OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 16, Nº. 2, TD3
Thematic Dossier
Rule of Law, Human Rights, and Institutional
Transformation in Times of Global and National Challenges
March 2026

JANUS.NET
e-journal of International Relations

PERSONAL DATA SOVEREIGNTY IN THE DIGITAL AGE: A COMPARATIVE ANALYSIS OF GLOBAL AND DOMESTIC REGULATORY FRAMEWORKS

LIDIIA MOSKVYCH
moskvichlida@gmail.com
Doctor of Law, Associate Professor of the Department of Criminal Procedure
Faculty of Prosecutor's Office Yaroslav Mudryi National Law University
Kharkiv (Ukraine) https://orcid.org/0000-0001-7339-3982

KHRYSTYNA KMETYK-PODUBINSKA
khrystyna.kmetyk@lnu.edu.ua
PhD (Juridical Sci.), Associate Professor on Intellectual Property, Information and Corporate Law
Department Faculty of Law, Ivan Franko National University of Lviv
Lviv (Ukraine) https://orcid.org/0000-0002-6572-7134

OLEKSANDR DYAKOVSKIY
o.dyakovskiy@gmail.com
PhD (Legal Sci.), Lecturer of the Department of Information, Economic and Administrative Law
National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute"
Kyiv (Ukraine) https://orcid.org/0000-0003-3412-9278

MAKSYM TERELA
academy_knowledge@meta.ua
PhD Student at the Department of Constitutional and Administrative Law
Zaporizhzhia National University Zaporizhzhia (Ukraine) https://orcid.org/0000-0002-7033-4765

VIKTORIIA SYDORENKO
lawnanu@gmail.com
PhD (Juridical Sci.), Associate Professor of the Department of Information, Economic and
Administrative Law Faculty of Sociology and Law National Technical University of Ukraine "Igor
Sikorsky Kyiv Polytechnic Institute" Kyiv Ukraine https://orcid.org/0000-0002-2787-9102

Abstract

In today's society, the number of companies collecting and processing personal data is growing, which poses a threat to the security of confidentiality and the security of the human right to privacy. That is why the role of legislative regulation of data privacy protection is growing. The study aimed to compare domestic legislative documents with European and American norms in personal data protection and to identify trends in the country's legal regulation of data privacy. It used bibliographic, induction-deduction, quantitative-comparative, trend, comparative-logical and graphical methods to achieve this goal. The results revealed the need to improve regulatory documents on personal data protection, especially for users of Internet resources. The problem of regulations exists in both Ukrainian and international law. The study has revealed similarities between the basic principles of the Law of Ukraine and the GDPR, but the liability in Ukraine is less than in Europe. A growing trend has been identified: in recent years, the number of court decisions on violations of personal data protection has increased significantly, and according to statistical forecasts, it will continue to grow. At the same time, the structure of court decisions showed that administrative, civil and criminal decisions predominate among the decisions. Hence, most cases relate to disseminating and processing data by public services.

Keywords

Law of Ukraine, personal data, confidentiality, privacy protection, consumer privacy, trends, court decisions.

Resumo

Na sociedade atual, o número de empresas que recolhem e processam dados pessoais está a crescer, o que representa uma ameaça à segurança da confidencialidade e ao direito humano à privacidade. É por isso que o papel da regulamentação legislativa da proteção da privacidade de dados está a crescer. O estudo teve como objetivo comparar documentos legislativos nacionais com normas europeias e americanas em matéria de proteção de dados pessoais e identificar tendências na regulamentação legal do país em matéria de privacidade de dados. Para atingir esse objetivo, foram utilizados métodos bibliográficos, de indução-dedução, quantitativos-comparativos, de tendências, comparativos-lógicos e gráficos. Os resultados revelaram a necessidade de melhorar os documentos regulamentares sobre a proteção de dados pessoais, especialmente para os utilizadores de recursos da Internet. O problema da regulamentação existe tanto no direito ucraniano como no direito internacional. O estudo revelou semelhanças entre os princípios básicos da Lei da Ucrânia e o RGPD, mas a responsabilidade na Ucrânia é menor do que na Europa. Foi identificada uma tendência crescente: nos últimos anos, o número de decisões judiciais sobre violações da proteção de dados pessoais aumentou significativamente e, de acordo com as previsões estatísticas, continuará a crescer. Ao mesmo tempo, a estrutura das decisões judiciais mostrou que as decisões administrativas, civis e criminais predominam entre as decisões. Portanto, a maioria dos casos está relacionada com a divulgação e o processamento de dados por serviços públicos.

Palavras-chave

Lei da Ucrânia, dados pessoais, confidencialidade, proteção da privacidade, privacidade do consumidor, tendências, decisões judiciais.

