**Prosecution** **Digital Privacy Rights and Surveillance Law in the Age of Big Data**

|  |
| --- |
| This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license [(https://creativecommons.org/licenses/by/4.0/)](https://creativecommons.org/licenses/by/4.0/) |

**ABSTRACT:** *This article analyses the legal aspects of the right to digital privacy within the framework of evolving surveillance legislation. The research objective was achieved through scientific methods, including legislative analysis, expert interviews (14 respondents), and comparative analysis. The findings indicate that the Law of Ukraine On Digital Content and Digital Services regulates specific civil legal relations between providers and consumers regarding the provision of digital services and defines the role of digital content. A notable risk identified is the emergence of dual legal terminology, which could lead to interpretive conflicts. Furthermore, the proposed legislation lacks substantive innovations concerning protecting personal data, technical support mechanisms, and safeguards against third-party surveillance and data leakage. The survey revealed that enhancing the legal framework for digital privacy requires stricter accountability for violations of personal data protection, necessitating amendments to current legislation. Future legal reforms should focus on minimizing data sharing with third parties and legally enforcing the principle of anonymity. Legislative changes must primarily address the factor of innovation.*

*The conclusions emphasize that adopting a comprehensive approach to legislative development will strengthen the existing legal framework.*

**Keywords:** *Privacy, Digitalization, Big Data, Legislative Regulation, Survey.*

1. **INTRODUCTION**

In the modern era of rapid technological advancements and the globalization of information exchange, the issue of maintaining digital privacy has become increasingly pressing, particularly within the context of legal relations. Working with Big Data represents a core aspect of innovative technologies, offering unprecedented opportunities for analysis, forecasting, and decision-making across various sectors of society, from medicine to marketing (Durovic & Watson, 2022; Gasanov, 2024). At the same time, these technologies present new challenges related to privacy preservation, protection of personal information, and the avoidance of excessive surveillance by state institutions, private corporations, and malicious actors.

The right to privacy is currently a fundamental component of human rights protection (Kovalenko, 2022; Siagian et al., 2023). However, the extensive digitalization of societal life has introduced significant challenges to this right, as the processes of mass data collection, storage, and processing often render personal information accessible to third parties who may utilize it at their discretion (Sakkoula & Lionarakis, 2024). The legislative frameworks that justify the necessity of surveillance are frequently rooted in ensuring national security or public order (Svitlychnyi, 2023; Mühlhoff, 2023). In practice, the implementation of such laws can exceed the boundaries established by international human rights standards, resulting in infringements on private life. This creates a need to reassess the balance between security norms and the essential right to privacy.

This problem is particularly significant in democratic countries, where the search for a balance between citizens' personal freedoms (including the right to privacy) and the application of innovative technologies to combat organized crime and terrorism remains a complex dilemma (Jurkiewicz, 2018; Sarferaz, 2024). Government surveillance programs, such as PRISM in the United States or similar digital initiatives in European and Asian countries, have provoked widespread public concern, drawing attention to the problematic interplay between transparency and the preservation of state authority to maintain order and legality. Consequently, scientific research aimed at analyzing the contemporary challenges to ensuring privacy rights in the age of Big Data, as well as developing recommendations for optimizing legal mechanisms to protect privacy in digital environments, is highly relevant and in demand.

The objective of this study is to analyze the legal aspects of digital privacy rights in the context of evolving surveillance legislation. Achieving this objective involves addressing several research questions, including:

Examining the Law of Ukraine “About digital content and digital services.” (Verkhovna Rada of Ukraine, 2023)

Analyzing expert survey responses to identify current challenges and opportunities in ensuring digital privacy.

The study hypothesizes that further improvements in the legal regulation of digital privacy and surveillance, particularly in the context of Big Data, require comprehensive solutions informed by international best practices.

1. **LITERATURE REVIEW**

The scientific issue of preserving the right to digital privacy in the era of modern digital technologies and Big Data is relevant for research. In particular, the issue of modern business relations using innovative information-gathering capabilities was studied by Aho and Duffield (2020), who traced the existing experience of the European Union and China in approaches to the legal understanding of privacy boundaries. Respect for personal boundaries was studied by Chugh (2023), who pointed out the difficulties of complying with the law in digital interaction as an example of intrusion into personal life. One of the problems identified by the researcher is that the fact of interference may be invisible to the individual, and compliance with the rights of business structures (corporations) and government agencies does not always oblige them to report the fact of surveillance of private information. Similarly, Järvis (2023) demonstrated that the use of information for official use within private entities may partially go beyond the scope of digital privacy, although specific cases of such interference are not easy to prove in court. On the other hand, Landini and Noussia (2022) consider the current trend towards restricting access to private information to be justified on ethical grounds, but interference with privacy has its right to exist, especially when it comes to actions legalised by a court, prosecutor or other law enforcement agencies. This analysis points to the importance of further studying the process of observing the right to digital privacy and discussing the possibilities of limiting it, which sometimes borders on direct interference with personal life. An important issue for the discussion was the compilation of some generalised developments in the field of compliance with restrictions on digital surveillance. Important comprehensive achievements include the work of Burri (2022), who, based on a thorough study of the legal and judicial experience of European countries, reviewed existing practices to counter digital threats to privacy. The possibilities for digital surveillance (based on the legal framework) were highlighted by Oluwatosin Reis et al. (2024), who tried to cover the best global practices in organising legal frameworks for surveillance that would not infringe on the right to digital privacy of others. Humble (2020) analysed the implementation of specific laws on investigative activities, pointing out the importance of following legal procedures and thoroughly gathering evidence to allow such surveillance to proceed. This brief overview shows that the legal aspects of surveillance and the use of Big Data are being actively discussed in scientific research, which is extremely important for the Ukrainian reality, where the investigative process in the digital age is much less developed from a theoretical point of view.

