International Journal of Law in Changing World

Special Issue: Women's Research in Law and Digital Technologies (2025) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v4i3.143

PROTECTION OF PERSONAL DATA FROM CYBER THREATS

Elizaveta Zainutdinova
Novosibirsk National Research State University, Novosibirsk, Russia

Article Information:

Received
April 1, 2025
Reviewed & Revised
May 12, 2025
Accepted
May 23, 2025
Published
June 28, 2025

Keywords:

personal data,
personal data protection,
data leak,
cyberattack,
personal data operator

ABSTRACT | 摘要 | RESUMEN

Personal data has become a valuable business resource, but is increasingly targeted by cyberattacks and leaks. This study uses comparative legal analysis and formal legal methods to examine how citizens' data rights can be better protected in the digital age. Focusing on liability and data breaches, the paper compares Russia's personal data protection framework with European and American approaches. The findings suggest that effective protection requires more than just listing rights for data subjects—it demands enforceable guarantees in cyberspace. The study proposes both compliance and post-control measures aimed at preventing breaches and addressing their root causes. It also recommends assigning liability to data operators proportionate to the harm caused and remedied. The analysis of current laws and enforcement practices reveals that strengthening legal accountability and implementing preventive mechanisms are essential steps toward safeguarding personal data in an increasingly digital and interconnected world.

FOR CITATION:

Zainutdinova, E. (2025). Protection of Personal Data from Cyber Threats. International Journal of Law in Changing World 4 (3), 55-70. DOI: https://doi.org/10.54934/ijlcw.v4i3.143

1. INTRODUCTION

According to the norms of the Federal Law of July 27, 2006, No. 152-FZ "On Personal Data" (hereinafter referred to as the Federal Law on Personal Data), personal data is considered in a broad sense and means any information related to, directly or indirectly, a defined or an identified individual. Such formulation allows all emerging new types of information in the digital environment to be classified as personal data, such as IP address, cookies, email address, and others. This allows the legislation on personal data to remain relevant to this day from the moment of its adoption.

We may compare the Russian approach towards personal data with the European and global practice. According to the provisions of the General Data Protection Regulation (GDPR) of the European Union (hereinafter referred to as the GDPR), personal data is also any information relating to an identified or identifiable individual. The list of personal data is also indicated, such as name, identification number, location data, online identifier, and other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. This definition is similar to the Russian one. In current realities, it is impossible to list all personal data; this is a task of judicial practice. Researchers state that it is still not possible to define in a precise and reliable manner the entire list. As a result, there may be legal uncertainty as to when data protection law applies in the context of data processing (Rupp, Grafenstein, 2024).

China's new Personal Information Law (PIPL) from November 2021 defines personal information as broadly as possible to cover the widest possible range of information. According to Article 4 of this law, personal information is all types of information recorded by electronic or other means relating to a specific or identifiable individual, with the exception of information after the use of anonymization technologies. Therefore, to process personal data, we require the consent of the data subject. The only limitation is that when anonymization is used, personal information ceases to relate to a specific or identifiable individual, and therefore, we do not need their consent. The Civil Code of the People's Republic of China also describes personal data broadly as information that can identify a natural person by itself or in combination with other information. As well as in the GDPR, it corresponds to the universal concept of direct and indirect identifiers of personal data [18]. However, it is not just the adoption but is has its own specifics influenced by domestic dynamics, cultural nuances, and China's unique data protection landscape [16].

https://doi.org/10.54934/ijlcw.v4i3.143

Some argue that while the GDPR provides for a consent-based privacy policy, the PIPL actually presents a compliance-based privacy policy that can even better promote both private and public interests [17]. Despite all the positive sides and novelties of the GDPR, it has its own critics. Researchers state that meaningful penalties for non-compliance are needed, as well as harmonised enforcement, the regulation stifles innovation narrative, defence of cross-border data rights, and proactive guidelines to address emerging technologies [5].

