ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 1(15), 2025

УДК 343.45
DOI 10.31732/2708-339X-2025-15-A2

ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ ПОШИРЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ГЛОБАЛІЗАЦІЇ

Горєлова В.Ю.,
кандидат юридичних наук, доцент,
доцент кафедри державно-правових дисциплін
Університет економіки та права «КРОК»
Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: HorelovaVY@krok.edu.ua
ORSID: https://orcid.org/0000-0001-6536-2422

ETHICAL AND LEGAL ASPECTS OF PERSONAL DATA DISSEMINATION IN THE CONTEXT OF GLOBALISATION

Horielova V.Yu.,
candidate of legal sciences
associate professor of department of state legal sciences of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: HorelovaVY@krok.edu.ua
ORSID: https://orcid.org/0000-0001-6536-2422

Анотація. *Стаття присвячена всебічному аналізу етичних і правових аспектів обробки персональних даних у глобалізованому світі, зокрема у контексті міжнародного співробітництва. У статті зазначено, що захист персональних даних стає пріоритетом у сучасному інформаційному суспільстві, де обробка великих обсягів інформації є основою для розвитку цифрових технологій. Зауважується, що Загальний регламент захисту даних (General Data Protection Regulation, GDPR) виступає як провідний стандарт, що гарантує прозорість, безпеку та відповідальність при обробці персональних даних не лише в Європейському Союзі, але й за його межами. Вказано на суттєві відмінності між підходами до захисту конфіденційності в ЄС та США, зокрема на прикладі США підкреслені недоліки що пов'язані з відсутністю єдиного федерального закону у Сполучених Штатах, що створює ускладнення що до уніфікації міжнародних підходів до захисту даних. Окремо розглянуто етичні виклики збору даних, зокрема важливість інформованої згоди користувачів, рівність доступу до технологій та використання великих масивів інформації для наукових і медичних досліджень. У статті наголошується, що сучасні виклики цифрового середовища, зокрема кіберзлочинність і цифрова нерівність, потребують адаптації міжнародного законодавства для забезпечення правової і технологічної гармонії. Зокрема, підкреслено важливість підтримання балансу між правовими, етичними, моральними та технологічними аспектами, що до захисту прав людини в умовах цифрової епохи. Розглянуто етичні виклики збору даних, зокрема важливість інформованої згоди користувачів, рівність доступу до технологій та використання великих масивів інформації для наукових досліджень. Наголошено про сучасні виклики цифрового середовища, зокрема кіберзлочинність і цифрова нерівність, потребують адаптації міжнародного законодавства для забезпечення правової і технологічної узгодженості. У стаття акцентується увага на необхідності створення міжнародних нормативних підходів, здатних ефективно реагувати на динамічні зміни у сфері обробки персональних даних та забезпечувати прозорість і справедливість цифрового середовища.*

Ключові слова: *персональні дані, конфіденційність, глобалізація, етика.*
Формул*: 0, рис.: 0, табл.: 0, бібл.: 9.*

Abstract. *The article is dedicated to a comprehensive analysis of the ethical and legal aspects of personal data processing in the globalized world, particularly in the context of international cooperation. The article emphasizes that personal data protection is becoming a priority in today's information society, where processing large volumes of data is the foundation for the development of digital technologies. It is noted that the General Data Protection Regulation (GDPR) serves as a leading standard, ensuring transparency, security, and accountability in data processing not only within the European Union but also beyond its borders. The article points out significant differences in privacy protection approaches between the EU and the USA, particularly highlighting the drawbacks associated with the absence of a unified federal law in the United States, which complicates the unification of international data protection approaches. Ethical challenges related to data collection are also discussed, especially the importance of informed consent, equal access to technology, and the use of large data sets for scientific and medical research. The article stresses that modern challenges in the digital environment, such as cybercrime and digital inequality, require the adaptation of international*

legislation to ensure legal and technological harmony. It specifically emphasizes the importance of maintaining a balance between legal, ethical, moral, and technological aspects in protecting human rights in the digital age. The article also highlights the need for creating international regulatory approaches that can effectively respond to dynamic changes in personal data processing and ensure transparency and fairness in the digital environment.
***Keywords**: personal data, privacy, globalization, ethics.*
***Formulas**: 0, fig.: 0, tabl.: 0, bibl.: 9.*

Problem statement. The article raises the issue of personal data protection in the context of globalisation, when digital technologies are becoming the basis of economic, social and political processes, creating new challenges for legal regulation and ethical responsibility.

