Relações Internacionais do Mundo Atual

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: 2316-2880

FINDING A BALANCE BETWEEN PERSONAL DATA PROTECTION AND PUBLIC SAFETY IN THE AGE OF DIGITALIZATION: INTERNATIONAL APPROACHES AND THEIR ADAPTATION

DAMIR DIGAY
Zhetysu University named after I. Zhansugurov, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0000-0774-991X
Email: damir.digay@mymail.academy

SVETLANA BOCHKOVA
Financial University under the Government of the Russian Federation, Russian Federation;
Russian State Agrarian University - Moscow Timiryazev Agricultural Academy, Russian Federation
ORCID: https://orcid.org/0000-0001-9349-0157
E-mail: s.s.bochkova@mymail.academy

DANA NURBEK
Zhetysu University named after I. Zhansugurov, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-5491-7952
E-mail: dana.nurbek@mymail.academy

TALGAT KHANOV
Karaganda University of Kazpotrebsoyuz, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-4288-699X
E-mail: talgat.khanov@mymail.academy

SERGEI KOLGANOV
Moscow Aviation Institute (National Research University), Russian Federation
ORCID: https://orcid.org/0000-0002-2684-4805
E-mail: kolganov@mymail.academy

AIZHAN MUSSEKENOVA
Zhetysu University named after I. Zhansugurov, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-3544-2311
E-mail: mussekenova_aizhan@bk.ru

Abstract

The paper examines the balance between personal data protection and ensuring public safety in the context of digitalization. Two opposing approaches are considered: the ethical and legal approach focused on the inviolability of personal data as a fundamental right and the utilitarian approach allowing the restriction of this right to increase security. The study, which included an expert survey (n=18) and a focus group (n=22), was conducted in 2024. The key problems of the current situation were identified, namely, insufficient transparency of data use and weak public control. The ranking of digitalization risks showed that the greatest concern is the expansion of opportunities for mass covert surveillance and the reduction of citizens' control over their data. A comparative analysis of international regulatory models revealed the advantages of the European approach (General Data Protection Regulation), but with the need to adapt it to national specifics. Practical recommendations for optimizing the balance were proposed, including increasing transparency, creating independent oversight, introducing a differentiated approach to data categories, and developing privacy by design technologies. It was concluded that it is necessary to integrate ethical and legal principles and practical aspects of security to form a balanced approach to personal data protection in the digital age.

Keywords: *privacy by design, ethical and legal approach, utilitarian approach, General Data Protection Regulation, regulation*

INTRODUCTION

The study problem lies in the growing contradiction between the expanding technical capabilities of states to control citizens' data and the right to personal data protection in the context of comprehensive digitalization. As more aspects of human life move into the digital environment – from government services (Fialkovskaya, 2024) to everyday communications – this information becomes potentially available for monitoring, which creates privacy risks (Cherckesova et al., 2024).

The discussion in the research community on this issue presents two opposing approaches: ethical and legal vs. utilitarian. The ethical and legal approach considers the inviolability of personal data as a fundamental human right, the violation of which undermines democratic institutions and the trust of citizens (Eflova et al., 2024). The utilitarian approach, on the contrary, allows for a temporary restriction of this right as a necessary measure to ensure public safety in certain circumstances.

The study's purpose is to determine the optimal approaches to regulating the protection of personal data to ensure information security in the context of the developing digitalization of public relations.

LITERATURE REVIEW

Conceptual approaches to the problem of balancing privacy and security

The ethical and legal approach is based on the recognition of the inviolability of personal data as a fundamental right. According to the General Declaration of Human Rights (art. 12) and the General Data Protection Regulation (GDPR), the right to personal data protection is inalienable. Mansoor (2025) emphasizes that privacy is a key element in protecting individual freedoms in the digital age and requires the formation of global coalitions to counter attacks on this right.

Proponents of this approach argue that attempts to justify the violation of personal data protection for the sake of security create prerequisites for technological totalitarianism. According to researchers (Palvia, 2024; Polovchenko, 2024b), uncontrolled access to

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-2880**

personal data by public and private organizations undermines the constitutional guarantees of the right to privacy (Kiryushin et al., 2024; Kiseleva, 2024; Palvia, 2024).

Murenzi (2024) points to the problem of the false dichotomy between security and freedom, when in practice the rights to privacy and security often come into conflict, especially in the context of counter-terrorism and law enforcement.