As for the US experience in the field of personal data, there is no single act at the federal level; this field of legislation is regulated at the state level. For example, the debatable California Consumer Privacy Act works with the broad definition of «personal information (data)» which includes everything from first name to search history or geolocation data. According to the Act, personal information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The legislation contains the following as personal information: 1) identifiers such as a real name, and others; 2) commercial information, including records of personal property; 3) biometric information; 4) Internet or other electronic network activity information; 5) geolocation data; 6) audio, electronic, visual, thermal, olfactory, or similar information; 7) professional or employment-related information; 8) education information; 9) profile about consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (The California Consumer Privacy Act). Although there is no specific list of everything that may be personal data, these groups are essential and give an exhaustive answer on what may be regarded as personal data (information) for the past 10 years. The enactment of this act was very debatable since the interests of all lobbying groups shall be taken into account, it is some kind of consensus between innovations and privacy, personal data as a commodity and as a right [4].

2. ISSUE OF LIABILITY

The consequence of violation of the legislation on personal data is administrative liability under Article 13.11 of the Code of Administrative Offenses of the Russian Federation of December 30, 2001, No. 195-FZ (hereinafter referred to as the Code of Administrative Offenses of the Russian Federation). Article 13.14 of the Code of Administrative Offenses of the Russian Federation is applied in cases where

https://doi.org/10.54934/ijlcw.v4i3.143

a person, who received access to personal data in connection with the performance of official or professional duties, allowed its disclosure.

For the disclosure of personal data, employees of an organization may also be subject to disciplinary action, for example, in the form of dismissal. And for damage caused to the employer as a result of the disclosure of information related to personal data, the employee is subject to financial liability in full, according to the Labor Code of the Russian Federation.

Criminal liability arises for more serious acts that supposedly may cause harm to the property or personal non-property rights of the data subject. As an example of causing such harm, one can cite the sending of personal messages, photos or videos of a citizen to third parties or posting them in the public domain. Such disclosure often takes place by posting information on the Internet.

Typically, such crimes are committed by bank employees or government officials. The following may serve as an example. In June and October 2021, a 35-year-old manager of the client department for servicing legal entities of the Kaliningrad branch of one of the banks, gave her friend information about the code word for identifying the client in the banking system and screenshots containing the full names, emails, mobile phone numbers and bank account numbers of two women – clients of the bank. This constituted a crime under Part 2 of Article 183 of the Criminal Code of the Russian Federation (illegal disclosure or use of information constituting a commercial, tax or bank secret).

Civil liability for leaks of personal data is also implied, but cases are rare, and the amounts of compensation are insignificant. As a result, companies are not so concerned about taking appropriate measures, including compliance, that would prevent personal data leaks in the future.

An example is the well-known leakage of Yandex.Food LLC's data, resulting in the public disclosure of personal data for 58,000 users. No more than twenty of them received small compensation. Yandex.Food LLC was charged with an administrative fine in the amount of 60 thousand Rubles (Yandex.Food LLC Civil Case of the First Instance No. 05-0413/101/2022). The "largest" amount of compensation to the affected personal data subjects, which the court recovered in this case, is 5,000 Rubles each of the 13 victims. Therefore, problems with confidentiality and personal data leaks have not been resolved, both in terms of their prevention and in terms of compensation for the harm caused.

https://doi.org/10.54934/ijlcw.v4i3.143

3. DATA LEAKAGE PREVENTION

The right to the protection of personal data, including in the digital environment in a situation of cyber threats, corresponds directly to the operator's obligation to take measures necessary and sufficient in order to ensure the fulfilment of their other duties (Article 18.1 of the Federal Law on Personal Data). Internal compliance is the implementation of internal control and/or audit of compliance of personal data processing with legislation and local acts of the personal data operator, including the operator's policy regarding the processing of personal data, which is of undeniable importance in light of the increasing frequency of personal data leaks.

The doctrine says that the term data leak itself is not used in the legislation; however, the Federal Security Service of Russia (Roskomnadzor) uses the term «personal data leaks» on its official website in the «incidents» section. Still, there is no interpretation of data leak or data leakage in the federal laws [19]. By the way, we may note that the legislator provides for the operator's obligation to detect facts of unauthorized access to personal data and take measures to detect, prevent, and eliminate the consequences of computer attacks on personal data information systems and to respond to computer incidents in them. In fact since July 2022, a mechanism for this interaction has appeared. The interaction is envisaged with the Roskomnadzor, the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation (GosSOPKA) in connection with the unlawful dissemination of personal data.