The issue of access to medical secrecy is also important in modern research publications. The digitalisation of healthcare services has its clear advantages and disadvantages, one of which is that information about the medical condition of individuals may be obtained by unauthorised persons (Ioannou & Tussyadiah, 2021; Maras & Wandt, 2019). In the Ukrainian context, the problem was studied by Khodieieva et al. (2021), who, based on the study of existing precedents, pointed out the importance of protecting patients' personal information, the theft of which is still not properly assessed in Ukrainian legislation. Serohin (2021) analyses research hypotheses on the possibility of protecting private information, which is a valuable addition to existing generalizations on this topic. Attention to this issue will require further study in terms of a comparative analysis of Ukrainian and international legal experience. Some studies in this area point to the possibility of forming some recommendations (Lytras et al., 2021), which may be extremely important for the Ukrainian experience.

Researchers have also discussed the relevance of the legislative framework on surveillance, especially in times of Big Data and various mechanisms of interaction with it. Mendelson and Mendelson (2017) studied the experience of certain European countries (in particular, Scandinavian countries) on the possibility of removing information from servers at the request of users, which allows them to further prevent its use for any purpose. Researchers have studied the issues of hacker attacks, data theft, and legal counteraction to international digital crimes both from the perspective of using supranational, international judicial organisations and from the perspective of increasing the jurisdiction of national courts in each country (Casanovas et al., 2017; Rahul Khanna, 2024; Murray & Fussey, 2019). Similar issues are also important for Ukraine, which has been subjected to Russian military aggression, which at the same time has signs of hybrid warfare (massive psychological attacks, interference with digital infrastructure, hacker attacks and increased cybercrime) (Onyshchenko et al., 2023). Establishing the legal boundaries between interference with privacy and operational activities in wartime, as Itzhak and Fer (2023) have shown, will require further definition and detailed verification, as in the context of the development of a democratic environment (and Ukraine's European integration), there are some reservations about haphazard surveillance using Big Data technologies and capabilities. Further study of this issue will help determine the relevance of Ukrainian legislation and its compliance with the latest models of international legal documents regulating the right to digital privacy in the age of Big Data. The problem of the Russian invasion, which requires tighter control, adds to the importance of this process, as the clash is not only on the battlefield. Russian hacker activity, organisation of sabotage groups or recruitment of informants is primarily carried out using innovative communication technologies. In countering such cases, there is a need to find a legal balance between monitoring the emergence of anti-Ukrainian elements and the requirement of non-interference in citizens' private digital lives.

1. **METHOD**

**Research design**

This paper is based on a case study aimed at analysing the rights to digital privacy in the context of studying the Law About digital content and digital services and its practical implementation in the context of rapid development of technologies for collecting and processing big data. The research involves the use of a qualitative method of data processing and interviews with experts. The choice to focus on the Law About digital content and digital services allows us to focus on a clear legal context that plays a key role in ensuring digital privacy in Ukraine. The main components of this study are

1. Analysis of the legislation

2. Conducting interviews with experts

3. Comparative analysis

**Sample and procedures**

The main materials for the study are regulatory acts, reports and scientific studies. The inclusion of these sources was based on a criterion-based sampling. The criteria for including scientific materials included such aspects as the year of writing, thematic relevance, content and validity (in the case of laws). Table 1 shows the main inclusion and exclusion criteria for academic literature, reviews, reports and laws.

**Table 1. Main inclusion and exclusion criteria**

|  |  |
| --- | --- |
| Inclusion criteria | Description |
| Time period | From 2018 to 2024, this will ensure that the most up-to-date data is processed. |
| Thematic relevance | The materials should describe the following aspects: data protection, legal regulation of digital information, effectiveness of laws, ensuring digital privacy. |
| Appropriate scientific and methodological level | Publications should be peer-reviewed and have a high level of validity of the issues under study. The study should indicate the course of its implementation, the main methods and limitations. |
| Practical aspect | Publications should address practical issues of big data collection and processing. Studies should also include examples of practical implementation of control over the observance of digital privacy rights. |
| Exclusion criteria | Description |
| Time period | Studies written before 2018 were excluded. |
| Inaccessible materials | The study does not include materials that were not in the public domain |
| Incomplete works | Studies that were incomplete in the public domain were rejected. |
| Low practical and methodological level | The study does not describe the practical aspects of monitoring the observance of digital privacy rights. It does not specify data processing methods and collection tools. |
| Information with restricted access | The study did not use restricted information, as it is not available to all participants in the research. |

Source: Author’s development

The participants of the study were experts from various fields: law, cybersecurity, science, IT, etc. The participants were selected based on a purposive sampling. The announcement of the data collection and interviews was made via social media. Potential participants had to fill in questionnaires about their data. A total of 25 questionnaires were collected. However, to be included, experts had to meet the following criteria:

1. Have at least 4 years of experience in digital law, cybersecurity or big data.

2. Involvement Involvement in the implementation, analysis or use of key digital-related legislation.

3. Experience with Ukrainian or international regulations.

4. Recognised authority in the professional community (publications, participation in conferences, acknowledgements, etc.).