The utilitarian approach considers the possibility of limiting the right to personal data protection as a temporary and proportionate measure to increase public safety. Javvaji (2023) notes that surveillance technologies provide significant security benefits, although they also carry privacy risks, including potential abuse and discrimination.

This approach recognizes that in emergencies (epidemics, terrorism), limited use of personal data may be justified if there is a clear regulatory framework. Kukava (2023) emphasizes the importance of legal guarantees when states conduct surveillance, referring to the case law of the European Court of Human Rights.

Models for regulating the balance between data protection and public safety

The European model: the priority of personal data protection

The European model is the most vivid embodiment of the ethical and legal approach, representing a comprehensive personal data protection system based on the GDPR. This model aims to ensure a high level of protection of the rights of data subjects by introducing strict rules for data processing, including consent requirements, the right to delete data, and mandatory notification of violations (Reis et al., 2024).

The technological aspects of regulation in the European model include control over the use of artificial intelligence and biometric technologies, which pose particular risks to privacy due to the possibility of processing huge amounts of personal data without explicit consent (Akhmetshin et al., 2024c; Chumakova et al., 2024). To overcome these risks, the European model actively develops privacy by design technologies that integrate data protection into the very architecture of information systems (Kiseleva et al., 2024).

The ethical dimension of the European model is reflected in the recognition of the special value of personal data and the need to protect them, regardless of the potential security benefits. Sanchez Díaz (2023) emphasizes the importance of this aspect in an environment where technological progress often does not consider the ethical component.

The American model: a sectoral approach

The American model is characterized by the lack of a comprehensive regulatory framework for data protection like the GDPR. Privacy protection in the United States is regulated based on the Fourth Amendment to the Constitution and industry laws, leading to the fragmentation of protection in different economic sectors and enforcement levels (Murenzi, 2024). This approach reflects a more balanced combination of ethical, legal, and utilitarian approaches, with an emphasis on regulatory flexibility.

In the technological aspect, the American model is characterized by a significant variety of approaches to regulating new technologies, from strict restrictions in certain sectors (for example, healthcare) to relatively free use in other areas (Osipova et al., 2025). This creates both innovation opportunities and potential protection gaps.

Ethical discussions within the American model often focus on finding a balance between innovation, competitiveness, and the protection of rights. Allahrakha (2023) notes the importance of considering ethical aspects when forming regulatory frameworks in the field of cybersecurity and privacy (Allahrakha, 2023).

The Chinese model: the priority of state control

The Chinese regulatory model is a striking example of a utilitarian approach, with special attention to state and public security, often at the expense of privacy restrictions. According to (Shehu & Shehu, 2023), digital technologies are considered primarily as a tool for ensuring security and stability in this model.

The technological aspect of the Chinese model is characterized by the active development and implementation of mass surveillance systems, AI, and biometric monitoring technologies. Liu (2024) points out that such use of technology poses significant risks to citizens' privacy and creates a sense of constant monitoring.

The ethical dimension of the Chinese model is based on the priority of collective security over individual rights, reflecting specific cultural and political traditions. This model demonstrates high efficiency in countering various threats, but it raises concerns in terms of protecting citizens' rights.

The Brazilian and Russian models: finding a balance

The Brazilian model, presented by the General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais, LGPD), seeks to adapt the European experience to local conditions. Gunther et al. (2020) note that this law regulates the processing of sensitive personal data, limiting government interference in protecting privacy rights. The technological aspects of the Brazilian model include the development of data protection mechanisms, considering the specifics of the developing economy.

The Russian regulatory model occupies an intermediate position between the European and Chinese approaches. On the one hand, Russia provides formal protection of personal data through the Federal Law "On Personal Data", but on the other hand, priority is often given to security issues. Zotov and Gubanov (2021) note the need to find a balance between private and public spheres in the use of personal data in the digital network space.

The technological aspect of the Russian model is related to the development of national information systems and databases, as well as the introduction of biometric identification technologies (Borodina et al., 2023; Revyakina et al., 2024). Karunnaya (2023) highlights the need to develop modern methods to detect and prevent data leaks in the context of digital transformation.

Development trends and prospects

The analysis of various regulatory models allows us to identify general trends in the development of a balance between personal data protection and public safety in the context of digitalization: expanding the technical capabilities of government monitoring (Shehu & Shehu, 2023), forming a more comprehensive legal framework for regulating personal data processing (Polovchenko, 2024a; Tiwari, 2024), and searching for technological solutions that can simultaneously ensure data protection and the effectiveness of security systems (Afanasyev & Karpova, 2024; Allahrakha, 2023).

