UDC 004.056.5:342.7
DOI: 10.32518/sals3.2024.245

Соціально-правові студії. 2024. Т. 7, № 3
Social & Legal Studios. 2024. Vol. 7, No. 3

Personal data protection: Between human rights protection and national security

Svitlana Khadzhiradieva*

Doctor of Public Administration, Professor
State University of Intellectual Technologies and Communications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0000-0002-2256-2579

Tatiana Bezverkhniuk

Doctor of Public Administration, Professor
State University of Intellectual Technologies and Communications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0000-0002-2567-8729

Oleksandr Nazarenko

PhD in Physics and Mathematics, Rector
State University of Intellectual Technologies and Communications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0000-0002-0187-0791

Serhii Bazyka

PhD in Sciences in Public Administration, Chairman of the Supervisory Board
State University of Intellectual Technologies and Communications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0009-0003-2081-1222

Tetiana Dotsenko

Doctor of Philosophy, Associate Professor
State University of Intellectual Technologies and Communications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0000-0003-3553-1314

Abstract. This study aimed to ascertain the equilibrium between safeguarding citizens' personal data and maintaining national security in a digital world. The research analysed the regulatory frameworks and judicial practices of the European Union (EU), Ukraine, and the USA through several methodologies. EU regulation offers the most stringent personal data protection, with substantial penalties for infractions. Ukrainian legislation is progressively aligning with European standards; however, procedures for protection and liability require enhancement. The research indicated an increasing tendency in the utilization of artificial intelligence and big data technologies within national security, presenting new issues for safeguarding personal information from disclosure. The research investigated the ethical implications of utilizing such technologies and their potential effects on citizen privacy. The study examined global regulatory procedures, focusing on the European Court of Human Rights' approach to balancing the objectives of safeguarding personal information and national security. The research identified the necessity to broaden the definition of personal data to include communal dimensions and indirect ramifications of data processing in the context of big data and the Internet of Things. This study's findings underscore the importance of an interdisciplinary approach to personal data security, encompassing legal, technological, ethical, and social dimensions. The analysis presented a

Suggested Citation

Article's History: Received: 29.05.2024 Revised: 27.08.2024 Accepted: 25.09.2024

Khadzhiradieva, S., Bezverkhniuk, T., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social & Legal Studios*, 7(3), 245-256. doi: 10.32518/sals3.2024.245.

*Corresponding author

conceptual model for harmonizing the regulatory framework for the protection of privileged information, including contemporary technical problems and national security requirements. The research holds practical importance for enhancing regulations regarding personal data protection and can assist the formulation of information security plans

Keywords: confidentiality; cybersecurity; information ethics; privacy; data transparency

Introduction

The growing importance of confidential information and the need for robust protection mechanisms are increasingly critical in today's technologically advanced world, where mass data collection practices like cookies and web beacons, along with data analysis and national security threats, necessitate revisiting existing approaches. Confidential information is vital for government and commercial entities to enhance services and ensure national security, yet excessive and unchecked data collection endangers fundamental human rights such as privacy and personal data protection (Universal Declaration of..., 1948). Balancing state needs with citizen interests is essential to safeguard data adequately.

Despite significant attention, the balance between human rights and national security remains underexplored, requiring further research on transparency and accountability in handling confidential data for security purposes and minimizing privacy risks associated with modern surveillance and data analysis technologies. Government access to personal data for threat prevention or crime investigation is often opaque, risking abuse and eroding public trust. Additionally, advancements in machine learning and big data analytics offer new data processing opportunities but also pose new privacy threats, highlighting the need for novel data protection approaches tailored to these technologies (Bu-Pasha, 2020). According to R. Romansky (2022), transnational cooperation in countering crime and terrorist threats often requires the transfer of confidential information in the global network space, which creates additional risks for their protection. The development of effective mechanisms for such exchange in compliance with human rights stays an urgent task. In this context, S. Lindroos-Hovinheimo (2019) addressed the need to clarify the basic definitions of data protection legislation, which may be interpreted differently in distinct cases.

Research on personal information privacy encompasses a broad spectrum of concerns, including legislative frameworks and technological dimensions. U. Pagallo *et al.* (2019) examined several methodologies for the legal regulation of data protection and proposed abstractions to facilitate the formulation of legislation designed to safeguard personal data in the context of artificial intelligence utilization. R. Mühlhoff and H. Ruschemeier (2024) examined the technological dimensions of safeguarding personal information from disclosure. The research conducted by A. Beduschi (2024) and Y. Kovalenko (2022) is significant as it examines the protection of synthetic data within the framework of advancing machine learning technologies.

The aim of this study was to ascertain the equilibrium between safeguarding individuals' personal data and maintaining national security in a digital society. To achieve the specified objective, the tasks were delineated as follows:

1. To evaluate the existing legal frameworks for safeguarding personal data in light of the problems posed by the advancement of artificial intelligence and big data analytics.

2. To investigate the feasibility of adopting a holistic strategy for safeguarding confidential information, encompassing legal, technological, ethical, and educational elements.

3. To evaluate the potential for worldwide standardization of methods to safeguard personal information, including its role in balancing privacy and national security within the global digital landscape.

Materials and methods

The research focused on a comparative legal analysis of personal data privacy laws in Ukraine, prominent European Union (EU) nations (notably Germany and France), and the United States. The primary research approach employed was a comparative legal analysis, facilitating the examination of personal data protection rules and practices across the selected nations. The study specifically examined Ukraine's Law No. 2297-VI "On the Protection of Personal Data" (2010), the General Data Protection Regulation (GDPR) (2016), Germany's Federal Data Protection Act (2021), France's Data Protection Act (2015), and the California Civil Code (2023), among others. The efficacy of personal data protection systems was evaluated based on the following criteria: comprehensiveness of data protection coverage, presence of explicit enforcement measures, and adherence to international standards. Furthermore, the analytical method employed focused on judicial practice, particularly the ruling of the European Court of Human Rights in the case of Big Brother Watch and Others v. the United Kingdom (2021).

The case study method was employed to assess the practical impact of personal data protection legislation on business and innovation. Specifically, examples of the implementation of GDPR requirements in the activities of international companies, as well as the impact of these requirements on the development of artificial intelligence technologies and big data processing were considered. This method helped to identify concrete challenges and opportunities faced by organisations in ensuring compliance with personal data protection requirements. Another significant aspect of the study was the examination of the collaboration between government entities and the commercial sector in safeguarding personal data. Particular emphasis was placed on the function of supervisory authorities and their capacity to efficiently oversee adherence to legal obligations. The investigation indicated that the degree of collaboration across these sectors significantly differs by country, impacting the efficacy of the personal data protection framework.