Relevance of the research topic. The topic is relevant due to the rapid spread of digital technologies, global information exchange, and the growing number of cases of personal data misuse. In the context of international cooperation and Ukraine's integration processes into the European Community, data protection is of critical importance for ensuring human rights and security.

Purpose of the article. The purpose of the article is to analyse the current ethical and legal approaches to personal data protection in the globalised world, and to identify the key issues and prospects for their resolution.

Analysis of the latest research and publications. Among modern studies on personal data protection, the following should be highlighted: Daniel J. Solove 'Understanding Privacy and The Digital Person', which explores the issue of privacy and personal data protection; Shoshana Zuboff's 'The Age of Surveillance Capitalism' examines the impact of data collection on privacy in the digital age; Julie E. Cohen's 'Configuring the Networked Self' focuses on privacy and data protection issues in the latest technologies. In Ukraine, the issues of personal data protection have been researched by such scholars as: O. Gron, O. Mervynskyi, G. Sutton, V. Onishchenko, S. Esimov and others.

Presentation of the main material. In a globalised world, data has become an important resource that all areas of activity rely on: from business to government to science. It is the basis for making decisions that affect the economy, politics and social sphere. However, the growing use of and access to digital technologies is accompanied by new challenges, in particular in the context of personal information protection. This issue is particularly relevant due to the importance of national and international security, when data can be used not only to support legitimate actions, but also for manipulation, espionage or abuse. One of the main challenges for Ukraine is the regulation of personal data processing in the framework of international cooperation. Existing laws do not always meet the requirements of modernity, which causes conflicts between national jurisdictions. This is vividly illustrated by the example of the European Union, which in 2018 implemented the General Data Protection Regulation (GDPR) [1], which aims to provide stricter control over the processing of personal information.

The Data Protection Regulation (GDPR) covers not only European countries, but also all companies that interact with EU citizens, regardless of company location [1]. The GDPR establishes clear rules for the processing of personal data, including giving individuals the right to control their data, request its correction, deletion or transfer to other organisations. In addition, the regulation requires companies to implement adequate security systems to avoid information leakage and provides for severe fines for violators. This approach is aimed at ensuring transparency in the use of personal data and protecting the rights of citizens from potential abuse by corporations or governments [2]. At the same time, the application of the GDPR poses certain challenges, particularly in countries where data protection legislation is less developed or where there are large tech companies that may try to avoid strict regulations. Thus, the issue of data protection in a global context requires a clear balance between innovation and ethics, legislative initiatives and international cooperation. Only in this way can we ensure reliable protection of personal information while maintaining competitiveness and the development of the digital economy.

GDPR is not just a set of rules, but a new approach to understanding privacy in the digital environment. In an environment where information is becoming an extremely valuable

resource, this regulation emphasises that data protection is about protecting the rights and freedoms of every individual. The GDPR is forcing companies around the world to consider data security by giving users more control over their personal information, as each individual has the right to say: 'My data is my property.' This creates a new order in data processing, where each step must be clearly justified and transparent [3].

In the United States, the first steps towards protecting personal data were taken back in 1974 when the Privacy Act was passed. This law can be compared to a fence protecting personal information. It establishes the principle of voluntary consent to data processing, although it provides for a number of exceptions for cases where data is used for national security or law enforcement. The law allows citizens to know what data about them is stored and to demand its correction or deletion, if necessary. However, unlike the EU, the US does not have a single law, and privacy is regulated through various laws relating to specific areas, such as healthcare, finance, or child protection [4].