Kukava (2023) emphasizes the importance of legal guarantees when states conduct surveillance, referring to the case law of the European Court of Human Rights. This tendency to strengthen legal guarantees is observed to varying degrees in all the regulatory models considered (Severgin, 2024).

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: 2316-2880

Thus, the literature review demonstrates the versatility of the problem of balancing personal data protection and ensuring public safety in the context of digitalization. Different regulatory models embody different combinations of the ethical and legal approach with the utilitarian approach, considering the technological, ethical, and legal aspects of the problem. The following sections of our study will present an empirical analysis of the effectiveness of these models and the main problems of ensuring balance in modern conditions.

MATERIALS AND METHODS

A comprehensive methodological approach was applied to study the balance between personal data protection and ensuring public safety in the context of digitalization, including quantitative and qualitative methods of data collection and analysis.

Research design

The study was structured in several stages and conducted between January and March 2025. At the first stage, an analysis of the research literature and the regulatory framework on the research topic was carried out. The second stage included the collection of empirical data using expert survey methods and focus groups. At the third stage, the data were processed using statistical methods and qualitative analysis.

Data collection methods

A survey of 18 experts in personal data protection, information security, law, and ethics of digital technologies was conducted. The experts were selected according to the following criteria:

- at least 5 years of professional experience in the relevant field;
- publication activity on the research topic;
- representation of various professional fields (academic environment, public sector, business, civil society).

The experts were offered a questionnaire, which included 15 questions aimed at evaluating:

- the existing balance between personal data protection and security;
- transformation of this balance in the context of digitalization;

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-2880**

- promising regulatory mechanisms in this area;
- assessment of international regulatory experience.

The survey was conducted online using a specialized research platform. The experts' answers were evaluated on a 5-point Likert scale, and the questionnaire also included open-ended questions for qualitative analysis.

Three focus groups were organized with a total of 22 participants (with 6 to 8 people in each group). The focus group participants represented the following categories:

- Focus group 1: Information technology and cybersecurity specialists (8 participants);
- Focus group 2: lawyers and human rights advocates specializing in personal data protection (7 participants);
- Focus group 3: representatives of government agencies responsible for regulation in information security and data protection (7 participants).

The focus group discussions were conducted in a mixed format (online and offline), lasting 90-120 minutes each. The discussions were structured around the following topics:

- Perception of the balance between privacy and security by various stakeholders;
- Assessment of the effectiveness of existing regulatory mechanisms;
- Promising models for ensuring balance in the context of digitalization;
- International regulatory experience and its applicability in the Russian context.

All discussions were recorded with the consent of the participants, transcribed and subjected to thematic analysis.

Statistical analysis

The following methods were used for the quantitative analysis of the expert survey data:

1. **Descriptive statistics**: to summarize and present quantitative data obtained during the expert survey, indicators of the central trend (median values) and measures of dispersion (interquartile ranges) were used, which allowed us to assess general trends and variability of expert opinions on key aspects of the study.

2. **Kendall's coefficient of concordance** was used to assess the consistency of expert opinions on the most important parameters of the balance between personal data protection and public safety. This nonparametric indicator is particularly relevant for the

analysis of expert assessments and allows one to determine the degree of unanimity of the expert community.

3. **Ranking and frequency analysis** were used to identify the hierarchy of risks of digitalization for the protection of personal data and identify the most significant problems from the expert point of view. For each factor, the average ranks, standard deviations, and frequency of mentions among the most important were calculated.

Statistical data processing was carried out using the SPSS Statistics 28.0 software.

Qualitative analysis

To analyze the data from the focus groups and open questions from the expert survey, a thematic analysis was used, which included the following steps:

1. Initial data familiarization and open coding;
2. Identifying recurring patterns and forming tentative themes;
3. Revision and clarification of topics;
4. Definition and naming of the final topics;
5. Interpretation of the results in the context of research questions.

To ensure the reliability of the qualitative analysis results, a data triangulation procedure was used, including a comparison of the results of an expert survey and focus groups, as well as cross-validation of the coding by two independent researchers.

All participants were informed about the study's goals and methods and gave informed consent to participate.

RESULTS

This section presents the main results of the study of the balance between personal data protection and public safety in the context of digitalization. The results are structured according to the applied research methods and the key aspects of the problem being studied.