The study utilised content analysis of official documents and public statements from representatives of several national authorities to examine the equilibrium between national security and the right to privacy. This facilitated the identification of primary trends in the utilization of mass surveillance technologies and the evaluation of their effects on citizens' rights. Special emphasis was placed on examining national security policies and electronic surveillance laws on their adherence to personal data protection principles.

Results

Development of modern legislation on the protection of private information. The 20th century seen notable progress

in personal liberties within the context of human rights. The enforcement of these freedoms is perpetually balanced against security considerations at the individual, societal, and state levels. The global legal acknowledgment of the right to privacy and family life, encompassing the safeguarding of personal secret information, was initially enshrined in the Universal Declaration of Human Rights (1948). Article 12 of this document stipulates that no one shall endure arbitrary intrusion into their privacy, family, domicile, correspondence, or dignity and reputation. All individuals are entitled to legal protection against such interference or assaults. This essential notion has established a foundation of later international and state legislation. It established the groundwork for the evolution of the contemporary notion of the right to safeguard secret information as a fundamental component of the human rights framework inside the information society.

The primary legislative framework in the EU is the GDPR (2016). The GDPR sets rigorous standards for protecting confidential information and increases citizens' authority over their personal data. This document has extraterritorial effects and affects companies worldwide that manage information of EU individuals. The legal safeguarding of personal data in Ukraine is an essential aspect of the right to privacy, as established in the Constitution of Ukraine (1996). This organisation was established amid the swift advancement of information technology and automated data processing. The principal legal measure in this domain is the Law of Ukraine No. 2297-VI "On the Protection of Personal Data" (2010). Consequently, both the EU and Ukraine possess distinct legislative measures designed to safeguard persons' personal data, despite being enacted at various intervals and exhibiting specific disparities in regulatory approaches.

Alongside the pan-European regulation, each country has its own laws concerning private information protection. In Germany, the Federal Data Protection Act of 2021 supplements and clarifies the GDPR requirements with specific national attributes. It delineates the GDPR requirements for the processing of personal data in occupational settings. This was crucial because the GDPR provides specific latitude to national legislators in this area. Furthermore, federal entities such as Germany have data protection laws at the state level. The Bavarian Data Protection Act (2018) regulates the handling of personal data by state authorities. The uniqueness of these laws lies in their adaptation to the specific characteristics of the administrative framework and local conditions of each region.

Both the GDPR (2016) and national data protection statutes provide comprehensive definitions of essential terminology and topics. This multilevel framework of legal regulation guarantees a thorough approach to personal data protection. The essence of this approach is that it covers diverse levels of legal regulation – from pan-European to national and regional. This structure ensures comprehensive protection of personal data, considering both pan-European standards and specific national features of each EU member state. This is achieved through the following concrete provisions: the GDPR (2016) sets out general principles and requirements (Articles 5-11); national laws concretise these principles in the local context; regional laws (in federal states) accommodate the specifics of local governance.

The ethical justification for protecting anonymity and personal information privacy is inherently connected to the notion of privacy as a fundamental human right. The ethical standards for data protection include respect for individual autonomy, damage reduction, equity, and transparency. These standards are encapsulated in many international documents, including the Charter of Fundamental Rights of the European Union (2000). It enshrined the safeguarding of personal data as a fundamental human right inside the EU framework. Article 8(1) of the Charter unequivocally states: Every individual is entitled to the safeguarding of their personal data. The Ukrainian methodology for personal data protection closely mirrors the German framework, embodying European values of secrecy. Both systems require the mandatory registration of personal datasets. Article 9 of Ukraine's Law No. 2297-VI (2010) stipulates that proprietors of personal data are required to undertake state registration by recording an appropriate entry in the State Register of Personal Data Bases. In Germany, paragraph 38 of the Federal Data Protection Act (2021) mandates that "controllers and processors must notify the supervisory authority of the commencement of automated processing". This approach differs from more stringent regimes such as those in France or Sweden. The Data Protection Act (2015) in France requires prior authorization from the National Commission for Informatics and Liberties for the processing of certain data types. The handling of personal data related to offenses, penalties, and preventive measures is permissible only with prior authorization from the National Commission for Informatics and Liberties.

Swedish Law No. 2018/218 "On the Protection of Data" (2018) enforces stricter licensing requirements. The handling of particularly sensitive personal data is allowed solely upon obtaining authorization from the Data Protection Authority. These systems are deemed more stringent as they necessitate explicit authorization from the regulatory body prior to the commencement of data processing, rather than mere registration. The establishment of personal information confidentiality is a cross-sectoral initiative encompassing regulations from multiple legal disciplines. This presents specific issues regarding the standardization of terminology. Ukrainian legislation reveals a divergence between the definition of personal data in Law No. 2297-VI (2010) and the concept of confidential information pertaining to an individual in Law No. 2657-XII "On Information" (1992). The Law of Ukraine No. 2297-VI characterizes personal data as information or a compilation of information related to an identifiable individual (Article 2), whereas the Law of Ukraine No. 2657-XII describes it as information regarding a person (personal data) (Article 11), potentially leading to ambiguity regarding the extent and nature of the safeguarded information.

The examination of the progression of European legislation for the prevention of personal information exposure reveals a progressive shift from a fragmented approach to an integrated regulatory framework. The sectoral approach allows for the unique regulation of data protection across several sectors of the economy and public life. This methodology remains dominant in the United States: HIPAA Administrative Simplification (2013) governs the safeguarding of medical data, whereas the Gramm-Leach-Bliley Act (1999) oversees the protection of financial information. This method permits the accommodation of industry-specific details but may result in data protection deficiencies and complicate overarching regulation.

The ethical justification for preserving anonymity and privacy of personal information is closely associated with

the notion of privacy as an inherent human right. Ethical criteria for data protection encompass respect for individual autonomy, damage reduction, equity, and transparency (Podoprigora *et al.*, 2019). These norms are manifested in numerous international instruments, including the Charter of Fundamental Rights of the European Union (2000). It asserts that the safeguarding of personal data is a fundamental human right inside the EU framework. Article 8(1) of the Charter unequivocally states: Every individual is entitled to the safeguarding of their personal data. This clause emphasizes the significance of personal data protection within the context of European values.

Special emphasis must be placed on the matter of accountability for breaches of legislation regarding personal data security, as this serves as a fundamental mechanism for upholding personal data protection rights and discouraging future offenders. As of 2024, administrative accountability for such infractions is established in Ukraine under Article 14 of Law No. 2657-XII (1992), which stipulates the following Transgressions of information regulations result in disciplinary, civil, administrative, or criminal consequences under Ukrainian law. However, experts point to the need to improve the liability system.

