administrative
and Informational Law Department,
Ph.D. in Law, Associate Professor
mariana.v.povalena@lpnu.ua,
ORCID: 0000-0001-5638-200X

Nazar LEVCHUK
Lviv Polytechnic National University,
student of the Educational and Research Institute of Law,
Psychology and Innovative Education,
nazar.levchuk.mpvprz.2025@lpnu.ua
ORCID: 0009-0008-7068-9612

LEGAL SUPPORT OF INFORMATION SECURITY IN THE FIELD OF PERSONAL DATA PROTECTION

http://doi.org/10.23939/law2025.48.350

The article examines current issues related to the legal aspects of personal data protection in the context of ensuring information security amid the digitalization of society. It argues that personal data are among the most vulnerable assets in today’s information environment, and that improper processing or leaks can lead to significant violations of human rights and freedoms, undermine trust in state institutions, and create threats to national security.

The paper analyzes the main legislative initiatives of Ukraine that regulate the procedures for collecting, processing, storing, and using personal data, including the provisions of the Laws of Ukraine “On Information,” “On the Protection of Information in Information and Telecommunication Systems,” “On State Secrets,” and “On Personal Data Protection.” It outlines key mechanisms for ensuring data security and highlights the role of state authorities in monitoring compliance with legal requirements.

Particular attention is paid to international standards and practices, notably the EU General Data Protection Regulation (GDPR), which significantly influence the development and improvement of national legislation. A comparative analysis is conducted to identify gaps in domestic legal regulation and to determine directions for its harmonization with European norms.

Special emphasis is placed on the challenge’s organizations face in complying with legislative requirements, including high financial costs, personnel shortages, the growing number of cyber threats, and a low level of legal awareness among the population. The paper also considers liability for violations of personal data processing rules, including administrative, civil, and criminal sanctions, as well as consequences for business entities such as loss of business reputation or restricted access to international markets.

Key words: personal data protection, information security, international standards, liability, data processing, data storage, public authorities, legal regulation, cybersecurity, data protection mechanisms.

Formulation of the problem. In today's information society, the issue of legal provision for information security in the sphere of personal data protection has acquired particular relevance. With the advancement of digital technologies, the widespread adoption of information and communication systems, and the expansion of electronic services, the volume of personal data processing has been rapidly increasing. This gives rise to new security challenges, as personal data is increasingly becoming the target of unauthorized access, cybercrime, manipulation, and abuse. Under such conditions, the state is obliged to ensure effective legal regulation that not only guarantees the inviolability of citizens' private lives, but also establishes clear mechanisms for monitoring the processing and safeguarding of personal information.

Despite the existence of a legal framework regulating personal data protection at both national and international levels, numerous gaps and deficiencies in its application are observed. Legislation often fails to keep pace with the dynamic changes in the sphere of digital technologies, while existing norms remain formalistic or are not adequately enforced in practice. The lack of unified standards, weak law enforcement practices, a low level of digital literacy among the population, and insufficient oversight by competent authorities only exacerbate the problem. Thus, there is a compelling need for a thorough analysis of the current legal mechanisms of information security in the context of personal data protection, identification of key problematic aspects, and the development of effective solutions for their resolution.

Analysis of the study of the problem. Analysis of the study of the problem. The issues of personal data protection, information security, and legal regulation in the field of ensuring confidentiality have been considered in the works of such scholars as T. I. Stoeva, A. O. Korenev, V. G. Pylypchuk, V. M. Bryzhko, as well as O. V. Petryshyn, T. I. Shevchenko, I. V. Kucheriavyi, S. V. Knysh, V. I. Teremetskyi, O. S. Cherniak, and others.

Various aspects of the adaptation of international standards for personal data protection, liability for violations, as well as cybersecurity mechanisms have been highlighted in both theoretical and applied research. However, a comprehensive analysis of the current system of legal regulation and the implementation of effective mechanisms for the protection of personal data in the context of the digitalization of society remains understudied. Special attention should be paid to finding a balance between technological development, innovation, and the guarantee of citizens' rights to privacy, as well as to the practical implementation of control by public authorities and society. This determines the necessity for further scientific analysis of the current state and prospects for the development of personal data protection in the context of information security and compliance with international standards.

The purpose and objectives of the publication. The issues surrounding the legal framework for information security in the context of personal data protection have repeatedly been the subject of scholarly research by both domestic and foreign specialists. In their works, they emphasize the need to adapt legislation to address emerging information threats, particularly in connection with the development of artificial intelligence, cloud computing, and big data. Researchers, in particular, draw attention to the uncertainty of legal categories related to digital rights, the challenges in ensuring valid consent for data processing, and the shortcomings of mechanisms for monitoring compliance with confidentiality requirements. Studies show that even in countries with well-developed democratic institutions, there is a high incidence of violations in the field of personal data protection, indicating a systemic problem−namely, the lag of legal regulation behind technological progress.