All participants also had to give their personal consent to the processing of their statements. Thus, 16 people met these inclusion criteria, but 2 people did not consent to data processing. Accordingly, 14 experts from various fields were involved in the study. Table 2 shows the composition of the experts and their basic data.

**Table 2. Information about experts**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Profession | Work experience (years) | Competent |
| 1 | Lawyer | 5 | Protection of personal data |
| 2 | Specialist in cyber defence | 6 | Technical privacy issues |
| 3 | Representative of a non-governmental organisation | 10 | Protection of user rights |
| 4 | Civil servant | 12 | Implementation of the law |
| 5 | Academic researcher | 15 | Law, digital law |
| 6 | Lawyer | 11 | Protection of personal data |
| 7 | Expert in big data technologies | 9 | Data analysis |
| 8 | Lawyer | 14 | Court practice |
| 9 | IT consultant | 10 | Development of digital platforms |
| 10 | Lawyer | 17 | Personal data protection |
| 11 | Project manager in the field of IT | 8 | Technological solutions |
| 12 | Public activist | 5 | Human rights on the Internet |
| 13 | Lawyer | 18 | Court practice |
| 14 | Civil servant | 9 | Implementation of the law |

Source: Author’s development

Therefore, the study involved 14 experts representing various fields related to the protection of digital information. As can be seen from Table 2, these individuals represented the following areas: law (lawyers, attorneys), cybersecurity, civil society, and big data technologies.

**Tools and procedure**

First, we collected and processed materials such as scientific literature and laws. The main opinions of scholars and legislators on digital privacy rights were identified.

This was followed by semi-structured interviews with experts. This was done to identify key opportunities and challenges in ensuring the right to digital privacy and surveillance in the big data era. These interviews were conducted on the ZOOM platform, where experts were given an hour to freely express their opinions. These specific questions were designed by the authors to consider the different principles, opportunities and challenges of ensuring digital privacy in the context of rapid technological development. These questions were as follows:

1. What changes in Ukrainian legislation do you consider necessary for more effective protection of personal data in the context of constant technological development?

2. How to effectively ensure the protection of digital privacy rights in a globalised digital environment where data crosses the borders of many countries?

3. What privacy principles are relevant to ensure the rights of users in the context of big data processing?

4. What are the main challenges in ensuring digital privacy in the context of the rapid development of big data collection and processing technologies?

5. How do you assess the effectiveness of the Law of Ukraine ‘About digital content and digital services’ in protecting the digital privacy rights of citizens?

6. What are the potential risks to user privacy associated with the introduction of tracking technologies: biometric data and other forms of real-time monitoring?

**Data analysis**

To analyse the data, we transcribed all the experts' answers. First, all video recordings were transcribed into text form. This was done using Sonix, which is one of the best online platforms for automatic transcription. This analysis tool was chosen because it supports the Ukrainian language. The software allowed us to upload video recordings from Zoom, after which it automatically generated an editable transcription.

Next, the data was coded to systematise the information. In particular, the answers related to aspects of digital privacy or surveillance were tagged with certain tags: legislation, technology, protection of rights, challenges. The coding was done using NVivo software, which facilitated the analysis of a large amount of data. After coding, the main responses were analysed. This was done to identify the main themes and patterns. Attention was paid to how often the experts mentioned the same issues, whether there were common opinions or disagreements between experts on certain aspects of legislation or technology. This allowed us to identify the main trends that experts or scholars pay attention to. After that, a comparative analysis of expert responses and opinions found in the scientific literature was carried out. This was done to compare the results with the opinions of other scholars. It also allowed us to see where there is agreement and where there are contradictions.

**III. RESULT**

The need to regulate digital relations that directly affect society (including Ukraine in the context of Russian aggression) is clearly justified (Kotenko et al., 2024). The Law of Ukraine ‘About digital content and digital services’ establishes separate civil legal relations between performers and consumers in the field of digital content provision or regulation of digital services (About digital content and digital services, 2023). Accordingly, it is determined that the provision of digital content or the use of digital services is carried out through the conclusion of a contract. In addition, in addition to the standard instruments of purchase or sale, the right to use, it also indicates the possibility of donation, as the contract may be either paid or not include direct payment (About digital content and digital services, 2023). In this respect, the Ukrainian experience already differs from that in Europe (Andrew & Baker, 2019).