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-2880**

Table 1. Assessment of the current balance between personal data protection and public safety (on a 5-point scale)

Evaluation parameter	**Median**	**Interquartile range**	**Kendall's coefficient of concordance**
Adequacy of the legislative framework	3.2	1.5	0.62
Effectiveness of technical means of protection	2.8	1.8	0.58
Transparency of data use	2.1	1.2	0.76
Ensuring proportionality in data collection	2.4	1.4	0.65
Public control over the use of data	1.9	1.0	0.82

Note: A scale from 1 to 5, where 1 is a very low level, 5 is a very high level; the Kendall coefficient of concordance: the closer to 1, the higher the consistency of expert opinions

As can be seen from Table 1, the experts rate the current state of balance between personal data protection and public safety rather poorly. The parameters "Public control over the use of data" (median 1.9) and "Transparency of data use" (median 2.1) received particularly low ratings. The highest consistency of expert opinions (Kendall's coefficient equaling 0.82) is demonstrated by the public control parameter, which indicates a general recognition of the insufficient accountability in the use of personal data to ensure security.

To identify the key risks associated with digitalization, experts were asked to rank potential threats to personal data protection (Table 2).

Table 2. Ranking of risks for personal data protection in the context of digitalization

Risk	**Middle rank**	**Standard deviation**	**Frequency of mentions in the top 3 (%)**
Expanding the possibilities of mass covert surveillance	1.8	0.9	83.3
Reduction of citizens' control over their data	2.3	1.1	77.8
Development of remote identification technologies	3.5	1.3	55.6
Integration of disparate government databases	3.9	1.5	50.0
Using predictive analytics to assess risks	4.2	1.4	38.9
Transfer of control functions to private companies	5.1	1.7	27.8
Using AI algorithms to make decisions	5.3	1.6	22.2

Note: Ranking from 1 to 7, where 1 is the most serious risk.

The most serious risks, according to experts, are the expansion of the possibilities of mass covert surveillance and the reduction of citizens' control over their data. These risks were mentioned in the top three by most experts (83.3% and 77.8%, respectively).

A qualitative analysis of the focus group discussions revealed four main topics of greatest concern to the participants (Table 3).

Table 3. Key topics identified during the focus group discussions

Topic	**Description**	**Frequency of mentions (%)**	**Examples of typical statements**
Insufficient transparency of government data use mechanisms	Discussion of the problem of the lack of clear rules and public information about how and for what purposes the collected personal data is used	86.4	"The citizens have no idea what their data is being collected and how it is being used by the state."
Insufficient technical protection mechanisms	Discussion about the imperfection of technical solutions to ensure data security during data collection and processing	77.3	"Existing technical solutions do not provide an adequate level of protection for large-scale data collection."
The need for a differentiated approach to different categories of data	Discussion of the importance of establishing different levels of protection for different types of personal data	72.7	"It is necessary to clearly distinguish the categories of data and establish different modes of access to them."
The need for independent control mechanisms	Discussion on the need to create effective mechanisms for independent supervision of the use of personal data	68.2	"Only the presence of a truly independent control body can ensure that the balance is maintained."

To determine the optimal approaches to regulating the balance between data protection and security, an expert assessment of existing international models was carried out (Table 4).

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-2880**

Table 4. Expert assessment of the effectiveness of various models for regulating the balance between data protection and security

Regulatory model	Median performance evaluation (1-5)*	Interquartile range	Strengths (most frequently mentioned)	Weaknesses (most frequently mentioned)
European (GDPR)	4.2	0.8	Complexity, high level of rights protection, significant fines	Complexity of implementation, high compliance costs
American (sectoral approach)	2.8	1.2	Flexibility, consideration of industry specifics	Fragmentation, regulatory gaps
Chinese (priority of state control)	2.3	1.1	Effectiveness of counteractions to threats, efficiency	Insufficient protection of citizens' rights, lack of transparency
Russian (current status)	2.5	1.0	Consideration of national security specifics	Lack of transparency, insufficient public control

Note: *A scale from 1 to 5, where 1 is very low efficiency, 5 is very high efficiency

The European model (GDPR) received the highest efficiency rating. The Russian regulatory model is assessed by the experts as having average efficiency. It exceeds the assessment of the Chinese model, but is lower than the American sectoral approach.