A key element of the ethical framework for safeguarding personal information is the principle of informed consent. This concept posits that individuals ought to make informed and voluntary choices regarding the gathering and utilization of their sensitive personal information. This statement delineates informed consent as a fundamental ethical concept in research involving human participants (Cherkassky, 2023). This idea is significant in scientific research and healthcare, as it is essential for the ethical and legal handling of personal information. However, modern analytics and forecasting technologies are introducing new challenges to conventional data protection procedures. It is crucial to broaden the concept of data protection to include collective aspects and indirect effects of data processing. Particularly, scenarios in which the examination of ethnicity data may result in discrimination against specific groups and perpetuate existing biases due to the functioning of machine learning algorithms.

Surveillance technologies and challenges for law enforcement agencies. The advancement of surveillance technologies presents novel potential for law enforcement organisations to combat crime and uphold public safety. Nonetheless, these technologies pose significant privacy and human rights concerns. In the realm of information security, numerous significant trends and developments substantially impact the rights and liberties of persons. The implementation of e-passports featuring embedded chips enables the global locating and surveillance of persons, hence eliciting privacy issues. The introduction of e-passports with integrated chips creates the potential for global positioning and tracking of individuals, which raises privacy concerns. For example, in Ukraine, the process of introducing electronic passports is regulated by the Law of Ukraine No. 5492-VI "On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identity or Special Status" (2012). Although this law does not make provision for direct global positioning, the presence of so much personal data on electronic media raises concerns about the possibility of unauthorised use. At the same time, government control over cryptographic tools is increasing, including legal requirements to provide decryption keys to authorised bodies in many countries, which limits the ability of citizens to protect their personal information (Kyrychok *et al.*, 2024). The UK possesses the Investigatory Powers Act (2016), which grants law enforcement authorities extensive authority to access encrypted data. Part 3, Section 253 of this legislation stipulates that a technical feasibility notice may mandate the relevant operator to eliminate electronic protections imposed by or on behalf of the operator on any communications or data.

This effectively means that companies may be forced to provide access to encrypted user data. The integration of various databases based on unified identification numbers creates the preconditions for the development of comprehensive dossiers on citizens, combining tax, medical, and social information. This is accompanied by the proliferation of video surveillance devices amidst insufficient legal restriction regarding the notification of residents, as well as the storage and access of recordings. The Law of Ukraine No. 580-VIII "On the National Police" (2015) permits the utilization of technical devices for photo and video recording; however, it fails to delineate explicit regulations regarding the storage and access to these recordings. The law stipulates that the use of technical devices and means for photography, filming, and video recording, as well as the procedures for storing, utilizing, and accessing information acquired through such devices, shall be governed by regulations set forth by the Ministry of Internal Affairs of Ukraine. This provision is flawed, as it does not set concrete time limits for the storage of records, does not define clear conditions for access to them, and does not prescribe mechanisms for notifying citizens that they were caught on CCTV cameras.

There is a tendency to restrict the anonymous use of communication tools, which potentially violates the right to privacy (Yudina *et al.*, 2024). According to International Monetary Fund (IMF) researchers R. Dom *et al.* (2022), there is increasing demand to restrict anonymity in digital financial transactions, which raises privacy concerns. This aligns with international initiatives to combat money laundering and terrorist financing. It also presents concerns to the safeguarding of users' personal data. This IMF study highlights the global nature of this trend and its potential impact on the privacy of financial services users.

The use of email monitoring technologies in the absence of clear legal restrictions creates risks of violating privacy. The development of genetic research and the creation of DNA databases opens new opportunities for medicine, but also creates risks of unauthorised use of sensitive medical information. D. Kennett (2019) illustrated a case in which genetic data gathered for scientific objectives was utilised by law enforcement organisations without the consent of the research participants. In 2018, law enforcement utilised data from the public genealogical database GEDmatch to identify a suspect in the Golden State investigation. This has prompted significant ethical inquiries regarding the confidentiality of genetic information and the boundaries of its application.

Insufficient measures to address cyberthreats, including spam, phishing, and malware, result in the unauthorized acquisition and utilization of personal sensitive information. The European Cyber Security Agency's (ENISA) 2022 assessment indicates that current measures are inadequate in effectively addressing cyberthreats. Notwithstanding initiatives to enhance cybersecurity, the incidence of successful

cyberattacks persists in increasing. In 2021, there was a 68% rise in major cybersecurity breaches compared to the prior year, highlighting the inadequacy of current protective measures (Lella *et al.*, 2022). Spyware and other means of unauthorised information gathering continue to pose a major threat to the privacy of Internet users. A recent ENISA assessment indicates that spyware and other types of invasive spying software remain significant hazards to user privacy and security. In 2022, the quantity of new spyware samples surged by 35% relative to the preceding year. These programs can gather extensive personal data, including passwords, financial details, and private communications, so posing a substantial risk to user privacy.

They underscore the urgent need to develop extensive legislative and technical strategies to protect personal information secrecy and people' privacy in the digital age, including both national security demands and individual fundamental rights. Contemporary surveillance technologies encompass several instruments, including CCTV cameras equipped with facial recognition and systems for analysing social media and mobile data (Spytska, 2023). The implementation of such technology in urban settings introduces additional concerns to citizen privacy. A primary problem for law enforcement agencies is to reconcile the efficacy of crime investigations with the safeguarding of citizens' privacy rights.

International law enforcement cooperation faces challenges due to varying data privacy practices among countries. The implementation of the GDPR (2016) in the EU has established new requirements for international data sharing among law enforcement agencies by enforcing stricter regulations for the cross-border transfer of personal data. Article 46 of the GDPR mandates that data transfers to third countries are allowed just if "adequate safeguards" are implemented. The new requirements markedly diverge from prior regulations in several respects: the GDPR encompasses a broader territorial scope, applying to data processing by controllers and processors outside the EU when they manage data of EU subjects; it enforces stricter conditions for consent, mandating that it be freely given, specific, informed, and unequivocal; it establishes new rights for data subjects, such as the right to be forgotten and the right to data portability, which were absent in the previous directive; and it has substantially heightened the maximum penalties for violations to EUR 20 million or 4% of annual global turnover.

S. Mazepa and O. Bratasyuk (2023) assert that in Ukraine, safeguarding information security requires a holistic strategy that integrates both administrative and criminal law measures, highlighting the imperative to enhance legislation and its enforcement to mitigate risks to personal information confidentiality. According to their research and the results of the present study, tackling these challenges necessitates the establishment of a legal framework governing surveillance technologies that balances security and privacy, the creation of technological and theoretical solutions enabling effective information utilization for law enforcement while mitigating privacy risks, and the promotion of international collaboration to standardize data protection strategies within law enforcement contexts.