How to cite this article
Moskvych, Lidiia, Kmetyk-Podubinska, Khrystyna, Dyakovskiy, Oleksandr, Terela, Maksym & Sydorenko, Viktoriia (2026). Personal Data Sovereignty in the Digital Age: A Comparative Analysis of Global and Domestic Regulatory Frameworks. *Janus.net, e-journal of international relations*. Thematic Dossier - Rule of Law, Human Rights, and Institutional Transformation in Times of Global and National Challenges, VOL. 16, Nº. 2, TD3, March 2026, pp. 210-225. https://doi.org/10.26619/1647-7251.DT0226.11

Article submitted on 25 November 2025 and accepted for publication on 23 December 2025.

PERSONAL DATA SOVEREIGNTY IN THE DIGITAL AGE: A COMPARATIVE ANALYSIS OF GLOBAL AND DOMESTIC REGULATORY FRAMEWORKS

LIDIIA MOSKVYCH

KHRYSTYNA KMETYK-PODUBINSKA

OLEKSANDR DYAKOVSKIY

MAKSYM TERELA

VIKTORIIA SYDORENKO

Introduction

In the era of technological progress, when digitalisation is being introduced into all industries and areas of activity, the issue of personal data protection deserves special attention. As personal data is used for various processes, every citizen has the right to protect personal data that may be misused. Today, the data that needs to be protected includes the confidentiality of consumer information, financial transactions, biometric data, health, education, and employment (Solove & Schwartz, 2020). Personal data protection legislation varies from country to country, but it is important because it can even threaten national security.

Despite the regulatory documents in the field of personal data privacy, there is a problem with their protection and confidentiality. Moreover, the threat of violating citizens' rights to their data security has been growing in recent years. This is due to technological progress and the increasing data distribution in the digital space among various industries. As a result, the cybersecurity system cannot fully control the protection of personal data, which individuals or companies mainly use.

Aim

The work aimed to compare domestic legislative documents with European and American standards in personal data protection and to identify trends in the legal regulation of data privacy in Ukraine. To achieve this goal, the study set the following objectives: to compare the Law of Ukraine on Personal Data Protection with the European Union's General Data Protection Regulation (GDPR) and the US California Consumer Privacy Act (CCPA); to assess the effectiveness of the application of the Law of Ukraine in practice by analysing the number of court decisions of the Unified State Register of Court Decisions; to forecast changes for the next 5 years based on the analysis of trends in the number of court decisions from 2010 to 2024 with the query "personal data protection"; to study the structure of court decisions on violation of the CCPA.

Literature review

Today, people actively use information technologies, such as social networks and online shopping sites, in their daily lives. At the same time, the growing digitalisation of the economy has led to low personal data protection and privacy (Aljeraisy et al., 2021). Social media and e-commerce site developers deal with sensitive data that needs to be protected from a human rights perspective. Thus, information technology legislation aims to protect data privacy while being linked to substantive and criminal justice (Lloyd, 2020; Baranovska, 2024). A threatening area of digitalisation is digital identification through face recognition. Although this step towards creating a digital ecosystem increases the possibilities of electronic services for the population in the country, it brings new challenges to protecting information privacy (Bulgakova & Bulgakova, 2023).

One of the challenges to data privacy protection is using artificial intelligence, which can carry risks of information leakage (Zhukevych, 2024). Makedon et al., 2020) highlights the risk of big data leakage of patients' health information from healthcare facilities. AI programmes are in the hands of individuals who cannot ensure high personal data protection. The leakage of such information can pose a threat related to de-identification and anonymisation, which, when applied to certain AI algorithms and techniques, can pose risks, especially for patients under private care. Concerns about the security of medical data have also increased with the widespread use of mHealth applications by people with various diseases, as the applications contain different software and may carry risks of data leakage (Nurgalieva et al., 2020).

In general, the issue of health data privacy is regulated in the United States by the Food and Drug Administration (FDA) and the Health Insurance Portability and Accountability Act (HIPAA), which emphasises the confidentiality of health data. However, recent studies have criticised these documents for excessive access to data (Arora, 2019). Instead, the European Union's General Data Protection Regulation (GDPR) adopted in 2018 in Europe and the California Consumer Privacy Act (CCPA) adopted in 2020 in the United States have become new regulatory documents that regulate the activities of online services and healthcare organisations. These documents protect the right of consumers to know how and where their information is collected, to whom it is shared, and by whom it may be used (Zuraw & Sklar, 2020). However, these two regulations differ in their approaches to personal data protection. The European model focuses on data protection in all areas by default, i.e., when collecting, processing and transmitting data of any kind, obtaining permission to use personal data is necessary (Hrytsak et al., 2025; Yermachenko et al., 2023).