A more recent innovation in Russian legislation, in our opinion, based on the experience of the European GDPR, «gold standard of data protection» [3], regulates the operator's procedure in the event of a personal data leak and their obligation to notify Roskomnadzor about it. This establishes a rule aimed at eliminating the consequences of personal data leaks and preventing new leaks based on the results of an internal investigation, which must be carried out within 72 hours from the moment of personal data leak, and interaction with Roskomnadzor. The purpose of this was to enhance the level of protection for the personal data of Russian citizens against potential leaks, as well as to enable Roskomnadzor to respond more quickly to such incidents. The GDPR also mandates a personal data protection impact assessment, specifying when this is necessary.

Another change in Russian legislation on personal data is the operator's obligation to assess the harm that may be caused to personal data subjects in the event of a violation of obligations by the operator.

https://doi.org/10.54934/ijlcw.v4i3.143

Based on this, Roskomnadzor established rules for assessing the harm that may be caused to subjects of personal data. Of course, this can affect the amount of compensation for harm and the practice of their implementation, but we should not forget that the key in this area should be the prevention of harm to subjects of personal data due to leaks and effective mechanisms to reduce the harm caused.

Article 51 of the Chinese law on personal data (personal information) obliges operators to formulate an internal management structure and rules for dealing with personal information, implement processes for managing personal information depending on their category, and technical protection measures (encryption, de-identification), formulate and implement a plan for responding to incidents related to personal information. That is, internal compliance is actually stipulated. External checks (audits) of compliance with legislation on personal information are also envisaged. Article 55 provides for an impact assessment on personal information, its protection, similar to the GDPR, in certain cases, which is broadly prescribed, such as "cases which may have a significant impact on individuals."

Noteworthy Article 58 of the Chinese law obliges operators of personal information providing important platform Internet services:

- monitor the protection of personal information;

- form an independent body to oversee the protection of personal information;

- stop providing a service or product that seriously violates the law on personal information;

- regularly publish reports on the protection of personal information.

In addition to this, in the Cybersecurity Law, enacted in China in 2016 [1], states measures that shall be taken to prevent unlawful obtaining of personal data, including stealing and data leaks. Some chapters of this Law specify remedial actions that shall be taken after data breaches.

This actually reflects the Chinese approach towards personal data protection: publicity, on the one hand, and a great role of the state, on the other hand. Activities of data operators in China are more tightly regulated, meaning greater accountability to authorities and greater liability for personal data leaks.

https://doi.org/10.54934/ijlcw.v4i3.143

4. ENFORCEMENT OF PROVISIONS ON PERSONAL DATA PROTECTION

As for European practice, of course, the GDPR played an undeniable role in shaping the obligations of operators and cases of holding them accountable, including for the disclosure of personal data to third parties as a result of leaks. Overall, fines imposed under the GDPR have reached phenomenal amounts, amounting to millions or even billions of euros. An example is the €265 million fine imposed on Meta by the Irish Data Protection Authority. The investigation began after media reports that certain information containing personal data of users of the social network Facebook appeared on a publicly accessible hacker platform. This leak of personal data affected the rights and legitimate interests of more than 530 million users, whose personal data (phone numbers and email addresses) were disclosed to third parties without their consent (Data Privacy Manager, 2024). The investigation examined Facebook's search tools, as well as Facebook Messenger and Instagram contact importers (Meta Platforms (social networks Facebook and Instagram) are prohibited in Russia. Based on the results of an analysis of the implementation of organizational and technical measures for the protection of personal data, the Irish Personal Data Protection Authority discovered a violation of Article 25 of the GDPR, and Meta Holding was held liable in the form of a fine. The considered example shows the importance and necessity for a company operating in European markets to take preventive measures in order to combat personal data leaks.

As for the Chinese experience, due to the changes in the legislation and the need to comply with the law, the number of data leaks significantly decreased. Enhanced data security measures increase companies' value and sustainability as well as promote social responsibility to all stakeholders [20].

Analysis of Russian practice shows that effective mechanisms for protecting rights and influencing offenders are needed in order to make the protection of personal data a reality. The Russian doctrine notes that a leak, in general, which constitutes an administrative offense, can be a consequence of both the deliberate actions of the personal data operator (his employees), and can be the result of a hacker attack on the operator's information systems in situations where the operator has not taken sufficient and reasonable measures [12].