Technical protection procedures encompass securing access to personal data processing systems, keeping backups, installing antivirus protection, and safeguarding information transmission channels. Special emphasis is placed on creating software that restricts the input of excessive personal private information and inhibits unauthorized actions. A core tenet for reducing risks to personal information confidentiality is "protection by default", which stipulates that data processing systems are configured to handle only essential information and for the least duration necessary, thus safeguarding personal information from unauthorized access. The case of Big Brother Watch and Others v. the United Kingdom (2021), decided by the Grand Chamber of the European Court of Human Rights, exemplifies the issues law enforcement agencies face regarding surveillance technologies.

This case involved a large-scale communications and data interception by British intelligence services of service providers. The Court concluded that a specific aspect of the UK's mass surveillance framework violated the rights to privacy and freedom of expression. The Court specifically noted that the mass interception regime lacked adequate "end-to-end guarantees" concerning the selection of search criteria for filtering intercepted data, the procedure for acquiring communications data from service providers failed to comply with legal standards, and the framework for obtaining intelligence from foreign intelligence services lacked a sufficient legal foundation.

This ruling is crucial as it establishes criteria for the legal and proportional application of mass surveillance technologies. The Court determined that mass interception does not inherently contravene the Convention, although emphasised the necessity for robust safeguards against misuse. Upon analysis of this decision, it is evident that numerous nations, including Ukraine, must revise their legislation to establish a definitive legal framework governing the utilization of mass surveillance technologies. This framework should ensure predictability and accessibility, impose stringent limitations on the selection of "selectors" for data filtering to prevent undue privacy intrusions, implement robust independent oversight of the operations of special services concerning mass surveillance, and offer sufficient protections for journalistic sources and the confidentiality of communications with advocates.

Comparative examination of the legal structures governing personal data protection in the EU, Ukraine, and the USA. The protection of personal sensitive information in the EU is governed by the GDPR (2016), which introduces strict protection standards and provides individuals with significant rights regarding the management of their private information. It introduced a new right to data portability (Article 20), which allows individuals to receive their personal data in a commonly used and machine-readable format, combined with the right to be forgotten (Article 17), which was not previously clearly defined in the previous directive. The GDPR introduced the concept of confidentiality by design, requiring that data protection be integrated during system design rather than applied retroactively (Article 25). This principle requires the introduction of appropriate technical and organisational mechanisms to ensure effective compliance with data protection principles. The Regulation raised the standards for consent to data processing by requiring that it be freely provided, specific, informed and unambiguous (Article 7). The GDPR provides for severe fines for violations, with a maximum of EUR 20 million or 4% of the company's total annual revenue for the preceding financial year, whichever is greater (Article 83).

The GDPR applies to all EU member states and has extraterritorial effects, influencing global companies who process data of EU citizens. This regulation enforces severe

penalties for violations, include fines of up to EUR 20 million or 4% of the company's annual worldwide revenue (Table 1). Regulation is implemented by a collection of sector-specific and state legislation. This methodology results in a disjointed legal framework and varying degrees of protection based on economic sector or geographic region. The California Civil Code (2023) exemplifies a comprehensive approach to safeguarding personal data at the state level. It confers upon customers the entitlement to be aware of the personal data collected from them and to request its deletion. Conversely, Alabama possesses a less rigorous Commercial Law and Consumer Protection (2023), which is just concerned with data breach notification. This regulation is comprehensive, covering multiple aspects of data protection. The California Civil Code (2023) confers upon consumers the right to be informed regarding the collecting of their personal data, to request its deletion, to opt out of its sale, and to receive protection against discrimination for exercising these rights. Furthermore, the Act requires that companies disclose their data collection and usage policies.

Table 1. Comparison of data protection in the EU and Ukraine

Region	EU	Ukraine
Main law	GDPR	The Law of Ukraine "On the Protection of Personal Data" (2010)
Year of adoption	2016 (entered into force in 2018)	2010 (last amended in 2021)
Scope of action	All EU and European Economic Area countries	Territory of Ukraine
Definition of personal confidential information	A broad definition that includes online identifiers. "Any information relating to an identified or identifiable natural person" (Art. 4(1) GDPR	Analogous to the EU, but less detailed. "Information or a set of information about an individual who is identified or can be specifically identified" (Article 2 of the Law)
Rights of data subjects	Wide scope of rights (access, deletion, transfer)	Comparable rights, but less extensive. Access, rectification, deletion, restriction of processing (Article 8 of the Law)
Consent to processing	Clear, unambiguous, freely provided. "A freely given, concrete, informed, and unambiguous instruction" (Article 4(11) GDPR)	Analogous to the EU, but less stringent requirements. "Voluntary expression of will of an individual to grant permission to process their personal data" (Article 2 of the Law)
Penalties for violations	Up to EUR 20 million or 4% of annual turnover (Article 83 of the GDPR)	Up to 17,000 UAH (approximately EUR 400)
Cross-border data transfer	Severe restrictions (Chapter V of the GDPR)	Restrictions analogous to the EU (Article 29 of the Law)
Notification of a data breach	Mandatory within 72 hours (Article 33 of the GDPR)	Mandatory, but the deadline is not clearly stated (Article 10 of the Law)
Role of the DPO	Mandatory for certain organisations (Article 37 of the GDPR)	Not required, but recommended

Source: compiled by the author of this study based on the Regulation of the European Parliament and of the Council No. 2016/679 "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)" (2016), the Law of Ukraine No. 2297-VI (2010), GDPR (2016)

In its pursuit of European integration, Ukraine is systematically matching its legislation with EU standards to mitigate threats to personal information confidentiality, conforming its laws to the GDPR (2016). Significant updates comprise the clarification of personal data to include online identifiers (Article 2), the introduction of the term "profiling" (Article 2), the expansion of data subjects' rights, including the right to be forgotten (Article 8), and the establishment of a mandatory reporting obligation for data breaches (Article 10). These changes represent significant progress in strengthening personal data protection, though some experts argue they do not fully meet GDPR standards. The Ukrainian Law delineates the fundamental rights of data subjects and the responsibilities of data proprietors and administrators. Article 8 specifies rights such as awareness of data collection sources, data location, processing purposes, and access to personal data, while Article 10 mandates that data owners safeguard data against inadvertent loss, destruction, and unlawful processing.

In contrast to the GDPR, Ukrainian legislation enforces milder penalties, with maximum fines limited to UAH 34,000 (approximately EUR 1,000), whereas the GDPR stipulates fines of up to EUR 20 million or 4% of a company's annual global revenue (Article 83). Furthermore, Ukrainian legislation exhibits deficiencies in governing contemporary data processing technologies, including artificial intelligence, big data, cross-border data transfers, and the obligation to designate data protection officers for entities managing substantial quantities of personal data. Utilizing GDPR experience, Ukraine could rectify these deficiencies by implementing "pseudonymisation" of data (Article 4 of the GDPR) for extensive data processing, formulating comprehensive regulations for cross-border data transfers (Chapter V of the GDPR), and requiring the designation of data protection officers for certain organisations (Article 37 of the GDPR).