The California model is based on a sectoral approach, meaning that it is regulated differently depending on the area of activity - medical, financial, educational, or commercial. Moreover, in the California model, data can be used at the discretion of the data collector unless prohibited by the personal data owner and other rules (Chander et al., 2020). From this point of view, citizens should be aware of their data protection issues. For this purpose, the authors recommend simplifying control over the circulation of consumers' data by creating icons and links in applications that would allow consumers to quickly refuse to sell or transfer their data to companies (Habib et al., 2021).

The privacy violation of medical data obtained from fitness bracelets and various applications for monitoring patient health remotely in outpatient settings has prompted the creation of legislative documents in various states. For example, in 2023, the Washington My Health My Data Act, New York State Assembly Bill 2023-A3007C, and other federal laws, such as Nevada's Consumer Health Data Privacy Act, Connecticut Data Privacy Act, California Confidentiality of Medical Information Act, came into force, which prohibit geofencing within 1,750 feet of any healthcare facility, that may be of interest to the consumer and prohibiting the use of any data from medical devices about a person's health status by third parties for marketing products or facilities that meet the health needs of users (Steffen, 2024).

That is why important aspects of legal regulation of artificial intelligence in cybersecurity are transparency and clarity of algorithms, protection of data privacy, and avoidance of injustice and bias (Rodrigues, 2020). The authors also emphasise the need for continuous improvement of artificial intelligence technologies, and to strengthen the legal context, they recommend improving accountability and liability for the possibility of harmful impact. After all, more companies are using personal data, even though only one was granted access. This indicates that users are unaware of the possibility of their data being sold, hacked or leaked to third parties that may pose a real threat. Moreover, various modern devices, from thermostats to fitness bracelets and social media to dating apps, pose a danger (Klosowski, 2021).

The issue of protecting consumers' data has become increasingly important as a result of the growing use of digital technologies. Accordingly, companies collect consumer data to identify business weaknesses, personalise advertising, and improve the quality of services. Companies can request customers' locations and receive personal data about consumers, which must be protected from hacking, information leaks, and privacy violations. Thus, businesses face a new challenge of increasing responsibility for consumer data security. As for consumers, surveys indicate that users have low confidence in the ability of companies to store their data, so they try to provide minimal information about themselves. Moreover, consumers are more likely to choose companies with a good reputation for protecting their personal data and customer base (Anant et al., 2024). Another aspect is the database of big data collected by artificial intelligence from comments, transactions, and physical movements, which should ensure privacy based on guarantees of compliance with data privacy laws, anonymisation, and pseudonymisation. Such an approach will not improve data protection in general but will only reduce risks based on compliance with the GDPR as the gold standard for cybersecurity (Andrew & Baker, 2021).

Another aspect is regulating data collection from vulnerable populations, namely children who actively use digital technologies and are unaware of the risks of providing personal data. In order to protect the data of children under 13, the Children's Online Privacy Protection Act (COPPA) was developed, which requires mandatory parental or guardian permission to collect data from children under 13. At the same time, there is little research on children's media literacy and the harms associated with data privacy violations on the Internet (Stoilova et al., 2021).

The issue of data privacy has become more acute with the onset of the COVID-2019 pandemic, which has increased the level of digital unfreedom in the interests of public health. After the pandemic, the appropriateness of such restrictions was rejected, so the focus was on initiating digital freedom, which includes control over personal information, protection from surveillance, respectful treatment of personal data and the right to bodily autonomy (Małagocka, 2024; Makedon et al., 2024). The pandemic has also led to a significant increase in remote economic activity, resulting in a growing amount of data in the digital environment. The industry has appreciated the benefits of changing the activity vector according to demand based on behavioural analysis and personal preferences. Thus, the industry's desire to acquire more data has led to risks of misuse, which violates the principles of democracy and hurts the emotional health of the population (Hartzog & Richards, 2020).

After analysing the literature, it was found that personal data protection is relevant due to the growing level of digitalisation in society (Petrovich, 2025; Rosales, 2025; Ilychok et al., 2023). This has led to the search for new legal documents and the improvement of existing ones to ensure the protection of privacy and confidentiality of information. Nevertheless, the existing regulatory laws and acts do not show significant effectiveness, encouraging a detailed analysis of the existing legal documents on personal data protection.

Methodology

To achieve the objectives, the study used the bibliographic, induction-deduction, and logical comparison methods to reveal the main provisions of the legislative documents of the Law of Ukraine on Personal Data Protection, the European Union's General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). A graphical method to visualise the results of the analysis of the Unified State Register of Court Decisions for the query "personal data protection" from 2010 to 2024 was applied. The trend analysis is used to identify trends in court decisions in personal data protection and forecast them. The research analyses the structure of court decisions in personal data protection cases from 01.01.2024 to 05.12.2024 by the form of proceedings.