The Law of Ukraine ‘About digital content and digital services’ establishes a list of regulated transactions, including applications, computer programs, individual video files, music or audio recordings, computer games, and e-books (About digital content and digital services, 2023). The law also establishes a certain correlation between this law and other legal documents regulating the functioning of the digital environment. It is noteworthy that in several legislative acts, some concepts may receive double terminology, which will inevitably create a number of situations regarding competition in legal interpretation. In such circumstances, there are difficulties in using legal means to enforce the rights and obligations of the parties to digital legal relations.

The analysed Law also contains little information on personal data protection, technical support and counteraction to surveillance, and data leakage to unauthorised persons (About digital content and digital services, 2023). The situation is similar to the right to digital privacy when interacting with private firms, corporations, etc. When it comes to digital content or digital services that are part of or interconnected with a product with digital elements, the proposed law does not regulate such legal relations. This creates situations of uncertainty when users' personal information is collected by producers of goods and services through the relevant software. Therefore, there is a need to improve the legal framework further (see Table 3).

**Table 3. What changes in Ukrainian legislation are needed to ensure more effective protection of personal data in the context of constant technological development?**

|  |  |  |
| --- | --- | --- |
| Changes | Expert’s voices | Expert’s opinions |
| Strengthening liability for violations of personal data protection rules | 5 | Expert 4: There is a need to introduce tangible financial penalties for violators.  Expert 10: It is important to provide not only administrative but also criminal liability for serious misconduct or malicious acts. Illegal digital surveillance or the use of private information may in some cases amount to terrorist activities. |
| Use of European experience, further harmonisation of Ukrainian legislation | 3 | Expert 1: Establishment and supervision of rules for processing digitally accessible information using EU legal frameworks.  Expert 14: The emergence of the institution of data protection officers, a position known from some European legal systems. |
| Increasing the rights of subjects to delete personal data | 3 | Expert 3: Legislative regulation (in the Ukrainian context, introduction) of the right to digital ‘oblivion’, i.e. complete removal of personal information from Big Data at the request of an individual.  Expert 7: Obtaining the right to receive detailed information on how the obtained digital data will be used in the future. |
| Continuous updating of legislation to understand the role of new technologies | 3 | Expert 11: Introduce legally justified processing of Big Data using artificial intelligence.  Expert 13: Ensuring appropriate security standards for organisations that work with personal data, regularly informing citizens about their options for protecting digital privacy. |

Source: Author’s development

To improve the legal framework for digital privacy, experts point to the need to increase liability for violations of personal data protection rules. All other possibilities are considered equally useful, but still more secondary. An important trend - the recognition of increased liability – is also evident in other elements of the survey. It refers to the effectiveness of ensuring the protection of digital privacy rights (see Table 4).

**Table 4. How can digital privacy rights be effectively protected in a globalised digital environment where data crosses the borders of many countries?**

|  |  |  |
| --- | --- | --- |
| Recommendations | Expert’s voices | Expert’s opinions |
| Increasing role of national regulators | 6 | Expert 5: There is a need to create special regulatory authorities that would coordinate the cross-border exchange of digital data.  Expert 7: An important aspect is the establishment of international Expanding cooperation between regulators in different countries. |
| Mechanisms for cross-border data protection | 4 | Expert 9: The use of legally defined rules for data exchange between states with the application of international norms.  Expert 12: The use of legal instruments such as standard contractual clauses, etc. could be considered effective. |
| Obligation to use the latest data protection technologies | 3 | Expert 3: A detailed implementation of provisions on digital encryption to protect personal information could be considered effective.  Expert 13: Legislative regulation of the use of blockchain technologies to comply with privacy standards is a possible option. |
| New educational standards | 1 | Expert 8: Developing special courses for administrators to ensure digital privacy. |

Source: Author’s development

The survey showed that experts are inclined to support the need to increase the role of digital market regulators, which echoes the previous survey regarding the recognition of increased liability. Obviously, such a tool would require changes to existing legislation (Drobotov, 2020). Other elements of such a process, such as the establishment of mechanisms for cross-border cooperation in the field of private data protection and a legal framework for the obligation to protect information using new technologies, received less support. However, as comprehensive elements of ensuring privacy in the digital environment, they are also important. Privacy principles are presented in a separate table (see Table 5).

**Table 5. What privacy principles are relevant to ensure the rights of users in the context of big data processing?**

|  |  |  |
| --- | --- | --- |
| Principles | Expert’s voices | Expert’s opinions |
| Transparency of personal data processing | 6 | Expert 2: Providing users with clear and consistent information about why and what information is collected and processed.  Expert 6: Possibility of legislative justification for requiring private companies to publish privacy policy descriptions in an understandable form. |
| Minimisation of data transferred for processing | 5 | Expert 9: Collecting only the digital information that is needed to fulfil a specific purpose, which should be communicated to consumers.  Expert 12: The principle of ‘privacy by design’, which requires gadget and software developers to consider privacy at the design stage of the system, should be legally established. |
| Anonymity | 3 | Expert 8: The possibility of using technologies that make identification of a person based on Big Data virtually impossible. Access to such information can only be obtained in the manner prescribed by law. |

Source: Author’s development

The use of the principle of transparency is one of the requirements of modern European legislation. They also discuss the importance of minimising the transfer of data to third parties (using only important information during digital interaction), which also minimises the digital footprint. Legislative compliance with the principle of anonymity is less popular among Ukrainian experts, although this principle is being actively discussed on the global stage. At the same time, the legislative application of such principles has its challenges (see Table 6).