In general, the results demonstrate the complex nature of balancing personal data protection and public safety in the context of digitalization. The experts express concern about the current state of this balance, especially regarding the transparency of data use and public control (Goncharov, 2024). The focus groups highlighted the importance of creating effective independent oversight mechanisms and the need for a differentiated approach to different categories of personal data. Among the international regulatory models, the European approach (GDPR) receives the highest rating, although the difficulty of its full implementation in the Russian context is recognized.

DISCUSSION

The results of the expert survey demonstrate a significant imbalance in the current system of personal data protection while ensuring public safety. The extremely low level of public control over the use of data (median 1.9 on a 5-point scale) and transparency of this use (median 2.1) are especially alarming. The high consistency of expert opinions on these parameters (Kendall's coefficient of 0.82 and 0.76, respectively) indicates the systemic nature of the problem.

The results confirm the basic assumption that there is an imbalance in the current system of personal data protection while ensuring public safety. The data correlate with the findings of (Mansoor, 2025), which highlighted the importance of privacy as a key element of protecting individual freedoms in the digital age and the need to form global coalitions to counter attacks on the right to personal data protection. Our results are also consistent with the work of (Abdulin, 2024; Glebova et al., 2023; Palvia, 2024) that highlighted the problem of uncontrolled access to personal data by public and private organizations.

The low ratings of the parameters "Transparency of data use" and "Public control" reflect the dominance of the utilitarian approach in current practice, which prioritizes security, often at the expense of personal data protection. This trend can be traced in (Javvaji, 2023), which noted that surveillance technologies, while providing benefits for public safety, posed significant risks to privacy.

The analysis of the ranking of risks for the protection of personal data in the context of digitalization reveals a clear hierarchy of threats. Two problems stand out as the most serious threats: expanding the possibilities of mass covert surveillance (average rank 1.8) and reducing citizens' control over their data (average rank 2.3).

It is noteworthy that technological aspects, such as the development of remote identification systems and the integration of government databases, occupy a middle position in the hierarchy of risks, and the use of AI for decision-making is assessed as the least serious risk. This may indicate that experts see the main problem not in the technologies themselves, but in their application in conditions of insufficient transparency and control.

This risk assessment correlates with the conclusions of (Abdullayev et al., 2024; Dagaev, 2024; Reis et al., 2024) who noted that the use of AI and biometric technologies in surveillance systems complicated privacy protection due to the processing of huge amounts of personal data without explicit consent. Our study clarifies these conclusions by demonstrating that it is the lack of transparency and uncontrolled use of technology, rather than the technology itself, that is perceived as key risks.

The revealed hierarchy of risks also corresponds to the concept of the false dichotomy between security and freedom described in (Murenzi, 2024). The results show that the experts are concerned not so much about the use of personal data to ensure security as such, but rather about the lack of proper restrictions and controls on this process.

The thematic analysis of the focus groups identified four key topics related to the prospects for achieving a balance between data protection and security. The participants are most concerned about the lack of transparency of government data usage mechanisms (86.4%), which confirms the results of the expert survey.

Two other identified topics deserve special attention: the need for a differentiated approach to different categories of data (72.7% of mentions) and the need for independent control mechanisms (68.2%). These topics point to potential ways to optimize the balance between data protection and security.

The idea of a differentiated approach to different categories of data is consistent with the findings of (Gunther et al., 2020) that analyzed the Brazilian experience in regulating the processing of sensitive personal data. Our results confirm and expand this understanding, demonstrating that a differentiated approach is in demand not only in the legal (Abdulin, 2024; Glebova et al., 2023), but also in the technical and organizational aspects of data protection.

The need for independent monitoring mechanisms is consistent with the conclusions of (Kukava, 2023) about the importance of legal safeguards in the conduct of surveillance by states. Our study highlights this necessity, pointing to the need to establish institutionally independent oversight bodies for the use of personal data for security purposes.

Evaluation of the effectiveness of different regulatory models demonstrates significant differences in approaches to ensuring a balance between data protection and security (Chumakova et al., 2023). The European Model (GDPR) received the highest efficiency rating (median 4.2), which indicates recognition of its comprehensive approach to the protection of citizens' rights.

The Russian regulatory model is assessed by experts as having an average efficiency (median 2.5), reflecting its intermediate position between the European and Chinese approaches. The weaknesses of the Russian model are the same problems that were identified in the expert survey and focus groups: a lack of transparency and insufficient public control.

Interestingly, experts think that considering the national security specifics is the strong point of the Russian model. This corresponds to the utilitarian approach, in which priority is given to ensuring security. However, as the results of the focus groups show, to achieve an optimal balance, it is necessary to integrate elements of the ethical and legal approach typical of the European regulatory model.