Results

In Ukraine, personal data protection is regulated by the Law of Ukraine On Personal Data Protection No. 2297-VI dated 01.06.2010. The law regulates the processing of personal data in automatic and non-automatic modes, which is aimed at preserving the rights and freedoms of individuals to privacy. Comparing the main provisions of the Ukrainian law and the GDPR, we found standard features of the universality of the law, which applies to all industries. At the same time, the CCPA is concerned with protecting the personal data of buyers and users of websites. The main differences between the Law of Ukraine on Personal Data Protection, the GDPR and the CCPA are presented in the table below.

As can be seen from the table, the Law of Ukraine has many similarities with the GDPR, is universal and has many restrictions. Nevertheless, the law does not contain any provisions for the processing of data of vulnerable citizens, such as children and people with disabilities. The European and Ukrainian regulations apply to companies and do not consider the threats of online data collection. At the same time, the California document focuses on data collection in the online space, which requires increased attention in the current environment. California's law is more concise and easier to understand for consumers, with the primary goal of making consumers aware of the dangers of the misuse of personal data and the ability to influence the dissemination and use of data through a simplified procedure. The laws also differ in terms of their scope. The Ukrainian law applies to companies operating in Ukraine and using citizens' data, while the GDPR applies in the EU and beyond if companies operate within the EU. The GDPR is universal and binding for EU member states, but in addition to the provisions of this regulatory document, the internal laws of EU member states are taken into account. The data protected by law differs. Ukrainian legislation, for example, has a longer list of data that is publicly available due to the operation of laws on corruption and tax violations. Ukrainian and European legislation provides for restrictions on biometric, ethnic, religious, and socio-cultural data, while the California Act has no such restrictions. The degree of liability also differs, which is more straightforward and transparent in the California document. At the same time, the European and Ukrainian laws require lengthy proceedings and the possibility of hefty fines. In general, these three documents have a common goal of preserving the human right to privacy, but they need to be improved, as they do not provide adequate protection (Makedon et al., 2025).

In this study, we analysed the status of court cases requesting "personal data" and determined their dynamics and structure. To achieve the goals, we reviewed cases in the Unified State Register of Court Decisions, which is publicly available. Figures 1 and 2 present the dynamics and trend of the number of court decisions for the period 2010-2024.

As can be seen from the figures, since adopting the Law on Personal Data Protection, the number of court decisions requesting "personal data protection" has increased yearly, indicating a positive experience of applying the law. We analysed the trend of changes in the number of court decisions for 2010-2024 with the request for "personal data protection". We found an increase in a polynomial relationship with a probability of further growth of R=0.9388 for the next 5 years.

Table 1. Key features of the Law of Ukraine on Personal Data Protection, GDPR and CCPA

Characteristics	**The Law of Ukraine on Personal Data Protection**	**General Data Protection Regulation**	**California Consumer Privacy Act**
The document applies to	Companies that collect and process personal data, including the owner, manager of personal data and a third party. The law does not apply to individuals acting for personal, journalistic, or creative purposes that do not violate the rights to respect for privacy and freedom of opinion.	All companies and institutions operating within the European Union, except those that process data for criminal, administrative liability and public order protection. It does not apply to an individual who carries out activities to meet personal or household needs.	Social networks, brokerages, and large companies collect the personal data of Californian residents. Companies that collect information from at least 50,000 California residents or businesses Companies with annual gross revenue exceeding $25 million Companies that receive 50% of annual revenue comes from the sale of personal data of Californian residents. California residents, even if they are located in other states. Persons who are temporarily or transiently in the state.
Legally regulated and restricted data	Data containing information with confidential content. The data specified in the declaration of a person performing the functions of state administration and local self-government, including the receipt of state funds and official property, are not included. The data of persons with tax debts are also excluded. The data on religion, race, ethnicity, biometric, genetic, and ideological data are subject to restrictions.	Name Identification number Location. Economic, social, political, cognitive, behavioural, and physiological factors can directly or indirectly identify a person. Data is subject to restriction: Religion Ethnicity Sexual preferences Biometric data Genetic characteristics	Names, pseudonyms Postal addresses Accounts Social insurance policy Passport details Driving licence Biometric data Geolocation Purchase history Information on education that is not public Information about employment
Consent to the processing and sale of personal data	It is mandatory to indicate the purposes of data collection and processing. If the purposes change, the subject's consent is required. Without consent, data may be processed for the purposes of national security, economic well-being, and human rights.	Required by default. Consent must be in a separate document written in clear language. The subject has the right to withdraw consent at any time. Children under the age of 16 must provide permission from a parent or guardian.	It is not required except for minors over 13 years of age. Parental or guardian permission is required for children under 13.
Special features	The law provides for the right to request information on the processing of personal data within 30 days, to request the destruction or modification of one's data, and to withdraw consent to data processing.	Processing security is provided, which includes data encryption, the use of pseudonyms, the ability to recover data after technical errors, and periodic checks of technical equipment.	Ability to prohibit the sale of personal data in one click