**Table 6. What are the main challenges in ensuring digital privacy in the context of rapidly developing technologies for collecting and processing big data?**

|  |  |  |
| --- | --- | --- |
| Challenges | Expert’s voices | Expert’s opinions |
| Innovative | 8 | Expert 1: The modern development of artificial intelligence, which has not yet been properly assessed in terms of legitimate use, can violate the confidentiality of digital data.  Expert 7: A complex problem is the constant growth of Big Data with the corresponding difficulties in protecting it. |
| The complexity of international control | 4 | Expert 10: Legislative difficulties in the process of establishing legal cooperation for the exchange of information between states on privacy standards or the activities of malicious actors, etc.  Expert 13: Global inconsistency in the field of Big Data rules, which cannot be overcome by discussion among scientists. |
| The need to maintain balance | 2 | Expert 3: The need to maintain a balance between the ease of access and use of innovative technologies for ordinary users and the protection of their personal information.  Expert 4: Legislatively unresolved conflict between the goals of business companies and the need to protect user information (including the high cost of such a process). |

Source: Author’s development

According to the respondents, the innovation factor will require special attention, as technologies are constantly evolving, and therefore changes to the legislative framework will need to be regularly updated. There is also a need to harmonise Ukrainian legislation with EU law, integrate current European experience or international documents that will allow for the regulation of Big Data at the cross-border level. Existing laws in Ukraine will need to be improved (see Figure 1).

8

Positive

6

Negative

***Figure 1.*** *How do you assess the effectiveness of the Law of Ukraine ‘About digital content and digital services’ in protecting citizens’ digital privacy rights?*

Experts generally believe that the proposed law will require significant improvement. Its tangible advantage is the increase in the competence of the State Consumer Service (the supervisory authority) and the formation of a standard for the protection of consumers of digital services and digital content. However, there is a strong possibility that some provisions of the Law will compete with the provisions of previously adopted legislation (Guseva et al., 2022). The law also weakly addresses the risks of privacy and countering unjustified surveillance (see Table 7).

**Table 7. What are the potential risks to user privacy associated with the introduction of tracking technologies (biometrics and other forms of real-time monitoring)?**

|  |  |  |
| --- | --- | --- |
| Risks | Expert’s voices | Expert’s opinions |
| Unjustified use of biometric data | 6 | Expert 4: Unlawful access to biometric information (fingerprints, face recognition, etc.) provided to third parties.  Expert 7: Lack of legal restrictions on the use of biometric data without the consent of users. |
| Lack of appropriate regulation | 5 | Expert 9: The risk of concentration of large amounts of information or unlawful access to Big Data by private or public entities.  Expert 11: Lack of legislation to control the use of personal, biometric, monitoring data. |
| Violation of anonymity and confidentiality | 3 | Expert 8: Inability to be anonymous in public places due to advanced surveillance technologies.  Expert 14: Permanent monitoring of users' movements or actions. |

Source: Author’s development

Respondents identified that one of the critical challenges in working with Big Data is the unwarranted use of biometric data, which may pose significant risks of surveillance by state institutions and private entities. The lack of adequate legislative regulation remains a pressing issue. Furthermore, the improper utilization of Big Data has the potential to undermine anonymity and compromise confidentiality.