At the same time, scholars underscore the necessity of integrating national personal data protection legislation with international standards, especially the provisions of the European Union's General Data Protection Regulation (GDPR), which sets high standards for transparency, accountability, and security in data processing. The research highlights the importance of a cross-sectoral approach to ensuring information security, which combines the provisions of information, administrative, criminal, and civil law. Special attention is paid to the role of institutional support−namely, the activities of bodies responsible for monitoring, auditing, and supervising the processing of personal data. However, despite some achievements in this field, the issue remains insufficiently studied in a comprehensive manner, calling for further scholarly analysis of the legal foundations of information security in conjunction with the technological and social aspects of the contemporary digital environment.

The aim of this article is to examine the legal framework for ensuring information security in the field of personal data protection, to analyze the current legislation, to identify the main problems and shortcomings in law enforcement practice, as well as to formulate proposals for improving the regulatory framework in view of contemporary information challenges and international experience. Within the scope of this research, a comprehensive analysis of the current national legislation of Ukraine in this area is envisaged, in particular, its compliance with international standards such as the GDPR. The research also aims to determine the key issues in legal regulation and enforcement practice, and to describe the role of competent state authorities in ensuring supervision and compliance with information security requirements. Special attention will be given to legislative gaps, legal uncertainty of certain terms and mechanisms, as well as the need to address these shortcomings through the introduction of effective, transparent, and digitally-adapted legal instruments.

Presenting main material. The legal framework for information security in the field of personal data protection is a key component of national security and a foundational element of a democratic society, where the right to privacy of the individual is a priority. In the contemporary conditions of rapid development of information technologies, in particular the deployment of e-government, digital services, mobile applications, and cloud platforms, the volume of personal data processed is increasing at a geometric rate. This creates not only new opportunities but also significant risks of leakage, unlawful collection, use, or destruction of such information. Accordingly, there is a necessity for a systematic analysis of the current normative-legal framework that regulates the procedures for processing, storage, transmission, and protection of personal data, as well as the identification of effective mechanisms to counter cyber threats and unauthorized access to confidential information.

Cybersecurity of computer users in the era of digital transformation is becoming an increasingly important task. The challenges associated with the growth in the number and complexity of cyberattacks, insufficient cybersecurity in the Internet of Things, social engineering and the development of innovative cyberthreats require a comprehensive approach and cybersecurity strategies. To effectively protect information technology in the era of digital transformation, it is necessary to combine technical, organizational and educational measures. [1, p. 145]

The Law of Ukraine "On Information" [2] establishes fundamental legal categories that are essential for understanding and ensuring information security. In particular, information is defined as any data and/or facts that may be stored on tangible media or represented in electronic form, which covers both traditional and digital forms of information. At the same time, the concept of information protection is defined as a set of legal, administrative, organizational, technical, and other measures aimed at ensuring the preservation, integrity of information, and the proper regime of access to it. Such a broad and comprehensive interpretation allows for the formation of a multi-level system of guarantees necessary for the effective functioning of the information sphere of the state under contemporary challenges.

The Law of Ukraine "On the Protection of Information in Information and Telecommunication Systems" [3] sets out key components of the legal mechanism for ensuring information security in the context of the digital environment. In particular, technical information protection is understood as a type of protection aimed at preventing leakage, destruction, blocking of information, as well as breaches of its integrity and access control. This type of protection is implemented by means of engineering, technical, and software tools. An important aspect is the clear delineation of the objects of protection within information and telecommunication systems−this includes both the information processed within the system and the software that ensures its processing. This approach emphasizes the interrelationship between technical infrastructure and information content, requiring a holistic and comprehensive approach to the protection of both the data and the tools used to process it.

The Law of Ukraine “On State Secrets” [4] defines key concepts that regulate the procedure for safeguarding information, the disclosure of which could pose a threat to national security. According to the law, a state secret (also referred to as classified information) is a type of confidential information encompassing data in the areas of defense, economy, science and technology, foreign relations, state security,

and law enforcement, the disclosure of which could cause harm to the national security of Ukraine. Such information is officially recognized as a state secret in accordance with the legally prescribed procedure and is subject to mandatory protection by the state.

Additionally, the law establishes the concept of degrees of secrecy, which includes such categories as "of special importance," "top secret," and "secret." These categories determine not only the level of importance of classified information but also the degree of restriction of access to it and the corresponding level of its protection. This enables a differentiated approach to the safeguarding of sensitive data within public administration.