Responsibility	The Ukrainian Parliament Commissioner for Human Rights and the courts control the law's implementation. Based on complaints or notifications, the Commissioner has the right to inspect personal data owners or managers, with the possibility of prohibiting the processing of personal data or imposing administrative liability in case of violations.	The severity, specificity, level of damage and duration of the damage impose the amount of the administrative fine. In case of violation of the duties of a controller, operator, monitoring or certification body, the fine may not exceed EUR 10 million or 2% of the company's annual revenue. For other violations, including consent violations, subject rights, and data transfers to a third party or country outside the EU, a fine of up to EUR 20 million or 4% of the firm's annual revenue is provided.	From $100 to $750 per consumer for a data breach that caused damage. USD 2,500 for an unintentional breach. 7500 USD fine for intentional violation

Source: compiled by the author based on the Law of Ukraine on Personal Data Protection, GDPR, CCPA.

This trend emphasises, on the one hand, the importance of the law and its effectiveness and, on the other hand, the growing demand of citizens for the protection of their data and awareness of their rights. Additional analysis of court practice in the field of personal data protection indicates the need not only for quantitative measurement, but also for in-depth qualitative interpretation of the decisions adopted, since it is the content of the courts' legal positions that allows assessing the real effectiveness of legislative norms and identifying existing gaps. In particular, a number of administrative cases have revealed a tendency toward broad interpretation of the powers of state bodies in accessing personal data, which sometimes leads to restrictions on an individual's right to privacy. In civil disputes, there is often a low level of public awareness of protection mechanisms, which indicates a need to improve digital literacy. In criminal proceedings, a key problem is the lack of established practice in applying sanctions for the illegal dissemination of personal information.

In order to determine which articles of the Law on Personal Data Protection appear in court decisions most often, we analysed the structure of court decisions depending on the form of proceedings in 2024. The structure is shown in Figure 3. As can be seen from the graph, the most frequent decisions concerned administrative, civil and criminal proceedings. Civil and administrative rulings mainly concerned the request for personal data by public authorities, including social services and border services. There were also lawsuits against the migration service regarding the change of personal data. Criminal cases also concerned law enforcement agencies' requests for personal data under Articles 14 and 16.

Figure 1. Court cases with a request for the Law on Personal Data Protection

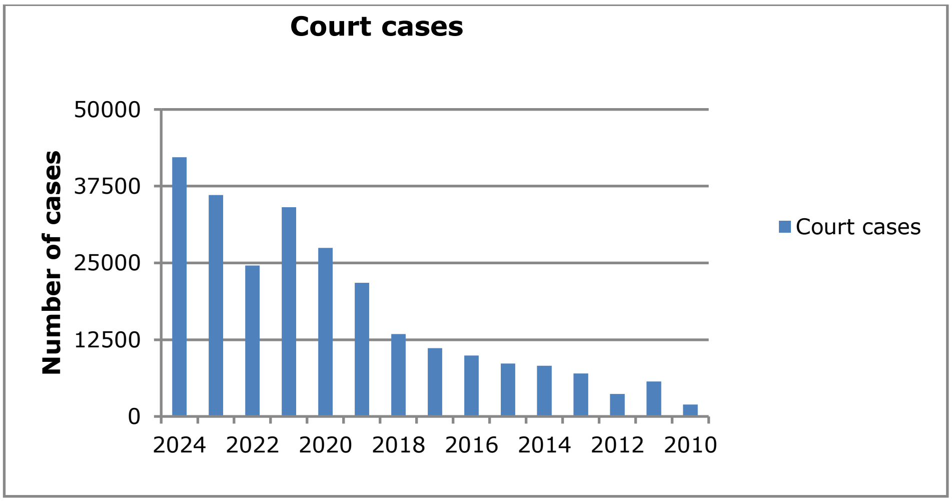
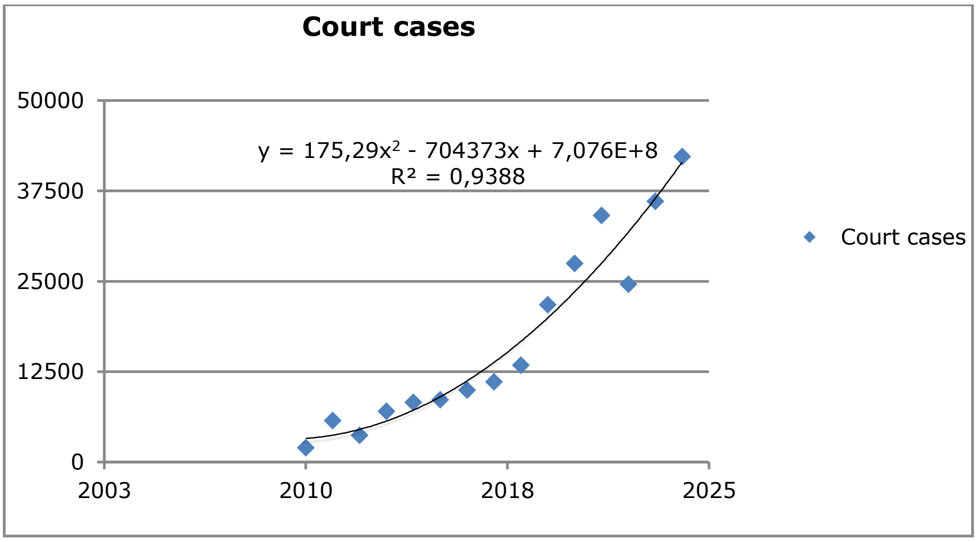
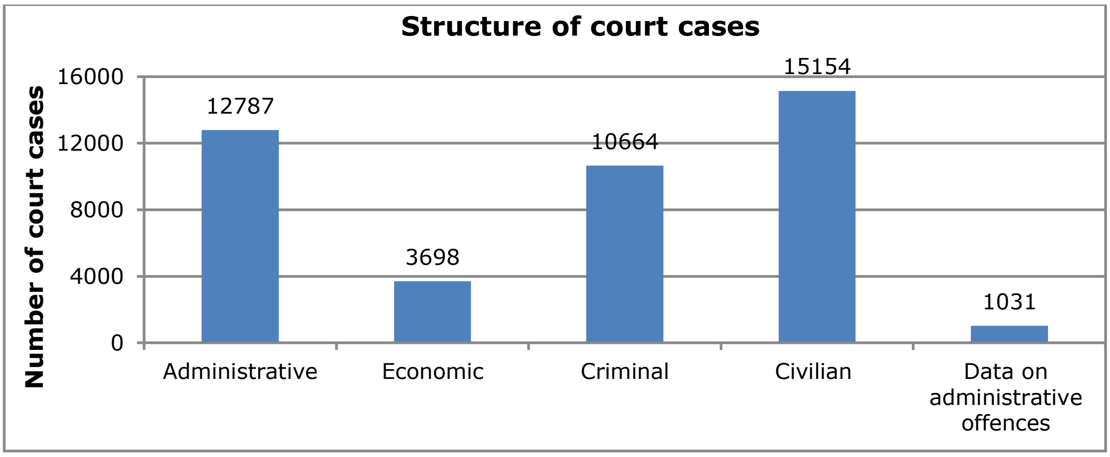