1. **DISCUSSION**

Digitalization on a global scale presents distinct advantages and disadvantages that must be carefully considered when shaping national legislation in any country, including Ukraine. The objective of this study is to examine the legal aspects of digital privacy rights amid the evolving legislative framework on surveillance. Achieving this objective involves addressing several research questions, including an analysis of the Law of Ukraine “About digital content and digital services” and an expert survey to identify current challenges and opportunities in ensuring digital privacy. The study also tests the hypothesis that advancing the legal regulation of digital privacy and surveillance in the context of Big Data requires a comprehensive approach that incorporates international best practices. The findings review the Law of Ukraine “About digital content and digital services,” which regulates specific civil relations between providers and consumers in the context of digital content and services. In addition to standard tools such as purchase, sale, or usage rights, the law introduces the concept of gifting and specifies a list of regulated operations, including applications, software, video files, music and audio recordings, video games, and e-books. However, overlapping terminology in various legislative acts poses the risk of interpretive conflicts. The law offers few innovations regarding personal data protection, technical support, and countering surveillance or data leaks to third parties. Other researchers examining this law have drawn similar conclusions, highlighting discrepancies between European legal standards and the Ukrainian framework (Guseva et al., 2022; Bachynskyi, 2024; Lyga, 2021). Notably, the European Parliament and Ukraine’s Verkhovna Rada adopted Directive 2019/770 on contracts for the supply of digital content and digital services (Horpyniuk, 2023). However, under the Association Agreement with the European Union, the adaptation of Ukrainian legislation to EU acquis is guided by annexes specified in the Agreement (Marushchak, 2019). Since Directive 2019/770 is not listed among these annexes, the implementation of the Ukrainian law does not fully align with the integration of EU norms, leading to potential misunderstandings (Cheberyako & Leshchenko, 2024). Furthermore, while some articles in Ukrainian law align with the Directive, discrepancies remain. This approach could result in legal inconsistencies during audits of Ukraine’s legislative alignment with EU standards (Kaldygozova, 2024; Ruivo et al., 2019). It is equally important to consider opportunities to enhance digital privacy and counteract surveillance in the context of Big Data utilization. The study results indicate that respondents advocate strengthening accountability for violations of personal data protection rules as a key measure to improve the legal framework for ensuring digital privacy. The findings reveal a notable trend: the recognition of enhanced accountability and the increased role of digital market regulators highlight the need for deeper legislative oversight. Such measures will require amendments to the current legislation. Mechanisms for cross-border cooperation in personal data protection and legal frameworks mandating the use of advanced technologies for data security received less support. Nevertheless, achieving these goals will be facilitated by adopting the principle of transparency in handling digital data. A feasible approach includes minimizing data sharing with third parties (collecting only essential information during digital interactions) and enacting legislative regulation of the principle of anonymity. Future legislative changes must primarily consider the factor of innovation, as technologies are evolving rapidly, necessitating continuous updates to the legal framework. Respondents identified the unregulated use of biometric data as a significant challenge in the Big Data era, potentially creating surveillance risks by state institutions and private entities. The proposed findings align with conclusions from other researchers on the importance of further adapting Ukrainian legislation to meet EU standards (Steiger, 2019; Wegge & Wetzling, 2020). This primarily involves leveraging the advanced practices of European countries and local judicial experiences to address issues related to surveillance, unlawful personal data collection, or other types of monitoring (Arora, 2019; Millett, 2023; Sehnálek, 2023). Scholars also highlight the dual risks of Big Data misuse by state institutions and private corporations (Hammond-Errey, 2023; Phireri, 2024).

According to experts, further reforms in Ukrainian legislation, including the Law of Ukraine “About digital content and digital services,” should focus on legislating the minimization of personal data sharing (Hijmans, 2021; Silaen & Sembiring, 2024). On the other hand, the application of restrictions on digital tracking using Big Data within Ukrainian legislation still requires development involving modern legal concepts of digital technologies and their capabilities, alongside regular updates to the legislative framework as a response to the challenges of the digital environment. This highlights the importance of adopting a comprehensive approach that considers both the current state of digital privacy rights and the potential challenges and opportunities presented by innovative tracking technologies in the future. Such an approach substantiates the study’s hypothesis that advancing the legal framework for digital privacy and surveillance in the context of Big Data requires comprehensive solutions informed by international experience.

The methodology employed in this study has certain limitations. Specifically, the survey method relied heavily on the subjective experiences of experts, which directly influenced their responses. Consequently, the recommendations derived from the study will require further critical evaluation in subsequent interpretations of the results.

1. **CONCLUSION**

The Law of Ukraine, “About digital content and digital services,” regulates certain civil relations between providers and consumers regarding the provision of digital services and defines the role of digital content. In addition to standard interaction tools, the law introduces the concept of gifting. It provides a legislative list of regulated operations and items, including digital applications, software, video files, music and audio recordings, video games, and e-books. An analysis of this law reveals a tangible risk of overlapping legal terminology, which could lead to conflicts in legal interpretation. Moreover, the proposed law offers few innovations regarding personal data protection, technical support, and safeguards against third-party surveillance or unauthorized access to data.

The survey findings highlight challenges and prospects for further adherence to digital privacy in the context of evolving surveillance legislation and the application of Big Data. Respondents proposed strengthening accountability for violating personal data protection rules to improve the legal framework for ensuring digital privacy. The recognition of enhanced accountability and the growing role of digital market regulators underscores the need for greater legislative oversight. Such measures will require amendments to existing legislation. Mechanisms for cross-border cooperation in personal data protection and legal frameworks mandating the use of advanced technologies for data security were deemed less popular tools. Future legislation should ensure the implementation of the principle of anonymity, protection of personal data with the right to minimize data sharing with third parties. Legislative changes must prioritize the factor of innovation as technologies continue to evolve rapidly, necessitating regular updates to the legal framework. A significant challenge in the context of Big Data is the unwarranted use of biometric data, which could pose potential surveillance risks by state institutions and private entities. Adopting a comprehensive approach to legislative development in the future will enable the improvement of the existing legal framework, ensuring it aligns with the demands of a rapidly advancing digital environment.