In the Law of Ukraine "On Personal Data Protection," [5] the key element is the definition of the term personal data, understood as information or a set of information about an individual who is identified or can be specifically identified. This means that personal data includes any information that directly or indirectly enables the identification of a person, including their name, identification number, address, employment details, marital status, medical information, and so on. Such an approach ensures broad coverage of the area subject to legal regulation, establishing obligations for entities processing such data regarding their storage, proper use, and protection against unauthorized access, interference, or dissemination. The law sets forth the fundamental principles for personal data processing, the rights of data subjects, and establishes mechanisms of state supervision over compliance in this sphere, which is a fundamental element of the modern information security system.

Despite the existence of a developed regulatory framework for information and personal data protection in Ukraine, a significant proportion of citizens lack sufficient awareness of the terms and rules governing these matters. Many people are unfamiliar with such concepts as "state secret," "personal data," "technical information protection," and other important terms that may be directly relevant to their protection. This creates favorable conditions for abuse, both on the part of law enforcement agencies−which may unjustifiably exploit citizens' ignorance−and from fraudsters who actively take advantage of the insufficient legal awareness among the population to pursue their criminal intentions. Unawareness of rights and obligations in the realm of information protection often leads to citizens becoming victims of information crimes, breaches of confidentiality, or the unlawful collection and use of their personal data.

Lawyers and legislators face a significant dilemma as to whether the current legal framework provides sufficient protection for personal data, or, conversely, whether there is a risk of excessive legislative regulation that could lead to unnecessary bureaucracy and complicate processes. On one hand, the development of digital technologies and the increasing volumes of data being processed present new challenges to the protection of personal information. Various technologies, such as artificial intelligence, big data, and cloud services, create more complex mechanisms for the processing and storage of personal data, which requires a clear, updated, and modern legal foundation. Legislation must be flexible and able to promptly respond to emerging threats and challenges, ensuring a high level of protection while not restricting technological progress and innovative development.

On the other hand, excessively detailed or overly strict legislation can create significant barriers to the development of business and technological startups, as requirements for the collection, processing, and protection of personal data might be too complicated or costly for small and medium-sized enterprises. Another important issue is the risk of overburdening state supervisory and regulatory authorities, which can lead to inefficient use of resources, bureaucratic delays, and reduced enforcement effectiveness. Taking this into account, there is a need to strike a balance between ensuring citizens' rights to the protection of personal data and maintaining economic and technological freedom in order to support innovation and not hinder the development of new technologies. This requires constant review of legislation, adaptation to new conditions, and the pursuit of optimal, rather than excessive, legal regulation−regulation that would ensure effective protection without creating unnecessary obstacles to economic development.

Given the rapid advancement of informatization and technological change, the protection of personal data is becoming increasingly relevant. The necessity to guarantee human rights in this sphere requires the creation of a comprehensive protection mechanism, which would include not only organizational and

technological measures but also legal instruments. An important step in this direction is the recognition of personal data as an object of legal protection, based on principles regulating societal relations concerning property and tangible assets. In accordance with this, a person's personal data may be recognized as their personal property, to which they are entitled to exercise all rights analogous to those of an owner of tangible property. Such recognition of personal data as property allows for the creation of a legal construct that provides the individual with control over its storage, processing, and use. This means that the individual may independently determine who, and under what conditions, has access to their personal data, as well as on what grounds and within what limits such data may be used. Ownership of personal data enables the protection of such data from unauthorized access, use, or disclosure.

However, in addition to ensuring and maintaining the stability of economic and informational security, further development is necessary. Recommendations on political and economic issues aimed at improving information and economic security may include strengthening control over the spread of disinformation and fake news. It is important to provide a transparent and reliable informational basis for political and economic decision-making, including access to accurate data and statistics. One of the key aspects of improving economic security is the development of a robust legal system that will ensure the protection of property rights and combat corruption. The involvement of qualified professionals in the fields of politics and economics can have a positive impact on the formulation of strategies and recommendations to ensure information and economic security. Coordination between political and economic institutions, including cooperation with international partners, can facilitate the implementation of recommendations regarding political and economic issues aimed at enhancing informational and economic security. [6, p. 39].

Conclusions. The protection of personal data within the modern information society is not merely a technical or organizational challenge; it is a fundamental component of human dignity, the effective realization of basic rights, and a core pillar of national security. The ongoing expansion of digital technologies, the intensification of data flows, and routine cross-border data processing exponentially increase the risks and consequences associated with data misuse, extending from individual harms−such as identity theft, discrimination, or undue surveillance−to large-scale systemic risks like a loss of public trust, threats to economic stability, and new avenues for hostile attacks.