Despite the fact that the US still does not have a single national law similar to the GDPR, individual states, such as California, have developed their own data protection laws that are closer to European standards. These laws aim to: ensure greater transparency in the use of data; and adequately ensure the rights of consumers to access, delete and control their data and how it is used. This indicates a general trend towards tighter legal control as data becomes an increasingly important factor for the development of the economy and society (Table 1)

Aspect.	EU	USA
Regulation	The General Data Protection Regulation (GDPR)	There is no single federal law, there are industry-specific laws (COPPA, GLBA)
Citizens' rights	Extensive rights to access, correct, delete and transfer data	Citizens' rights vary by law and industry
Data transmission	Strict rules on data transfers outside the EU	Less stringent requirements, depending on the industry
Control and supervision	Independent data protection authorities with powers to impose fines	Federal and state agencies (FTC)
User consent	More attention is paid to obtaining explicit user consent	Often rely on self-regulation of company
Reporting violations	Stricter data breach notification requirements (72 hours)	Requirements vary by state and industry
Data anonymisation	An important aspect of privacy protection, anonymisation requirements	Less stringent requirements for data anonymisation
Processing of children's data	Special rules, parental consent for children under 16	Children's Online Privacy Protection Act (COPPA) for children under 13
Fines and sanctions	High fines for GDPR violations (up to EUR 20 million or 4% of annual global turnover)	Fines vary by law and industry

Table 1 was developed by the author based on sources [2], [3], [4].

At the same time, globalisation raises new ethical questions, in particular about the inequality in access to technology between developed and less developed countries.

Technologies such as 5G are spreading rapidly in wealthier countries, while other regions face limited access to basic internet services. This leads to a digital divide between societies, which can deepen existing inequalities [4]. Therefore, in the context of globalisation, it is necessary to take into account ethical aspects when collecting and processing data, especially in international research projects that emphasise the importance of international cooperation, the latest technologies and legal regulation to improve modern research and maintain high standards of information protection [3]. Such projects include the MRFF (Medical Research Future Fund) project, which represents an innovative approach to global medical cooperation and involves the organisation of multinational clinical trials in compliance with strict standards of patient data confidentiality [5]; The ALLEA (All European Academies) initiative is working to facilitate the exchange of pseudonymised data between countries [6]; Snowflake's Precision Healthcare Initiative project integrates genetic data and digital pathology to create personalised treatments [7]; artificial intelligence, which is becoming the basis for data processing, the role of which is to analyse large amounts of information, among which personal data occupies a significant place [8]. All of these projects are examples of how modern science balances the need for access to big data with the preservation of human privacy. At the same time, ethical principles such as informed consent or privacy protection may be interpreted differently depending on the cultural and legal characteristics of each region.

Globalisation has made it much more difficult to hold people accountable for human rights violations, especially in the context of personal data privacy violations. When the data of citizens of one country are misused by a company based in another country, the question is how to ensure the protection of personal data. This issue remains relevant and requires the active development of international cooperation and generalised legislation to ensure the protection of human rights in the digital world [9]. In Ukraine, the dissemination of personal data faces numerous ethical, legal and technical challenges. One of the main ethical aspects is ensuring the confidentiality of personal data, which means protecting information from unauthorised access and use.

Equally important are the issues of fairness and transparency of data processing. Citizens should be informed about how their data is used and have the opportunity to opt out of further processing. At the same time, organisations that process data should be responsible for their safety and security [4]. Technical challenges include the fight against cybercrime, as personal data is becoming a target for hackers, which can lead to major financial and reputational losses. In addition, there is the problem of information inequality, when not all users have access to technologies that allow them to effectively protect their personal data. Social aspects are also an important issue, as data breaches cause distrust in the organisations that collect the data. This requires an ethical approach to the use of information so as not to violate the rights and freedoms of citizens [4].