**V. REFERENCES**

1. Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187–212. <https://doi.org/10.1080/03085147.2019.1690275>
2. Andrew, J., & Baker, M. (2019). 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>
3. Arora, P. (2019). General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. *Surveillance & Society*, *17*(5), 717–725. <https://doi.org/10.24908/ss.v17i5.13307>
4. Bachynskyi, O.-S. (2024). Mechanism for the Formation and Implementation of HR Policy: The Global Experience. *Futurity of Social Sciences*, *2*(2), 62–78. <https://doi.org/10.57125/FS.2024.06.20.04>
5. Burri, M. (2022). Privacy and Data Protection. In *The Oxford Handbook of International Trade Law (2e)* (2nd ed., pp. 745–768). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192868381.013.29>
6. Casanovas, P., De Koker, L., Mendelson, D., & Watts, D. (2017). Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology*, *7*(4), 335–349. <https://doi.org/10.1007/s12553-017-0190-6>
7. Cheberyako, O., & Leshchenko, I. (2024). Social protection and social security in Ukraine under martial law. *World of Finance*, *1*(78), 98–110. <https://doi.org/10.35774/sf2024.01.098>
8. Chugh, U. (2023). The Evolution of Privacy Laws in the Digital Age: Challenges and Solutions. *Indian Journal of Law*, *1*(1), 51–60. <https://doi.org/10.36676/ijl.2023-v1i1-07>
9. Drobotov, S. A. (2020). National security and human rights in Ukraine. *Scientific Journal of Public and Private Law,* 2(3), 16–22. https://doi.org/10.32844/2618-1258.2020.3-2.3
10. Durovic, M., & Watson, J. (2022). AI, Consumer Data Protection and Privacy. In *The Cambridge Handbook of Artificial Intelligence* (pp. 273–287). Cambridge University Press. <https://doi.org/10.1017/9781009072168.027>
11. Gasanov, E. I. (2024). The Experience of Using AI in the Forensic Economics: A Scoping Review. *Futurity Economics&Law*, *4*(3), 261–277. https://doi.org/10.57125/FEL.2024.09.25.16
12. Guseva, O. Y., Kazarova, I. O., Dumanska, I. Y., Gorodetskyy, M. A., Melnichuk, L. V., & Saienko, V. H. (2022). Personal Data Protection Policy Impact on the Company Development. *Wseas Transactions on Environment and Development*, *18*(25), 232–246. <https://doi.org/10.37394/232015.2022.18.25>
13. Hammond-Errey, M. (2023). Big Data and Intelligence in Practice. In *Big Data, Emerging Technologies and Intelligence* (pp. 83–113). Routledge. <https://doi.org/10.4324/9781003389651-5>
14. Hijmans, H. (2021). Data Protection and Surveillance: The Perspective of EU Law. In *Surveillance and Privacy in the Digital Age*: European, Transatlantic and Global Perspectives (pp. 235–254). Oxford: Hart Publishing. <https://doi.org/10.5040/9781509925209.ch-009>
15. Horpyniuk, O. P. (2023). Protection of personal data used to ensure the activities of criminal justice bodies, taking into account the standards of the European Union and the practice of the European Court of Human Rights. In *Development trends in legal science and education of Ukraine in the context of European integration* (pp. 206–211). Baltija Publishing. <https://doi.org/10.30525/978-9934-26-372-9-53>
16. Humble, K. P. (2020). International law, surveillance and the protection of privacy. *The International Journal of Human Rights*, *25*(1), 1–25. <https://doi.org/10.1080/13642987.2020.1763315>
17. Ioannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, *67*, 101774. <https://doi.org/10.1016/j.techsoc.2021.101774>
18. Itzhak, A., & Fer, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, 43, 100637. <https://doi.org/10.1016/j.ijcip.2023.100637>
19. Järvis, M. (2023). Leadership in the Era of Sustainable Development: Challenges and Opportunities for Modern Managers. *Law, Business and Sustainability Herald*, *3*(4), 4–20. https://lbsherald.org/index.php/journal/article/view/50
20. Jurkiewicz, C. L. (2018). Big Data, Big Concerns: Ethics in the Digital Age. *Public Integrity*, *20*(1), 46—59. <https://doi.org/10.1080/10999922.2018.1448218>
21. Kaldygozova, S. (2024). Using mobile technologies in distance learning: A Scoping Review. *E-Learning Innovations Journal*, *2*(1), 4–22. <https://doi.org/10.57125/ELIJ.2024.03.25.01>
22. Khodieieva, N., Yasynok, M., Kuryliuk, Y., Filippov, S., Zemko, A., & Yasynok, D. (2021). Protection of the Right to Information on One’s Health – A Non-Jurisdictional Form of Protection. *International Journal of Criminology and Sociology*, *10*, 630–635. https://doi.org/10.6000/1929-4409.2021.10.73
23. Kotenko, M., Ruslan, K., Sopilko, I., Andrusiv, V., & Yermakova, H. (2024). Personal data protection in Ukraine via the prism of European judicial institutions’ practise. *Estudios en Derecho a la Información*, *10*(19), 151–173. <https://doi.org/10.22201/iij.25940082e.2025.19.19032>
24. 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. <https://doi.org/10.5817/mujlt2022-1-2>