In total, fines imposed on operators for personal data leaks in 2023 amounted to more than 3.7 million Rubles. A famous case is the leak of personal data of employees, students and applicants of the Higher School of Economics (Hse.ru, 2023). Despite the fact that the investigation of the leak of personal data was carried out by the educational institution on time, in accordance with the part 3.1 of the Article

https://doi.org/10.54934/ijlcw.v4i3.143

21 of the Federal Law "On Personal Data", Roskomnadzor was notified of this situation, the court district of the magistrate No. 387 in the Basmanny District of Moscow fined the Higher School of Economics 60 thousand Rubles for leaking personal data under the part 1 of the Article 13.11 of the Code of Administrative Offenses of the Russian Federation ("Processing of personal data in cases not provided for by the legislation of the Russian Federation"). At the same time, the problem that arose was not properly resolved, and there are reasonable suspicions that personal data were made publicly available on the Internet.

This practice of data leaks continues in 2024, 2025 and is to continue in the future. When a leak is detected (the leak is reported to Roskomnadzor), formal measures are taken, and no substantial (preventive or restorative) measures are taken to eliminate the consequences of the leak. An example of this is the leak of a database with personal data of clients of the insurance company "Spasskie Vorota" in September 2024. This database was made publicly available on one of the shadow forums. It contains about 70 thousand unique phone numbers, 100 thousand unique email addresses, hashed passwords and other information, including API access logs on the spasskievorota.ru server. In turn, the insurance company "Spasskie Vorota" sent information on the leak of personal data of clients to Roskomnadzor. This was reported after the media reported on the alleged leak of the company's clients ' data. In 2024, overall, Roskomnadzor recorded 135 cases of database leaks, which contained more than 710 million records about Russian citizens.

At the end of August 2024, the World Class fitness club chain was subjected to a hacker attack, which resulted in the leak of personal data of hundreds of thousands of visitors. In particular, the 1C:Enterprise database with a volume of more than 146 GB was made publicly available in the Internet.

An analysis of judicial practice leads to the conclusion that, as a rule, an organization is presumed to be guilty if there is a leak of personal data in its information systems. That is, the very fact of a leak of personal data in an organization entails its legal, above all, administrative responsibility. The issue of insufficient measures taken by the organization is not investigated. The courts proceed from the assumption that the organization had a real opportunity to ensure compliance with the requirements of the law, that is, to prevent the leakage of personal data. Courts suppose that the operator must ensure the security of access to the personal data of its clients, and the measures taken by the operator are not examined in detail (Resolution of the Magistrate's Court of the Judicial Precinct No. 374 of the Tagansky District of Moscow dated March 17, 2023 in Case No. 5-240/2023).

https://doi.org/10.54934/ijlcw.v4i3.143

As a result, the one who is to protect the personal data of clients (operator) is fined, and the amount of the fine is not substantial. However, persons who, in reality, through their malicious actions, have unlawfully accessed personal data go unpunished, and leaks continue to occur. Thus, the question arises of how it is possible to ensure and improve the level of protection of personal data in the current situation: cyberattacks and cyber threats, in a situation in which personal data can become publicly available on the Internet and used by attackers.

5. CHANGES IN LEGISLATION REGARDING PERSONAL DATA LEAKS

In accordance with Part 3.1 of Article 21 of the Federal Law on personal data, the Roskomnadzor is notified by the personal data operator about the leak of personal data that has occurred. In order to record information about the leak of personal data, the Roskomnadzor maintains a special register, defining the procedure and conditions for interaction with operators within its jurisdiction (part 10 of Article 23 of the Federal Law on Personal Data). It is also interesting to note that in this notification, the Roskomnadzor, as an authorized body, is notified of the compromised personal data database, the alleged causes of the incident, harm to the subjects of personal data, and the measures taken to eliminate the consequences of the leak of personal data. Are these measures sufficient to prevent new leaks of personal data and effectively apply the rules on the protection of the rights of personal data subjects in the digital environment?

Various points of view were expressed in order to improve the current legislation on personal data. By analogy with the European data protection regulation, GDPR, it was proposed to establish negotiable fines against operators who have committed an unlawful or accidental leak of personal data. It was proposed even to establish criminal liability for the illegal collection, storage, use, and transfer of personal data databases, which is aimed at combating the consequences of personal data leaks.