Despite positive legislative steps towards personal data protection in Ukraine, a persistent gap remains between formal legal regulation and its practical enforcement. This is evidenced by limited public awareness, insufficient institutional capacity, and uneven application of data protection norms. Therefore, efforts to bridge this gap should prioritize accessible public education on data rights and risks, the provision of practical tools and sector-specific guidance for data controllers and processors, as well as enhanced and proportionate oversight by authorities. Strengthened capacity-building, specialized training, and risk-based supervision are critically important to ensure meaningful compliance.

At the same time, the volatile pace of technological innovation−ranging from artificial intelligence and biometrics to cloud computing and data brokerage−demands regulatory frameworks that are both technologically neutral and anchored in enduring principles, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and accountability. Ukrainian legislators should continue aligning with evolving European standards, particularly the GDPR, and embed "privacy by design and by default" into all large-scale ICT systems, public procurement, and critical infrastructure. Special consideration should be given to regulating high-risk processing activities, such as algorithmic profiling, through clear mandates for human oversight, explainability, and effective avenues for individual redress.

A pressing issue for both scholars and policymakers is clarifying the legal regime of ownership and control over personal data. While the notion of private ownership can enhance individual sovereignty, legal models must avoid commodifying data in ways that undermine autonomy. The focus should be on inalienable data subject rights−such as access, rectification, erasure, and portability−coupled with strong requirements for informed, revocable consent, and regulated frameworks for data intermediaries that prioritize the interests of individuals. Structures for secure data sharing, including data trusts or cooperatives, could allow greater citizen participation in data-driven innovation without relinquishing privacy.

The efficacy of data protection ultimately depends on the capacity and integrity of supervisory authorities. These bodies must be well-resourced, independent, and technologically adept, with sufficient investigative powers and the ability to conduct systematic audits, investigate breaches, and proactively manage emerging risks. Interagency cooperation, transparent reporting on compliance and breaches, and the development of relevant oversight metrics will further strengthen accountability.

Organizationally, robust risk management and the implementation of "security by default" are crucial. This includes regular staff training, comprehensive data protection impact assessments, adoption of secure architectures and encryption protocols, thorough supply-chain due diligence, and well-rehearsed incident response plans. Economic proportionality should also be maintained so that compliance obligations are scaled to the risk level and organizational capacity, thereby encouraging entrepreneurial activity and privacy-enhancing technologies without compromising protection.

Finally, fostering public trust requires not just formal compliance, but a tangible, culture-wide commitment to privacy. This must be supported by open and comprehensible communications about the use of data, the societal benefits and risks involved, and broad-based digital literacy initiatives embedded across all levels of education. Ukraine's integration with European and international standards not only facilitates cross-border cooperation, but also strengthens domestic safeguards, enabling both data-driven innovation and protection of fundamental rights.

In sum, an effective system of personal data protection arises from the dynamic convergence of clear legislation, empowered institutions, risk-based organizational practices, and an informed and vigilant public. By continually updating and harmonizing these elements−and ensuring that regulation is both principled and practically enforceable−the state can reliably safeguard individual autonomy, enable trustworthy technological advancement, and reinforce national security for today's digital era.

Acknowledgements None.

Funding. The author declares no financial support for the research, authorship, or publication of this article.

Author contributions: Pjvalena Mariana – 50%, Levchuk Nazar – 50%. The authors approve this work and take responsibility for its integrity.

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

REFERENCES

1. Tarasyuk D., Prokopov S. Cybersecurity of Computer Users in the Era of Digital Transformation. Modern Information Technologies in the Activities of the National Police: Materials of the All-Ukrainian Scientific and Practical Conference (Dnipro, November 2, 2023). Dnipro: 2024. 184 p., pp. 144–146. [In Ukrainian].

2. On Information: Law of Ukraine No. 2657-XII of October 2, 1992 (as amended as of November 15, 2024). Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення: 04.08.2025) [In Ukrainian].

3. On the Protection of Information in Information and Telecommunication Systems: Law of Ukraine No. 80/94-VR of July 5, 1994 (as amended as of June 28, 2024). Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-vr#Text (Дата звернення: 04.08.2025) [In Ukrainian].

4. On State Secrets: Law of Ukraine No. 3855-XII of January 21, 1994 (as amended as of October 30, 2024). Retrieved from: https://zakon.rada.gov.ua/laws/show/3855-12#Text (Дата звернення: 04.08.2025) [In Ukrainian].