Such integration could include increased transparency in the use of data and the introduction of effective independent control mechanisms, while maintaining consideration of national security specifics (Akhmetshin et al., 2024a; Shafazhinskaya et al., 2024). This is consistent with the conclusions of (Sánchez Díaz, 2023) about the need for a balance that considers both the ethical component and the practical aspects of ensuring safety.

Practical recommendations

Based on the conducted study, several practical recommendations can be formulated to optimize the balance between personal data protection and public safety in the context of digitalization:

1. **Development and implementation of mechanisms to increase transparency** in the use of personal data for security purposes, including the regular publication of anonymized statistics and informing citizens about the purposes and scope of data collection.

2. **Creation of an independent body overseeing** the use of personal data in security systems, involving representatives of civil society and the expert community.

3. **Implementation of a differentiated approach** to the protection of various categories of personal data with the establishment of different access levels and authorization thresholds depending on the sensitivity of the information (Akhmetshin et al., 2024b).

4. **The development of privacy by design technologies** in the creation of security systems, which will ensure the protection of personal data at the architecture level of technical solutions (Kazakov et al., 2024).

5. **Adaptation of elements of the European regulatory model** (GDPR) to Russian conditions, considering national security specifics.

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: 2316-2880

These recommendations aim at overcoming the problems identified in the study and may contribute to a more balanced approach to personal data protection while ensuring public safety in the context of digitalization.

CONCLUSIONS

Our study revealed a significant imbalance between the protection of personal data and ensuring public safety in the context of digitalization.

An analysis of the risks of digitalization to protect personal data showed that the greatest concern is the expansion of opportunities for mass covert surveillance and the reduction of citizens' control over their data. It is noteworthy that the technological aspects themselves (AI, biometrics) are assessed as less significant risks compared to the institutional problems of their application.

A comparative analysis of various regulatory models revealed the advantages of the European approach (GDPR), but it highlights the need to adapt successful international practices to Russian conditions, considering national security specifics.

Based on the study, practical recommendations were proposed, including the development of mechanisms to increase transparency in data use, the creation of an independent supervisory authority, the introduction of a differentiated approach to various categories of personal data, the development of privacy through design technologies and the adaptation of elements of the European regulatory model.

The study's limitations include a relatively small sample of experts and focus group participants, as well as a focus primarily on the Russian context. It seems promising to conduct a quantitative analysis on a larger sample, including representatives from different countries, and to study the long-term effects of the introduction of various regulatory mechanisms.

REFERENCES

Abdulin, R. S. (2024). Vozniknoveniye i evolyutsiya termina “sudebnoye upravleniye” [The emergence and evolution of the term “judicial management”]. *Genesis: Historical Research, 1*, 20-27. https://doi.org/10.25136/2409-868X.2024.1.39794

Abdullayev, I., Ljubimova, E., Sychanina, S., Laxmi Lydia, E., & Vijaya Kumar, K. (2024). Analysis of how artificial intelligence and machine learning are employed in the field of marketing. In V. Bhateja, H. Lin, M. Simic, J. Tang, & V. Sivakumar Reddy (Eds.), *Big data analytics and data science* (pp. 315-323). Singapore: Springer. https://doi.org/10.1007/978-981-97-8666-4_26

Afanasyev, V. V., & Karpova, A. I. (2024). Inzhenernoye myshleniye v strukture professional'noy podgotovki studentov tekhnicheskikh vuzov: komponenty, podkhody i sposoby razvitiya [Engineering thinking in the structure of professional training of students of technical universities: Components, approaches and methods of development]. *Anthropological Didactics and Upbringing, 7*(3), 35-47.

Akhmetshin, E., Begishev, I., Abdullaev, I., Laxmi Lydia, E., & Archana Acharya, T. (2024a). Analysis of managing and controlling bank customers using machine learning algorithms. In V. Bhateja, H. Lin, M. Simic, M. Attique Khan, & H. Garg (Eds.), *Cyber security and intelligent systems* (pp. 377-388). Singapore: Springer. https://doi.org/10.1007/978-981-97-4892-1_32

Akhmetshin, E., Fayzullaev, N., Klochko, E., Shakhov, D., & Lobanova, V. (2024b). Intelligent data analytics using hybrid gradient optimization algorithm with machine learning model for customer churn prediction. *Fusion: Practice and Applications, 14*(2), 159-171. https://doi.org/10.54216/FPA.140213

Akhmetshin, E., Kirillova, E., Abdullayev, I., Fedorov, A., Tretyak, E., & Kochetkov, E. (2024c). Legal status and the issues of legal personhood of artificial intelligence. *Relacoes Internacionais no Mundo Atual, 1*(43), 356-366, e-6722.