Thus, the proliferation of personal data in the context of globalisation requires a careful balancing act between legal norms and ethical principles, as this issue concerns not only legal regulation but also fundamental human rights and freedoms. This approach is implemented differently in different countries and regions, including the European Union and the United States. In the EU, the main focus is on protecting human rights, which is reflected in the GDPR regulation, which creates clear rules for the processing of personal data, including guarantees of control over the use of information by its owners. At the same time, in the US, legislation is focused on balancing the interests of the state, business and citizens, where privacy rights are not always as high a priority as in the EU, which creates a contrast in approaches to data protection.

The ethical principles underlying data processing should be focused on the protection of human dignity. However, sometimes these principles may conflict with legal requirements. For example, in medical or scientific research, disclosure of personal data may be beneficial to society, but it may also violate individual rights, including loss of employment or reputation. This conflict between ethical and legal norms complicates decision-making, especially in emergency situations when it is necessary to temporarily ease restrictions on access to data for the public good. In addition, new technologies,

such as social media data analytics, provide powerful tools for solving global problems, but also pose additional risks, including misuse and unfair access to information resources. This poses a challenge to society to find an optimal balance between privacy protection and the need to process data to achieve public goals.

Conclusions. Globalisation poses significant challenges to the protection of personal data due to the disparity of technological advances and the diversity of regulatory approaches in different countries. At the same time, this process creates the need for universal protection standards that take into account the global context of the digital environment. This task is not solely the responsibility of governments and international organisations, but also of every individual, because in the context of digital globalisation, everyone participates in shaping the future of how they use their own data, which defines modern digital life.

Therefore, effective personal data protection requires: 1) continuous improvement of international legislation, which must adapt to the rapid development of technology and growing threats in the digital space; 2) active cooperation between countries in order to combine public efforts to create an effective system that will guarantee the protection of personal information and ensure fair, transparent and ethical use of personal data.

References:

1. The GDPR as Global Data Protection Regulation? (2020). Cambridge University Press. URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 (Accessed 23.01.2025)

2. General Data Protection Regulation (GDPR). (2018). URL: https://privacyinternational.org/learn/general-data-protection-regulation (Accessed 23.01.2025)

3. Data Privacy Laws: GDPR vs US Data Privacy Laws. (2024). PECB Insights. URL: https://insights.pecb.com/data-privacy-laws-gdpr-vs-us-data-privacy-laws/ (Accessed 23.01.2025)

4. EU vs US: What Are the Differences Between Their Data Privacy Laws? (2024). Endpoint Protector by CoSoSys Ltd. URL: https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/ (Accessed 23.01.2025)

5. MRFF – 2024 International Clinical Trial Collaborations Round 1 and 2 Grant Opportunity (GO6825). (2024). NHMRC. URL: https://www.nhmrc.gov.au/funding/find-funding/mrff-2024-international-clinical-trial-collaborations-round-1-and-2-grant-opportunity-go6825 (Accessed 23.01.2025)

6. International Sharing of Personal Health Data for Research. (2023). ALLEA. URL: https://allea.org/international-transfer-of-health-data-for-research/ (Accessed 23.01.2025)

7. ViVE 2024: How Increased Data Sharing Can Improve Health Outcomes. (2024). Tech Solutions for Healthcare. URL: https://healthtechmagazine.net/article/2024/03/vive-2024-how-increased-data-sharing-can-improve-health-outcomes (Accessed 23.01.2025)

8. Trendspotting: What's Coming for Clinical Trials and Research in 2024 (2024). Pubs - Clinical Research News Online. URL: https://www.clinicalresearchnewsonline.com/news/2024/01/03/trendspotting-what-s-coming-for-clinical-trials-and-research-in-2024 (Accessed 23.01.2025)

9. Overview of the Privacy Act: 2020 Edition. (2020). Justice. URL: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction (Accessed 23.01.2025)

Стаття надійшла до друку 23 січня 2025 року