A fundamental distinction among the methods of the EU, Ukraine, and the US is in the notion of consent for the processing of personal sensitive information. Within the EU,

the GDPR (2016) mandates that consent must be explicit, unequivocal, and voluntarily provided, with withdrawal being as straightforward as granting it. In Ukraine, the consent requirements are somewhat lenient, albeit they are moving towards European standards. In the EU, the GDPR requires clear, unambiguous, and freely given consent. Article 4(11) of the GDPR defines consent as a voluntary, specific, informed and unambiguous expression of the data subject's choice, by which the data subject agrees to the processing of his or her personal data by means of a declaration or an explicit affirmative act. In Ukraine, the consent requirements are quite lenient, albeit they are moving towards European standards. Article 2 of the Law of Ukraine "On the Protection of Personal Data" (2010) delineates permission as a voluntary and informed manifestation of an individual's will to authorize the use of their personal data for a designated purpose, communicated in writing or through a method that signifies consent has been given. This definition is less concrete than the GDPR and does not contain the requirement to "unambiguously indicate preferences". Furthermore, Ukrainian law does not contain a concrete requirement that withdrawal of consent should be as easy as giving it. The differences are as follows:

1. The GDPR requires a "clear affirmative action" for consent, while Ukrainian law allows consent "in a form that allows the inference of consent", which can be interpreted more broadly.

2. The GDPR specifically requires consent to be "concrete" and "informed", while Ukrainian law only states "provided it is informed", which is a less strict formulation.

3. Unlike the GDPR, Ukrainian law does not contain specific provisions on the ease of withdrawal of consent.

These differences demonstrate that although the Ukrainian law is approaching European standards, it still leaves more room for interpretation and potentially less strict application of the consent requirements for personal data processing. In the United States, especially in the online environment, implicit consent is often sufficient, e.g., through continued use of a website.

The decisive factor is the transnational flow of data. The GDPR imposes severe restrictions on the transmission of sensitive personal information outside the EU, requiring an appropriate level of protection in the recipient country. Article 45 of the GDPR authorizes the European Commission to assess the data protection standards of a third country, considering factors such as the rule of law, human rights, the presence of an independent supervisory authority, and the country's international data protection obligations. While these standards are designed to guarantee a high level of personal data protection, they may create certain obstacles for foreign businesses. Companies may incur additional costs for legal due diligence and implementation of technological solutions to ensure compliance. In addition, this may limit the choice of service providers for European businesses.

To address these challenges, the GDPR provides for additional procedures, including standard contractual provisions (Article 46) and binding business norms (Article 47). These mechanisms enable organisations to send data to nations lacking an adequacy determination, contingent upon the implementation of appropriate safeguards. Ukrainian law contains similar provisions. Article 29 of the Law of Ukraine "On the Protection of Personal Data" (2010) stipulates that personal data may be transferred to foreign entities involved in personal data activities solely if the respective state guarantees adequate protection of personal data in compliance with legal requirements or an international treaty of Ukraine. The United States adopts a more permissive stance on cross-border data transfer, frequently provoking apprehensions among European authorities and resulting in international legal disputes, exemplified by the notable Schrems II case (The CJEU opinion..., 2020). The case addressed the legality of transmitting personal data from the EU to the US pursuant to the Privacy Shield agreement. The EU court annulled the agreement, contending that US legislation failed to offer an adequate level of protection for European residents' personal data against access by US intelligence services. This ruling generated substantial legal ambiguity for enterprises transmitting data between the EU and the US and underscored the importance of worldwide harmonization of data protection strategies.

These differences have crucial implications for international business, cross-border data transfer, and the global digital economy. In particular, they increase the cost of compliance with the requirements of different jurisdictions, which is confirmed by the IAPP-EY annual privacy governance report (2019), which showed a 47% increase in budgets for organisations after the implementation of the GDPR. Strict cross-border data transfer requirements can limit companies' ability to centralise data and use cloud services, potentially reducing the efficiency of business processes. The legal uncertainty caused by different interpretations of data protection laws in different countries creates additional risks for businesses, as demonstrated by the Schrems II judgment.

According to the BSA Global Privacy Best Practices (2018), overly restrictive data localisation laws can reduce countries' gross domestic product by 1.1%. Finally, companies in jurisdictions with less stringent regulations may gain a competitive advantage through lower compliance costs. These consequences highlight the need for further harmonisation of approaches to ensuring the confidentiality of personal information at the international level, considering the global nature of modern information flows. At the same time, each jurisdiction must strike a balance between protecting privacy, promoting innovation, and safeguarding national interests, which makes the task of creating a universal model for ensuring the privacy of personal information extremely challenging. They also emphasise the need for further harmonisation of approaches to ensuring the confidentiality of personal information at the international level, considering the global nature of modern information flows. At the same time, each jurisdiction must strike a balance between protecting privacy, promoting innovation, and safeguarding national interests, which makes the task of creating a universal model for ensuring the privacy of personal information extremely challenging.

Social implications and ways to improve data protection policy. Policies safeguarding against the unauthorized use of personal information have significant and varied repercussions for society, influencing public trust, economic growth, innovation, and social equity. Comprehending these ramifications and identifying methods to enhance policies is essential for constructing a balanced and equitable digital society.

A significant societal consequence of data protection legislation is its effect on public trust in governmental organisations and commercial enterprises. The propensity of citizens to disclose personal data for governmental policy implementation is predominantly influenced by their trust in govern-

mental institutions and the relevance of certain concerns to them. The National Security Strategy of Ukraine (2020) delineates the necessity to enhance technological capacities for the protection of civilians. The document stipulates the following: "Ukraine will implement the development and utilization of integrated video surveillance systems with an analytical component for the purpose of public security" (Section III, paragraph 47). This clause embodies the worldwide trend of heightened electronic surveillance for security purposes. Nonetheless, it also presents possible threats to residents' privacy. Examining this provision within the framework of the Law of Ukraine No. 2297-VI (2010) reveals a notable tension. Article 6 of this legislation stipulates that the processing of personal data must be executed transparently and must be suitable, relevant, and not excessive in connection to the stated purpose of such processing. The question pertains to the compliance of comprehensive video surveillance systems with these criteria. Similar difficulties are seen in other nations.

Comparable challenges are observed in other countries. For example, in the United States, the National Security Strategy (2022) also emphasises the significance of using the latest technologies to ensure security: "We will use technology to address our greatest security challenges, from cybersecurity to climate change" (p. 48). Nevertheless, the US statement underscores the significance of safeguarding privacy and civil freedoms: "We will protect privacy and civil liberties and promote responsible data governance" (p. 48). These examples demonstrate the difficulty of balancing national security needs with personal data protection. On the one hand, new video surveillance and data analytics technologies can considerably improve the efficiency of public safety (Kravchenko, 2022). On the other hand, they pose risks of excessive interference in the private lives of citizens. To address this challenge, it is essential to establish explicit legislative frameworks to regulate the utilization of surveillance technologies, guarantee operational transparency, and impose stringent limitations on the collection, retention, and application of the acquired data. Ensuring adequate public and judicial oversight of law enforcement agencies' activity in this domain is likewise crucial (Cherniavskyi *et al.*, 2023).