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age, 4*(2), 78-121. https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.121

Borodina, M., Idrisov, H., Kapustina, D., Zhildikbayeva, A., Fedorov, A., Denisova, D., Gerasimova, E., & Solovyanenko, N. (2023). State regulation of digital technologies for sustainable development and territorial planning. *International Journal of Sustainable Development and Planning, 18*(5), 1615-1624. https://doi.org/10.18280/ijsdp.180533

Cherckesova, L., Revyakina, E., Safaryan, O., Porksheyan, V., & Kazaryan, M. (2024). Analysis of the possibilities of carrying out attacks on the functions of transferring control to operating system console using active intelligence methods. *International Research Journal of Multidisciplinary Scope, 5*(2), 516-534. https://doi.org/10.47857/irjms.2024.v05i02.0558

Chumakova, E., Korneev, D., Gasparian, M., Titov, V., & Makhov, I. (2024). Analysis of the possibilities of carrying out attacks on the functions of transferring control to operating system console using active intelligence methods. *International Research Journal of Multidisciplinary Scope, 5*(2), 461-471. https://doi.org/10.47857/irjms.2024.v05i02.0542

Chumakova, E. V., Korneev, D. G., Gasparian, M. S., Ponomarev, A. A., & Makhov, I. S. (2023). Building a neural network to assess the level of operational risks of a credit institution. *Journal of Theoretical and Applied Information Technology, 101*(11), 4205-4213.

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: 2316-2880

Dagaev, D.V. (2024). Instrumental'nyy podkhod k programmirovaniyu v sisteme Mul'tiOberon [Instrumental approach to programming in MultiOberon system]. *Software Systems and Computational Methods, 1*, 31-47. https://doi.org/10.7256/2454-0714.2024.1.69437

Eflova, M., Poroshenko, O., & Maximova, O. (2024). Artificial intelligence in the context of the development of human intellect and personality in a digital society. *Revista Juridica, 3*(79), 827-838.

Fialkovskaya, I. D. (2024). Printsipy predostavleniya publichnykh uslug: sistema i soderzhaniye xPrinciples of public service provision: System and content]. *NB: Administrative Law and Administration Practice, 1*, 23-38. https://doi.org/10.7256/2306-9945.2024.1.69515

Glebova, I., Berman, S., Khafizova, L., Biktimirova, A., & Alhasov, Z. (2023). Digital divide of regions: Possible growth points for their digital maturity. *International Journal of Sustainable Development and Planning, 18*(5), 1457-1465. https://doi.org/10.18280/ijsdp.180516

Goncharov, V. V. (2024). Predstavitel'nyye organy mestnogo samoupravleniya kak ob"yekt obshchestvennogo kontrolya: konstitutsionno-pravovoy analiz [Representative bodies of local self-government as an object of public control: Constitutional and legal analysis]. *Administrative and Municipal Law, 1*, 1-12. https://doi.org/10.7256/2454-0595.2024.1.39878

Gunther, L. E., Comar, R. T., & Rodrigues, L. E. (2020). A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do estado [Protection and treatment of sensitive personal data in the digital age and the right to privacy: The limits for state intervention]. *Relações Internacionais no Mundo Atual, 2*(27), 25-41.

Javvaji, S. (2023). Surveillance technology: Balancing security and privacy in the digital age. *EPRA International Journal of Multidisciplinary Research, 9*(7), 178-185. https://doi.org/10.36713/epra13852

Karunnaya, Ya. A. (2023). Problemy zashchity personalnykh dannykh v usloviyakh tsifrovoi transformatsii [Problems of personal data protection in the context of digital transformation]. *Juridical Science and Practice, 19*(3), 47-56. https://doi.org/10.25205/2542-0410-2023-19-3-47-56

Kazakov, O., Azarenko, N., & Kozlova, I. (2024). Developing a method for building business process models based on graph neural networks in the absence of task identifier data. *Qubahan Academic Journal*, *4*(1), 19-25. https://doi.org/10.58429/qaj.v4n1a333