The Bill No. 502104-8 "On Amendments to the Code of the Russian Federation on Administrative Offences" was enacted. This Bill, in general, tightens responsibility, differentiating it depending on the amount of personal data subjected to leakage and the affected subjects of that data. In the event of repeated violations of the duty of confidentiality regarding personal data, this bill provides for turnover fines (fines as a percentage of revenue). The Bill on Amendments to the Criminal Code of the Russian Federation

https://doi.org/10.54934/ijlcw.v4i3.143

provides for criminal liability for persons who illegally collect, store, use and/or transfer computer information containing personal data obtained through unlawful access to means of storing, processing or transmitting computer information or by other illegal means.

The issue of insurance against personal data leaks is also being considered in the doctrine and practice. The idea is to conclude agreements with insurance organizations or create a compensation fund from which payments will be made to persons affected by personal data leaks. In view of the above, it is necessary not only to tighten responsibility, which will lead to the concealment of cases of personal data leaks [9], but also to take actions to smooth over the harm and prevent its occurrence.

The amendments specified above shall be assessed positively, but the legislator's attention shall be focused not only on strengthening legal liability for personal data leaks, but also on preventing leaks by introducing measures for internal compliance and informing the public as provided for in Chinese law.

However, the Ministry of Digital Development, Communications and Mass Media of Russia plans to introduce mandatory notification of citizens about cases of leakage of their personal data. This initiative is being discussed after the adoption of a law toughening penalties for such incidents. This was announced at the end of May 2024 by the Deputy Chairman of the Council for the Development of the Digital Economy. This sounds reasonable, but may require additional state budget funds, so a financial justification is needed for such a measure.

In foreign literature, not only legal literature, the issue of the impact of fines on the number of personal data leaks is discussed. The most common cases of personal data leakages include: 1) a hack by an external party or malware; 2) port (leakage by using a portable device); 3) stat (leakage by a stationary computer loss); 4) inside management and people's capital problems (due to employee's, contractor's or customer's fault); 5) some kind of unintended disclosure not involving hacking, intentional breach or physical loss; 6) physical loss (paper documents are lost, discarded or stolen); 7) card's leakage (frauds with data involving debit and credit cards). According to the research, data breaches caused by hacking account for a third of all cases. The next important case for data leakage is human intentional acts that accounts for a fourth of all cases [7].

These statistics are fully consistent with he Russian legal reality: the results of data breach and leakage cases in Russian courts, legal issues of determining and identifying persons who committed a

https://doi.org/10.54934/ijlcw.v4i3.143

hacker attack, and issues of holding employees and other persons accountable to the personal data operator.

6. PROTECTIVE MEASURES THAT MAY PREVENT OR STOP PERSONAL DATA LEAKS

Some researchers focus not only on liability measures, but also on protective measures that may prevent or stop personal data leaks. Users often transmit personal data through smartphones and personal computers, which can be used, including for illegal purposes, by other persons. That is, users need to be more vigilant, aware of their rights and legal consequences. In this sense, the emphasis is on the need for subjects of personal data to take some self-defence measures, which allows them to ensure the safety of their own personal data.

Nowadays, a person, without even realizing it, provides a vast amount of information about themselves to various companies every minute. The more personal data about a person is collected and processed, the higher the risk of violating their right to the protection of personal data [13]. All this is a prerequisite for personal data leaks and gives rise to different problems in law enforcement. However, it seems that much of taking measures to protect personal data should also depend on personal data operators and on what measures they take to prevent and eliminate personal data leaks. Accordingly, it seems illogical to assign the full legal consequences solely to the subjects of personal data who act as consumers.

Nowadays, in an information society, such services are offered as monitoring customer data (searching for published leaks and aggregated arrays of accounts, as well as data related to the customer's information systems). Additionally, these services include monitoring shadow forums and DarkNet platforms for leaks of internal business or customer information. This presumes preparation and constant update of a list of features (data formats, keywords, etc.) indicating the ownership of information.

As far as data leaks are concerned, investigating incidents related to data leaks is needed, which includes an analysis of sources and prerequisites for data leaks. This way, evidence for appeals to law enforcement agencies and for civil proceedings is collected.