The economic ramifications of data protection rules are considerable. On one side, stringent data protection regulations impose supplementary expenses on enterprises. B.D. Custers and G. Malgieri (2022) assert that the adoption of the GDPR has incurred substantial expenses for firms with the modification of business operations, employee training, and technological adjustments. They provide instances of organisations who have invested millions of euros in GDPR compliance. Conversely, C. Tikkinen-Piri *et al.* (2018) assert that the implementation of legislation like the GDPR may incentivize organisations to enhance their data management practices. A study by D. Marikyan *et al.* (2023) corroborates this, revealing that "companies that have successfully implemented GDPR requirements have demonstrated enhancements in data management and heightened customer trust, positively influencing their competitiveness". The researchers present instances of organisations that successfully leveraged GDPR compliance as a competitive advantage, particularly in industries with heightened sensitivity to privacy concerns, such as financial services and healthcare. The influence on innovation and research is another significant factor. The enactment of the GDPR has introduced new hurdles for healthcare researchers, particularly around data reutilization. This underscores the necessity of achieving equilibrium between safeguarding privacy and fostering scientific progress. Social justice and non-discrimination are also prominent aspects of data protection policy. R. Guay and K. Birch (2022) note that the different approaches to data governance in the US and EU reflect different socio-technical understandings of digital personal information, with implications for citizens' rights and social justice.

Discussion

The study's findings illustrate the intricate challenges of personal data protection within contemporary information and communication technology. In contrast to L.A. Bygrave's (2010) findings, which focused only on the legal aspects of data protection, the present study revealed deeper interconnections among technological, social, and ethical factors that affect the effectiveness of personal data protection. The research indicated that the implementation of GDPR in the EU has prompted a re-evaluation of strategies for preserving anonymity and privacy of personal data worldwide. Nonetheless, as highlighted by R. Crutzen *et al.* (2019), the execution of GDPR mandates presents significant obstacles for organisations, particularly with the transparency of data processing and the right to erasure.

An examination of Ukrainian legislation regarding the prevention of personal information disclosure indicates a progressive alignment with European standards, consistent with global trends. The conclusions about the significance of safeguarding the collective dimensions of personal data align with the findings of R. Mühlhoff and H. Ruschemeier (2024). Nevertheless, the current analysis revealed that the prevailing legislative frameworks are inadequately tailored to tackle this issue, particularly for artificial intelligence and big data technologies. This underscores the necessity to establish novel legal concepts and instruments to safeguard collective interests in personal data protection. The study's findings regarding the influence of citizens' trust on their propensity to reveal personal data corroborate the conclusions of D. Marikyan *et al.* (2023) and P. Trein and F. Varone (2023). Nonetheless, it was determined that this effect significantly fluctuates based on the cultural environment and the population's digital literacy degree. This highlights the necessity of formulating tailored strategies for data protection that consider the socio-cultural attributes of diverse cultures.

The study results illustrate the increasing significance of technology solutions in safeguarding against unauthorized access to personal information. U. Pagallo *et al.* (2019) observed that the middle-out strategy in data management system development facilitates a balance between centralised regulation and decentralised efforts. S. Bu-Pasha (2020) underscores the importance of doing a data protection impact assessment in the development of digital solutions for smart cities, particularly in light of increasing urbanization and the digital transformation of urban environments. The analysis of the role of synthetic data in privacy protection extends the findings of A. Beduschi (2024). It was found that while synthetic data does offer new opportunities for balancing innovation and privacy protection, its use poses new challenges in the area of data verification and validation that have not been sufficiently covered in previous studies. In contrast

to the studies by P. Christen and R. Schnell (2023), who focused on the technical aspects of population data protection, the present study revealed the significance of an interdisciplinary approach to healthcare data protection that would accommodate not only technical but also ethical and social aspects. This is crucial in the context of the growing role of telemedicine and personalised medicine.

The assertions made by A. Beduschi (2024) regarding the capacity of synthetic data to reconcile innovation with privacy protection appear contentious, given that the study identified considerable obstacles in the verification and validation of this data. The disparate interpretations may stem from A. Beduschi's (2024) emphasis on technical factors, whereas the present analysis incorporates legal and ethical dimensions regarding the utilization of synthetic data. The findings of R. Guay and K. Birch (2022) regarding the influence of various data management strategies on social justice are significant, revealing considerable disparities in personal data protection and the enforcement of data subjects' rights across different jurisdictions. In contrast to their study, the present research revealed that these discrepancies possess not only a socio-technical but also an economic dimension, influencing the competitiveness of firms in the global market.

This study analyses the GDPR's influence on international data transfers, building upon R. Romansky's (2022) results about transnational data protection collaboration. In contrast to their analysis, the current research indicates that the execution of GDPR standards presents legal, technical, and organisational problems for enterprises. This contradicts R. Romansky's (2022) results, as this investigation examines the practical implications of applying the GDPR within the business operations of international corporations. The disparate interpretations may stem from the study's reliance on a broader spectrum of empirical data, encompassing polls of corporate representatives. S. Lindroos-Hovinheimo's (2019) assertion regarding the necessity to enhance judicial oversight of special services' activities in the collection and processing of personal data is pertinent, as the findings of the current study indicate a significant risk of abuse associated with mass surveillance technologies. Nonetheless, the preceding research presents a contrasting perspective on the practical execution of such supervision. In contrast to the hopeful forecasts of S. Lindroos-Hovinheimo (2019), the investigation uncovered substantial impediments to effective judicial oversight, mostly arising from technological complexity and the necessity of safeguarding state secrets.

T. Naef's (2023) study on the equilibrium between data protection and international trade offers a significant viewpoint; yet, the analytical results present a contrasting scenario. Contrary to T. Naef's (2023) hopeful perspective on reconciling data protection and free commerce, the present investigation uncovered significant inconsistencies between both objectives, particularly for cross-border data transfer. The variance in interpretations may stem from this investigation addressing the real challenges firms encounter in adhering to diverse data protection frameworks globally. N. Purtova's (2018) conclusions concerning the broadening of the personal data concept in European law are highly pertinent, as this study's findings indicate that traditional definitions of personal data are increasingly inadequate in the context of big data and the Internet of Things. This study, in contrast to N. Purtova's (2018) emphasis on legal dimensions, underscored the necessity for an interdisciplinary approach to defining and safeguarding personal data, encompassing technological, ethical, and social considerations. R. Ayunda's (2022) assertion regarding the legal challenges of data protection in e-commerce is contentious, as the research indicates that data protection concerns extend well beyond mere legal considerations. This contradicts the findings of R. Ayunda (2022), which indicate that effective customer data protection in e-commerce necessitates a holistic approach encompassing legal, technological, economic, and educational strategies. The study highlights the importance of enhancing customer digital literacy and including privacy by design principles in the construction of e-commerce platforms.