Kiryushin, I. I., Ivanov, I. P., Timofeev, V. V., & Zhmurko, D. Y. (2024). Ispol'zovaniye tekhnologii blokcheyna v pravookhranitel'noy deyatel'nosti [The use of blockchain technology in law enforcement]. *Police Activity, 1*, 27-41. https://doi.org/10.7256/2454-0692.2024.1.44207

Kiseleva, E. (2024). Povysheniye effektivnosti protivodeystviya korruptsii kak usloviye obespecheniya natsional'noy bezopasnosti [Increasing the effectiveness of anti-corruption as a condition for ensuring national security]. *National Security, 1*, 33-46. https://doi.org/10.7256/2454-0668.2024.1.69502

Kiseleva, I. A., Tramova, A. M., Chernikova, E., Karakaeva, E., & Sozaeva, T. (2024). Modeling decision-making under risk and uncertainty. *Revista Juridica, 3*(79), 757-770.

Kukava, K. (2023). Balancing the right to privacy and national security interests in the digital age. *Journal of Law, 2*, 338-353. https://doi.org/10.60131/jlaw.2.2023.7711

Liu, S. (2024). Legal mechanisms for the protection of personal information in public surveillance. *Lecture Notes in Education Psychology and Public Media, 55*, 139-146. https://doi.org/10.54254/2753-7048/55/20240044

Mansoor, S. I. (2025). An interface between digital privacy and human rights: The challenges ahead. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5019128

Murenzi, R. (2024). *The balance between privacy and security in the information age*. Open Science Framework Preprints.

Osipova, E., Kutyrkina, L., Panasenko, S., Babarykin, V., Badmaeva, S., Osipova, A., & Panasenko, N. (2025). Public demand for information on green technologies in residential construction. *International Journal of Ecosystems and Ecology Science, 15*(1), 139-150. https://doi.org/10.31407/ijees15.116

Palvia, R. (2024). Right to privacy in the digital age: addressing challenges in the era of technological advancements. *Journal of Unique Laws an Students, 3*(1), 77-85. https://doi.org/10.59126/v3i1a7

Polovchenko, K. (2024a). Directions for improving legal education: Interactive techniques. *Relacoes Internacionais no Mundo Atual, 4*(46), 133-152.

Polovchenko, K. (2024b). The status of political parties in the constitutional system of the modern state: Theoretical problems and role of cc in their practical solutions. *Revista Juridica, 2*(78), 699-720, e-7296

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (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

Revyakina, E., Cherckesova, L., Safaryan, O., & Lyashenko, N. (2024). Improving performance, cryptographic strength of the post-quantum algorithm ntruencrypt and its resistance to chosenciphertext attacks. *Journal of Theoretical and Applied Information Technology, 102*(1), 186-194.

Sánchez Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital [The right to the privacy of personal data in the digital age]. *Revista Eurolatinoamericana de Derecho Administrativo, 10*(1), e235. https://doi.org/10.14409/redoeda.v10i1.12626

Severgin, A. D. (2024). Yurisdiktsiya gosudarstv v metavselennoy [Jurisdiction of states in the metaverse]. *International Law, 4*, 121-136. https://doi.org/10.25136/2644-5514.2024.4.72828

Shafazhinskaya, N., Vaslavskaya, I., Kochetkov, E., Alimamedov, E., Barchukov, V., & Biryukova, L. (2024). Building an effective knowledge management system in the concept of artificial intelligence system organization. *Relacoes Internacionais no Mundo Atual, 4*(42), 657-671.

Submetido em: 25/04/2025
Aprovado em: 20/10/2025
Avaliação: Double Blind Reviewe
ISSN: 2316-2880

Shehu, V. P., & Shehu, V. (2023). Human rights in the technology era – Protection of data rights. *European Journal of Economics, Law and Social Sciences, 7*(2), 1-10. https://doi.org/10.2478/ejels-2023-0001

Tiwari, R. (2024). Digital privacy and data protection in the age of surveillance. *International Journal of Law, Justice and Jurisprudence, 4*(2), 195-200. https://doi.org/10.22271/2790-0673.2024.v4.i2c.139

Zotov, V. V., & Gubanov, A. V. (2021). Balans privatnogo i publichnogo v ispolzovanii personalnykh dannykh v tsifrovom setevom prostranstve [Balance of private and public in the use of personal data in the digital network space]. *Communicology, 9*(2), 15-30. https://doi.org/10.21453/2311-3065-2021-9-2-15-30