25. Landini, S., & Noussia, K. (2022). Big Data, Privacy, and Protection of the User of Autonomous Vehicles: Ethical Issues, Insurance Aspects, and Human Rights. In *AIDA Europe Research Series on Insurance Law and Regulation* (pp. 131–172). Springer International Publishing. <https://doi.org/10.1007/978-3-030-82704-5_6>
26. Lyga, A. I. (2021). Genesis of legal regulation of consumer rights in Ukraine. *Economics and Law*, *1*(60), 102–115. <https://doi.org/10.15407/econlaw.2021.01.102>
27. Lytras, D. M., Lytra, H., & Lytras, M. D. (2021). Healthcare in the times of artificial intelligence: setting a value-based context. In *Artificial Intelligence and Big Data Analytics for Smart Healthcare* (pp. 1–9). Elsevier. <https://doi.org/10.1016/b978-0-12-822060-3.00011-5>
28. Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, *4*(2), 160–177. <https://doi.org/10.1080/23738871.2019.1590437>
29. Marushchak, A. I. (2019). Methods of Legal Regulation of the Security of the Individual, Society, State in the Information Sphere. *Journal of the National Academy of Legal Sciences of Ukraine*, *26*(3), 88–107.
30. Mendelson, D., & Mendelson, D. (2017). Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework. *Ethics, Medicine and Public Health*, *3*(1), 37–55. <https://doi.org/10.1016/j.jemep.2017.02.005>
31. Millett, E. (2023). Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection. *Security and Human Rights*, *33*(1), 1-20. <https://doi.org/10.58866/hqke7327>
32. Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society*, *10*(1). <https://doi.org/10.1177/20539517231166886>
33. Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, *52*(1), 31–60. <https://doi.org/10.1017/s0021223718000304>
34. Oluwatosin Reis, Nkechi Emmanuella Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, & Temitayo Oluwaseun Abrahams. (2024). Privacy law challenges in the digital age: A global review of legislation and enforcement *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. <https://doi.org/10.51594/ijarss.v6i1.733>
35. Onyshchenko, S., Burbii, A., Boikov, A., Riabiy, S., & Korniiko, S. (2023). Personal data protection on the internet under martial law: The case of Ukraine. *Revista Amazonia Investiga*, *12*(69), 204–215. <https://doi.org/10.34069/ai/2023.69.09.18>
36. Phireri, P. (2024). Urgency of Human Rights Protection in the Digital Age in the Perspective of Data Security and Privacy. *International Journal of Business, Law, and Education*, *5*(2), 2596–2600. <https://doi.org/10.56442/ijble.v5i2.905>
37. Rahul Khanna. (2024). Cybersecurity Law: Challenges and Legal Frameworks for Protecting Digital Assets and Privacy Rights. *Indian Journal of Law*, *2*(3), 15–20. <https://doi.org/10.36676/ijl.v2.i3.28>
38. Ruivo, P., Santos, V., & Oliveira, T. (2019). Success Factors for Data Protection in Services and Support Roles. In *Censorship, Surveillance, and Privacy* (pp. 814–829). IGI Global. <https://doi.org/10.4018/978-1-5225-7113-1.ch042>
39. Sakkoula, N., & Lionarakis, A. (2024). Tracing the Philosophical and Theoretical Origins of Openness in Education. *Futurity Philosophy*, *3*(3), 114–130. <https://doi.org/10.57125/FP.2024.09.30.07>
40. Sarferaz, S. (2024). Data Protection and Data Privacy. In *Embedding Artificial Intelligence into ERP Software* (pp. 173–187). Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-54249-7_10>
41. Sehnálek, D. (2023). Sharenting and Children’s Privacy Protection in International, EU, and Czech Law. *Central European Journal of Comparative Law*, *4*(1), 111–132. <https://doi.org/10.47078/2023.1.111-132>
42. Serohin, V. (2021). Information privacy: A conceptual approach. *Constitutional and legal academic studies*, (2), 52–60. <https://doi.org/10.24144/2663-5399.2020.2.06>
43. Siagian, R., Leonard Siahaan, & Muhammad Ichwan Hamzah. (2023). Human Rights in The Digital Era: Online Privacy, Freedom Of Speech, and Personal Data Protection. *Journal of Digital Learning and Distance Education*,  *2*(4), 513–523. <https://doi.org/10.56778/jdlde.v2i4.149>
44. Silaen, R. N., & Br. Sembiring, T. (2024). Legal Protection of Intellectual Property Rights in the Digital Era. *Ipso Jure*, *1*(4), 1–8. <https://doi.org/10.62872/9hn74238>
45. Steiger, D. (2019). International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3430035>
46. Svitlychnyi, V. A. (2023). Protection of personal data under martial law in Ukraine. *Law and Safety*, *90*(3), 226–236. <https://doi.org/10.32631/pb.2023.3.19>
47. Verkhovna Rada of Ukraine. (2023). About digital content and digital services: Law of Ukraine on August 10, 2023, № 3321-IX. <https://zakon.rada.gov.ua/laws/show/3321-20?lang=en#Text>
48. Wegge, N., & Wetzling, T. (2020). Countering Hybrid Threats Through Signals Intelligence and Big Data Analysis? In *Intelligence Relations in the 21st Century* (pp. 69–88). Springer International Publishing. <https://doi.org/10.1007/978-3-030-34004-9_4>