5. On the Protection of Personal Data: Law of Ukraine No. 2297-VI of June 1, 2010 (as amended as of January 18, 2025). Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Дата звернення: 04.08.2025) [In Ukrainian].

6. Kurilo, D., Svitlychnyi, V. Application of Unmanned Aerial Vehicles for Combating Law Violators. Commandant's Hour. Modern information technologies in the activities of the National Police. Materials of the All-Ukrainian Scientific and Practical Conference (Dnipro, November 2, 2023). Dnipro: Dnipropetrovsk State University of Internal Affairs, 2024. 184 pp., pp. 37–39. [In Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Тарасюк Д., Прокопов С. Кібербезпека користувачів комп'ютерів в епоху цифрової трансформації. Сучасні інформаційні технології в діяльності Національної поліції: Матеріали Всеукраїнської науково-практичної конференції (Дніпро, 2 листопада 2023 р.). Дніпро: 2024. 184 с., с. 144–146.
2. Про інформацію: Закон України № 2657-XII від 2 жовтня 1992 р. (зі змінами від 15 листопада 2024 р.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення: 04.08.2025).
3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України № 80/94-VR від 5 липня 1994 року (зі змінами від 28 червня 2024 року). URL: https://zakon.rada.gov.ua/laws/show/80/94-vr#Text (Дата звернення: 04.08.2025).
4. Про державну таємницю: Закон України № 3855-XII від 21 січня 1994 року (зі змінами від 30 жовтня 2024 року). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (Дата звернення: 04.08.2025).
5. Про захист персональних даних: Закон України № 2297-VI від 1 червня 2010 року (зі змінами від 18 січня 2025 року). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Дата звернення: 04.08.2025).
6. Курило Д., Світличний В. Застосування безпілотних літальних апаратів для боротьби з порушниками закону. Командирська година. Сучасні інформаційні технології в діяльності Національної поліції. Матеріали Всеукраїнської науково-практичної конференції (Дніпро, 2 листопада 2023 р.). Дніпро: Дніпропетровський державний університет внутрішніх справ, 2024. 184 с., с. 37–3

Received: 19.08.2025
Revised: 10.09.2025
Accepted: 29.09.2025
Published (online):12.12.2025
Printed:26.12.2025

Мар’яна ПОВАЛЕНА
Національний університет “Львівська політехніка”,
доцент кафедри адміністративного
та інформаційного права
Навчально-наукового інституту права,
психології та інноваційної освіти,
кандидат юридичних наук, доцент
mariana.v.povalena@lpnu.ua,
ORCID: 0000-0001-5638-200X

Назар ЛЕВЧУК
Національний університет “Львівська політехніка”,
студент Навчально-наукового інституту права,
психології та інноваційної освіти,
nazar.levchuk.mpvprz.2025@lpnu.ua
ORCID: 0009-0008-7068-9612

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

У статті розглядаються актуальні питання, пов’язані з правовими аспектами захисту персональних даних у контексті забезпечення інформаційної безпеки в умовах цифровізації суспільства. Обґрунтовується, що персональні дані є одним із найбільш уразливих об’єктів у сучасному інформаційному середовищі, а їх неналежна обробка чи витік можуть призвести до суттєвих порушень прав і свобод людини, підриву довіри до державних інституцій, а також створення загроз для національної безпеки.

У роботі здійснено аналіз основних законодавчих ініціатив України, що регулюють порядок збирання, обробки, зберігання та використання персональних даних, зокрема положень Законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю» та «Про захист персональних даних». Розкрито ключові механізми забезпечення безпеки даних, а також висвітлено роль державних органів у контролі за дотриманням законодавчих вимог.

Особлива увага приділена міжнародним стандартам і практикам, зокрема Загальному регламенту ЄС про захист даних (GDPR), які значно впливають на розвиток та вдосконалення національного законодавства. Проведено порівняльний аналіз, що дозволяє виявити прогалини у вітчизняному правовому регулюванні та визначити напрями його гармонізації з європейськими нормами.

Окремо акцентується на викликах, з якими стикаються організації у процесі виконання законодавчих вимог, серед яких високі фінансові витрати, кадровий дефіцит, збільшення кількості кіберзагроз і низький рівень правової культури населення. Також, розглядаються питання відповідальності за порушення норм обробки персональних даних, включаючи адміністративні, цивільно-правові та кримінальні санкції, а також наслідки для суб'єктів господарювання у вигляді втрати ділової репутації чи обмеження доступу до міжнародних ринків.

Ключові слова: захист персональних даних, інформаційна безпека, міжнародні стандарти, відповідальність, обробка даних, зберігання даних, органи державної влади, правове регулювання, кібербезпека, механізми захисту даних.