Figure 2. Dynamics of court cases with a request for the Law on Personal Data Protection



A systematic review of the impact of new technologies on the legal regulation of personal data protection highlights a number of fundamental challenges. The use of artificial intelligence in the processing of large amounts of information creates the risk of automated decision-making without proper control and transparency of algorithms, which can lead to discriminatory practices and violations of the principles of fairness. Biometric technologies, in particular facial and fingerprint recognition, pose a new level of threat, as unlike passwords or codes, such data cannot be changed in the event of a leak. The Internet of Things complicates legal regulation, as billions of devices collect sensitive information about users' behavior and health, which goes beyond the traditional approach to personal data.

Figure 3. Structure of court cases by form of proceedings



The research has revealed the need to improve regulatory documents on personal data protection. The number of companies collecting personal data is growing. The problem of legislation in this area concerns both Ukrainian and international law. Analysing the Law of Ukraine and modern European and American regulatory documents revealed more remarkable similarities with European norms. However, the responsibility in Ukraine is less than in Europe. Nevertheless, the number of court decisions on personal data protection violations has increased significantly in recent years, and according to statistical forecasts, it will continue to grow. Most cases relate to the dissemination and processing of data by public services, which still indicates low public confidence in the law. However, the threats to citizens are increasing in online information collection.

It should also be emphasized that qualitative analysis of judicial practice in the field of personal data protection is no less important than quantitative tracking of trends, as it allows for the identification of underlying problems in law enforcement and contradictions in the interpretation of norms. A study of specific legal positions of courts demonstrates a low level of unification of approaches, which necessitates the harmonization of national legislation with European standards. Such an approach will contribute to improving the effectiveness of law enforcement practices and lay the foundation for Ukraine's full integration into the digital legal space of the European Union.

Discussions

This research has revealed similarities between the personal data protection laws of Ukraine and the EU, but in the digital age, the legal innovations of the California Act are relevant. As the risks for users of social networks and websites are increasing. Balai and Horlopolov (2024) emphasised the increase in the amount of data processed due to the growing role of digitalisation in the economy. The authors also emphasised the importance of digital analytics, namely Privacy-Centred Analytics, for securely processing users' data in compliance with legal regulations. Padden and Öjehag-Pettersson (2024) identified three threats of digitalisation to personal data: threats to elections through manipulation, discrimination through automated decision-making, and threats to democracy through pervasive surveillance. The authors emphasised the imperfections of the GDPR in regulating profiling and the anti-democratic digitalisation model. Numerous studies have focused on the threats to data processing, online transactions, the risk of data breaches, and inadequate privacy policies (Mannan, 2024).