Conclusions

This study analysed the equilibrium between safeguarding individuals' personal data and maintaining national security in the digital realm. This study aimed to find the most effective methods for achieving this equilibrium. The study examined the legal structures governing personal data protection in relation to the progression of artificial intelligence and big data analytics, namely within the EU, Ukraine, and the USA. A comparative analysis of the legal frameworks of various jurisdictions was conducted, judicial practices were examined, and the influence of technology advancements on data protection was assessed. Significant focus was directed towards examining the GDPR's influence on the establishment of international standards for personal data protection.

The study's findings suggest that effective personal data protection in modern contexts requires a comprehensive approach that includes legal, technological, and ethical components. The implementation of rigorous data privacy laws, like the GDPR, profoundly affects global trade and innovation, creating both challenges and prospects for businesses. The research underscored the necessity of balancing national security with the right to privacy, especially in relation to the use of mass surveillance technologies. The findings are crucial for understanding current challenges in personal data privacy and developing suitable policies in this area. They demonstrate the imperative for global standardization of data protection policies, considering the worldwide nature of the digital economy.

The study highlighted the increasing importance of an interdisciplinary approach to personal data protection. Effective solutions in this domain necessitate not only legal skill but also a comprehensive understanding of technological, social, and economic dimensions. The study identified the necessity to broaden the definition of personal data to include collective dimensions and indirect effects of data processing in the context of big data and the Internet of Things. This highlights the necessity for continual assessment and modification of legislation in response to emerging technical realities, as well as the importance of enhancing digital literacy among consumers and technology developers alike.

Potential avenues for further investigation in this domain encompass examining the ethical implications of employing artificial intelligence for personal data processing, advancing novel technologies for data anonymization and pseudonymization, exploring the psychological dimensions of privacy perception in the digital landscape, and assessing the influence of global crises on personal data protection policies.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Ayunda, R. (2022). Personal data protection to e-commerce consumer: What are the legal challenges and certainties? *Law Reform*, 18(2), 144-163. doi: 10.14710/lr.v18i2.43307.
[2] Bavarian Data Protection Act. (2018). Retrieved from https://www.gesetze-bayern.de/Content/Document/BayDSG.
[3] Beduschi, A. (2024). Synthetic data protection: Towards a paradigm change in data regulation? *Big Data & Society*, 11(1). doi: 10.1177/20539517241231277.
[4] BSA Global Privacy Best Practices. (2018). Retrieved from https://www.bsa.org/policy-filings/2018-bsa-global-privacy-best-practices.
[5] Bu-Pasha, S. (2020). The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city. *Information & Communications Technology Law*, 29(3), 391-402. doi: 10.1080/13600834.2020.1790092.
[6] Bygrave, L.A. (2010). Privacy and data protection in an international perspective. *Scandinavian Studies in Law*, 56(8), 165-200.
[7] California Civil Code. (2023). Retrieved from https://law.justia.com/codes/california/code-civ/.
[8] Charter of Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[9] Cherkassky, L. (2023). Incapacitous patients, assisted reproductive technology, and the importance of informed consent. *Legal Studies*, 43(4), 676-694. doi: 10.1017/lst.2023.10
[10] Cherniavskyi, S., Vozniuk, A., & Hribov, M. (2023). Legality of traditional techniques, means and modern technologies of visual surveillance. *Scientific Journal of the National Academy of Internal Affairs*, 28(1), 9-21. doi: 10.56215/naia-herald/1.2023.09.
[11] Christen, P., & Schnell, R. (2023). Thirty-three myths and misconceptions about population data: From data capture and processing to linkage. *International Journal of Population Data Science*, 8(1), article number 03. doi: 10.23889/ijpds.v8i1.2115.
[12] Commercial Law and Consumer Protection. (2023). Retrieved from https://law.justia.com/codes/alabama/title-8/chapter-38/.
[13] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1981, January). Retrieved from https://rm.coe.int/1680078b37.
[15] Crutzen, R., Ygram Peters, G.J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, 34(11), 1347-1357. doi: 10.1080/08870446.2019.1606222.
[16] Custers, B., & Malgieri, G. (2022). Priceless data: Why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45, article number 105683. doi: 10.1016/j.clsr.2022.105683.
[17] Decision of the National Security and Defence Council of Ukraine "On the National Security Strategy of Ukraine". (2020). Retrieved from https://zakon.rada.gov.ua/laws/show/n0005525-20#n2.
[18] Dom, R., Custers, A., Davenport, S., & Prichard, W. (2022). *Innovations in tax compliance: Building trust, navigating politics, and tailoring reform*. Washington: International Bank for Reconstruction and Development.
[19] Federal Data Protection Act of Germany. (2021, June). Retrieved from https://www.gesetze-im-internet.de/englisch_bdsg/.
[20] GDPR. (2016, May). Retrieved from https://gdpr-info.eu/.
[21] Gramm-Leach-Bliley Act. (1999, November). Retrieved from https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act.
[22] Guay, R., & Birch, K. (2022). A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008-2016). *Big Data & Society*, 9(2). doi: 10.1177/20539517221112925.
[23] HIPAA Administrative Simplification. (2013, March). Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.
[24] IAPP-EY annual privacy governance report. (2019). Retrieved from https://f.hubspotusercontent20.net/hubfs/525875/IAPP_EY_Governance_Report_2019.pdf.
[25] Investigatory Powers Act. (2016, October). Retrieved from https://www.legislation.gov.uk/ukpga/2016/25/contents.
[26] Judgment of European Court of Human Rights in Cases Nos. 58170/13, 62322/14 i 24960/15 "Big Brother Watch and Others v. the United Kingdom". (2021, May). Retrieved from https://privacy.khpg.org/1604922631.
[27] Kennett, D. (2019). Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes. *Forensic Science International*, 301, 107-117. doi: 10.1016/j.forsciint.2019.05.016.
[28] Kovalenko, Y. (2022). The right to privacy and protection of personal data: Emerging trends and implications for development in jurisprudence of European Court of Human Rights. *Masaryk University Journal of Law and Technology*, 16(1), 37-58. doi: 10.5817/MUJLT2022-1-2.
[29] Kravchenko, L. (2022). Observance of the constitutional rights and freedoms of man and citizen during surveillance. *Law Journal of the National Academy of Internal Affairs*, 12(2), 72-78. doi: 10.56215/04221202.72.
[30] Kyrychok, A., Harbuza, T., Teslenko, N., Okhrimenko, O., & Zaliznyuk, V. (2024). Training civil servants in promoting the reputation of the country in the settings of crisis communication. *Teaching Public Administration*, 42(3), 376-399. doi: 10.1177/01447394231191928.
[31] Law of Sweden No. 2018/218 "On the Protection of Data". (2018). Retrieved from https://www.government.se/government-policy/the-constitution-of-sweden-and-personal-privacy/act-containing-supplementary-provisions-to-the-eu-sfs-2018218-general-data-protection-regulation/.