Having analysed the number of court decisions requesting personal data protection, we found a progressive increase in cases that testify to applying this law and its active implementation in public life. Docksey and Hijmans (2019) emphasised the importance of court decisions as a factor of influence on society, which stimulates action within the framework of this law, using the example of three high-profile cases of violations of personal data protection: Digital Rights Ireland, Google Spain and Schrems. Having determined the structure of decisions by the form of proceedings, we found that the Law of Ukraine "On the Personal Data Protection" is used mainly by state authorities to ensure public order, justice, and social standards is used mainly by state authorities to ensure public order, justice, and social standards (Varenia, 2024). At the same time, they found a low number of decisions on violating individuals' data, including on social networks and the Internet. In the literature, the authors also emphasise the low level of coverage of personal data rights violations on the Internet, namely the lack of mechanisms to influence the Internet of Things (Karale, 2021). The authors also emphasise the lack of effectiveness of existing legislative initiatives, namely the Electronic Communication Privacy Act, the Health Insurance Portability and Accountability Act, and the Fair Information Practice Principles, and recommend the creation of new laws to implement the protection of personal data of Internet users. Another aspect of the imperfection of privacy laws is the requirement to prove harm in court, which reduces liability for violations of rights (Citron & Solove, 2022).

Conclusions

This research has revealed the relevance of personal data protection and the need to improve legislation. When comparing the Ukrainian Law on Personal Data Protection, we found similarities with the European GDPR, which consisted of the universality of the law, the requirement of consent to the processing of personal data by default, the data to be protected and the approach to liability. Instead, the study found a low level of effectiveness of personal data protection on the Internet, which could be improved by applying some provisions of the CCPA. The article reveals an increase in the number of court decisions on personal data protection requests in Ukraine in recent years. However, the structure of court decisions is dominated by criminal, administrative and civil cases, which mostly request personal data in the interests of public authorities.

Funding

This research received no external funding.

Conflicts of Interests

The authors declare no conflict of interest.

References

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2021). Privacy laws and privacy by design schemes for the Internet of things: A developer's perspective. *ACM Computing Surveys (CSUR), 54*(5), 1–38. https://doi.org/10.1145/3450965

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. McKinsey & Company. https://www.mckinsey.com/uk/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20consumer%20data%20opportunity%20and%20the%20privacy%20imperative/The-consumer-data-opportunity-and-the-privacy-imperative.pdf

Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics, 168*, 565–578. https://doi.org/10.1007/s10551-019-04239-z

Arora, C. (2019). Digital health fiduciaries: Protecting user privacy when sharing health data. *Ethics and Information Technology, 21*(3), 181–196. https://doi.org/10.1007/s10676-019-09499-x

Balai, N., & Hordopolov, V. (2024). Digital analysis in the company's information security system. *Journal of the Balkan Tribological Association, 30*(5). https://openurl.ebsco.com/EPDB%3Agcd%3A14%3A14730414/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A180766063&crl=c&link_origin=scholar.google.com

Baranovska, T., Ihnatiuk, O., Sokha, S., Moskvych, L., & Dragan, O. (2024). Theoretical and practical dimensions of legal responsibility in criminal justice. *Multidisciplinary Science Journal, 6*. https://doi.org/10.31893/multiscience.2024ss0737

Bulgakova, D., & Bulgakova, V. (2023). The compliance of facial processing in France with Article 9 Paragraph 2 (a) (g) of the (EU) General Data Protection Regulation. *NaUKMA Research Papers. Law, 11*, 64–76. https://doi.org/10.18523/2617-2607.2023.11.64-76

Chander, A., Kaminski, M. E., & McGeveran, W. (2020). Catalysing privacy law. *Minnesota Law Review, 105*, 1733.

Citron, D. K., & Solove, D. J. (2022). Privacy harms. *Boston University Law Review, 102*, 793.

Docksey, C., & Hijmans, H. (2019). The court of justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law. *European Data Protection Law Review, 5*, 300. https://doi.org/10.21552/edpl/2019/3/6

Habib, H., Zou, Y., Yao, Y., Acquisti, A., Cranor, L., Reidenberg, J., … Schaub, F. (2021, May). Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–25). https://doi.org/10.1145/3411764.3445387

Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *Boston College Law Review, 61*, 1687. https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3

Hrytsak, N., Bartish, S., Kuchma, N., Liubinetska, M., & Nehodiaieva, S. (2025). Intermediality and literary reception in the digital age: The impact of modern media on interpretation. *International Journal on Culture, History, and Religion, 7*(SI1), 225–241. https://doi.org/10.63931/ijchr.v7iSI1.163

Ilychok, B., Karkovska, V., Dziurakh, Y., & Marmulyak, A. (2023). Changing trends in Ukraine's demographic security as a key indicator of socioeconomic stability. *Financial and Credit Activity: Problems of Theory and Practice, 2*(49), 350–360. https://doi.org/10.55643/fcaptp.2.49.2023.4183

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things, 15*. https://doi.org/10.1016/j.iot.2021.100420

Klosowski, T. (2021). The state of consumer data privacy laws in the US (and why it matters). *New York Times*. https://www.confidentialitycoalition.org/wp-content/uploads/2021/09/Attachment-16.pdf

Law of Ukraine On Protection of Personal Data of 01.06.2010 No. 2297-VI. (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text

Lloyd, I. J. (2020). *Information technology law*. Oxford University Press.

Makedon, V., Budko, O., Salyga, K., Myachin, V., & Fisunenko, N. (2024). Improving strategic planning and ensuring the development of enterprises based on relational strategies. *Theoretical and Practical Research in Economic Fields, 15*(4), 798–811. https://doi.org/10.14505/tpref.v15.4(32).02

Makedon, V., Myachin, V., Aloshyna, T., Cherniavska, I., & Karavan, N. (2025). Improving the readiness of enterprises to develop sustainable innovation strategies through fuzzy logic models. *Economic Studies (Ikonomicheski Izsledvania), 34*(5), 165–179. https://archive.econ-studies.iki.bas.bg/2025/2025_05/2025_05_09.pdf

Makedon, V., Zaikina, H., Slusareva, L., Shumkova, O., & Zhmaylova, O. (2020). Use of rebranding in marketing sphere of international entrepreneurship. *International Journal of Entrepreneurship, 24*(1S). https://www.abacademies.org/articles/use-of-rebranding-in-marketing-sphere-of-international-entrepreneurship-9325.html

Małagocka, K. (2024). Navigating digital privacy and surveillance: Post-Covid regulatory and theoretical insights. *Politics and Governance, 12*. https://doi.org/10.17645/pag.8572

Mannan, M. A. (2024). Data privacy in e-commerce: Challenges and best practices. In *Analysing privacy and security difficulties in social media: New challenges and solutions* (pp. 415–440). IGI Global.

Nurgalieva, L., O'Callaghan, D., & Doherty, G. (2020). Security and privacy of mHealth applications: A scoping review. *IEEE Access, 8*, 104247–104268. https://doi.org/10.1109/ACCESS.2020.2999934

Padden, M., & Öjehag-Pettersson, A. (2024). Digitalisation, democracy and the GDPR: The efforts of DPAs to defend democratic principles despite the limitations of the GDPR. *Big Data & Society, 11*(4). https://doi.org/10.1177/20539517241291815

Petrovich, V., Moskvych, L., Shcherbakova, N., Doroshenko, L., & Aloshyn, O. (2025). Regulatory framework for e-documentation and cyber protection amidst society's digital shift. *Salud, Ciencia y Tecnología – Serie de Conferencias, 4*. https://doi.org/10.56294/sctconf20251336

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology, 4*. https://doi.org/10.1016/j.jrt.2020.100005

Rosales, R. J. (2025). The Filipino idea of the "sacred" in the context of personalism as man prepares to his end. *International Journal on Culture, History, and Religion, 7*(1), 38–54. https://doi.org/10.63931/ijchr.v7i1.93

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law*. Aspen Publishing.

Steffen, B. (2024). Consumer health data privacy & security. https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_PGHD_Legislative_Table_20211201.pdf

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online: A systematic evidence mapping. *Information, Communication & Society, 24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Varenia, N., Moskvych, L., Olkhovskyi, O., Lykhoshapko, D., & Aloshyn, O. (2024). Enhancing the handling of digital evidence in Ukraine's criminal justice system. *Journal of Lifestyle and SDGs Review, 5*(2). https://doi.org/10.47172/2965-730X.SDGsReview.v5.n02.pe03390

Yermachenko, V., Bondarenko, D., Akimova, L., Karpa, M., Akimov, O., & Kalashnyk, N. (2023). Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects. *Economic Affairs (New Delhi), 68*(1), 617–633. https://doi.org/10.46852/0424-2513.1.2023.29

Zhukevych, I., Moskvych, L., Manhora, T., Melnyk, A., & Mykolaiets, V. (2024). Analysis of the issues related to the legalization of artificial intelligence, its use in legal proceedings, legal consultation and law enforcement system. *LSD Journal, 27*, 1–38. http://www.lsd-journal.net/archives/Volume27/AI.pdf

Zuraw, R., & Sklar, T. (2020). Digital health privacy and age: Quality and safety improvement in long-term care. *Industrial Health Law Review, 17*, 85. https://heinonline.org/HOL/LandingPage?handle=hein.journals/inhealr17&div=12&id=&page=