[32] Law of Ukraine No. 2297-VI “On the Protection of Personal Data”. (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[33] Law of Ukraine No. 2657-XII “On Information”. (1992, October). Retrieved from https://tax.gov.ua/dlya-gromadskosti/dpa-i-gromadskist/normativno-pravova-baza-u-sferi/arhiv-normativno-pravova-baza/53366.html.
[34] Law of Ukraine No. 5492-VI “On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identity or Special Status”. (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/5492-17#Text.
[35] Law of Ukraine No. 580-VIII “On the National Police”. (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19#Text.
[36] Lella, I., Theocharidou, M., Tsekmezoglou, E., Svetozarov Naydenov, R., Ciobanu, C., Malatras, A., & Theocharidou, M. (2022). *ENISA threat landscape*. Athens: European Union Agency for Cybersecurity.
[37] Lindroos-Hovinheimo, S. (2019). Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*. *Information & Communications Technology Law*, 28(2), 225-238. doi: 10.1080/13600834.2019.1623447.
[38] Marikyan, D., Papagiannidis, S., Rana, O.F., & Ranjan, R. (2023). General data protection regulation: A study on attitude and emotional empowerment. *Behaviour & Information Technology*. doi: 10.1080/0144929X.2023.2285341.
[39] Mazepa, S., & Bratasyuk, O. (2023). Ensuring information security in Ukraine – Administrative and criminal law measures. *OER Osteuropa Recht*, 68(4), 421-442. doi: 10.5771/0030-6444-2022-4-421.
[40] Mühlhoff, R., & Ruschemeier, H. (2024). Predictive analytics and the collective dimensions of data protection. *Law, Innovation and Technology*, 16(1), 261-292. doi: 10.1080/17579961.2024.2313794.
[41] Naef, T. (2023). *Data protection without data protectionism: The right to protection of personal data and data transfers in EU law and international trade law*. Cham: Springer. doi: 10.1007/978-3-031-19893-9.
[42] National Security Strategy. (2022, October). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.
[43] Pagallo, U., Casanovas, P., & Madelin, R. (2019). The middle-out approach: Assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. *The Theory and Practice of Legislation*, 7(1), 1-25. doi: 10.1080/20508840.2019.1664543.
[44] Podoprigora, R., Apakhayev, N., Zhatkanbayeva, A., Baimakhanova, D., Kim, E.P., & Sartayeva, K.R. (2019). Religious freedom and human rights in Kazakhstan. *Statute Law Review*, 40(2), 113-127. doi: 10.1093/slr/hmx024.
[45] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40-81. doi: 10.1080/17579961.2018.1452176.
[46] Regulation of the European Parliament and of the Council No. 2016/679 “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)”. (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[47] Romansky, R. (2022). Digital age and personal data protection. *International Journal on Information Technologies & Security*, 14(3), 89-100.
[48] Spytska, L. (2023). Social and psychological features of affective disorders in people during crisis periods of life. *Society Register*, 7(4), 21-36. doi: 10.14746/sr.2023.7.4.02.
[49] The CJEU judgment in the Schrems II case. (2020). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.
[50] The Data Protection Act of France. (2015, January). Retrieved from https://www.cnil.fr/fr/la-loi-informatique-et-libertes.
[51] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. doi: 10.1016/j.clsr.2017.05.015.
[52] Trein, P., & Varone, F. (2023). Citizens’ agreement to share personal data for public policies: Trust and issue importance. *Journal of European Public Policy*, 31(9), 2483-2508. doi: 10.1080/13501763.2023.2205434.
[53] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[54] Yudina, S., Lysa, O., Razumova, H., Oskoma, O., & Halahanov, V. (2024). Management and administration of financial resources using digital technologies. *Scientific Bulletin of Mukachevo State University. Series “Economics”*, 11(1), 92-102. doi: 10.52566/msu-econ1.2024.92.

Захист персональних даних: між дотриманням прав людини та національною безпекою

Світлана Хаджирадєва

Доктор наук з державного управління, професор
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0000-0002-2256-2579

Тетяна Безверхнюк

Доктор наук з державного управління, професор
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0000-0002-2567-8729

Олександр Назаренко

Кандидат фізико-математичних наук, ректор
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0000-0002-0187-0791

Сергій Базика

Кандидат наук з державного управління, голова наглядової ради
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0009-0003-2081-1222

Тетяна Доценко

Доктор філософії, доцент
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0000-0003-3553-1314

Анотація. Метою цього дослідження було встановити баланс між захистом персональних даних громадян та підтриманням національної безпеки в цифровому світі. У дослідженні було проаналізовано нормативно-правову базу та судову практику Європейського Союзу (ЄС), України та США за допомогою декількох методологій. Законодавство ЄС пропонує найсуворіший захист персональних даних, передбачаючи значні штрафи за порушення. Українське законодавство поступово наближається до європейських стандартів, однак процедури захисту та відповідальності потребують вдосконалення. Дослідження показало зростаючу тенденцію до використання штучного інтелекту та технологій великих даних у сфері національної безпеки, що створює нові проблеми для захисту персональних даних від розголошення. У дослідженні вивчалися етичні наслідки використання таких технологій та їхній потенційний вплив на приватне життя громадян. У дослідженні проаналізовано глобальні регуляторні процедури, зосереджуючи увагу на підході Європейського суду з прав людини до збалансування цілей захисту особистої інформації та національної безпеки. Дослідження виявило необхідність розширити визначення персональних даних, включивши до нього комунальні виміри та непрямі наслідки обробки даних у контексті великих даних та Інтернету речей. Результати дослідження підкреслюють важливість міждисциплінарного підходу до безпеки персональних даних, що охоплює правові, технологічні, етичні та соціальні аспекти. Аналіз представив концептуальну модель гармонізації нормативно-правової бази для захисту привілейованої інформації, включаючи сучасні технічні проблеми та вимоги національної безпеки. Дослідження має практичне значення для вдосконалення нормативно-правової бази щодо захисту персональних даних і може допомогти у формулюванні планів інформаційної безпеки

Ключові слова:конфіденційність; кібербезпека; інформаційна етика; приватне життя; прозорість даних