As far as banks are concerned, we need to identify insiders who may be involved in the theft of data. This is made by the use of the content analysis of information sold on the black market and by testing the capabilities of employees for unauthorized access to information resources.

https://doi.org/10.54934/ijlcw.v4i3.143

The use of such protective measures significantly reduces the likelihood of sensitive data being leaked by intruders due to the timely identification of vulnerabilities and the adoption of appropriate measures.

In this context, V.V. Arkhipov, correctly points out that recognizing personal data not as goods, as some in the doctrine indicate, but as an intangible benefit, will help to combat violations in this field. M.A. Rozhkova, acknowledging the existence of the concept of personal data as a commodity [10], notes that if personal data is not anonymized (clause 9 of Article 3, part 7 of Article 5, clause 9 of part 1 of Article 6 of the Law on Personal Data), it cannot be used in civil circulation. In turn, big data, which includes anonymized personal data, may be the object of civil law transactions [15]. These approaches seem to be correct. At the same time, practice appears to have taken a different path. Thus, personal data is universally recognized as a commodity. For example, when registering on a social network, we "pay" with personal data. By providing our personal data as if for free, in fact, in exchange for the advertising provided and the use of our personal data by other services for commercial purposes, we receive the use of social network services for communication, promotion of our own goods and services, use of news aggregators, etc.

V.I. Soldatova, noting, in general, the problem of insecurity of citizens' personal data from unauthorized access by an unlimited number of persons [14], comes to the conclusion that the available means of protecting personal data are insufficient in the context of the use of digital technologies, and increased liability is necessary. It is, of course, necessary to agree with this; however, emphasizing the fact that it would be necessary to provide not just for the increased legal liability, but also for the effective mechanisms for compensating harm to those affected by leaks and the implementation of measures aimed at preventing leaks of personal data.

A.Yu. Burova also notes that we should avoid uniform user consent for the processing of personal data in all services of the digital platform ecosystem, as this may lead to an increased risk of leakage of the user's personal data [6]. A reasonable approach to protecting the rights to personal data will, indeed, allow a subject of personal data if not prevent, then at least to minimize the consequences of leaks.

https://doi.org/10.54934/ijlcw.v4i3.143

7. CONCLUSIONS

It seems that in the current situation, it is necessary to implement appropriate preventive measures that would allow a priori to minimize leaks of users' personal data. Compliance may be used in order to technically and legally identify existing risks to the security of personal data, violations by an operator of certain legal provisions, and access of third parties to personal data, etc. Such measures, of course, should be implemented in local regulations at the level of personal data operators, and legislation shall also be improved in order to clarify the requirements for compliance, which in general are already provided for by current legal norms. In addition, at the level of market entities, employees shall be trained on an ongoing basis in the basics of secure management of personal data in order to understand what the misuse of personal data is and prevent it.

Of course, post-control is also necessary, which consists of checking an operator's activities for violations that led to the leakage of personal data. The law enforcement body (Roskomnadzor) can thus identify the exact cause of the leak of personal data and how it can be prevented in the future.

An integrated approach, including both preventing harm and assessing an operator's activities for violations, is to change the current situation with the circulation of personal data. It is necessary not only to minimize the consequences of leaks and encourage operators to comply with legislation on personal data by strengthening liability measures, but also to prevent and eliminate the causes of personal data leaks. The above will help reduce the number of personal data leaks in the Russian Federation and minimize the negative consequences of the state, business and society.

REFERENCES

[1] Aimin, Qi, Guosong, S., & Wentong Z. (2018). Assessing China's Cybersecurity Law. Computer Law & Security Review, 34, 1342-1354. https://doi.org/10.1016/j.clsr.2018.08.007

[2] Arhipov, V.V. (2018). The Problem of Qualifying Personal Data as Intangible Goods in the Digital Economy, or there is Nothing More Practical than a Good Theory, Zakon, 2, 52-68.

[3] Ayala-Rivera, V., Portillo-Dominguez, O., & Pasquale, L. (2024). GDPR Compliance via Software Evolution: Weaving Security Controls in Software Design. Journal of Systems and Software, 216, 22 p. https://doi.org/10.1016/j.jss.2024.112144

[4] Baik, J. (2020). Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA). Telematics and Informatics, 52. https://doi.org/10.1016/j.tele.2020.101431

[5] Buckley, G., Caulfield, T., & Becker, I. (2024). How Might the GDPR Evolve? A Question of Politics, Pace and Punishment. Computer Law & Security Review, 54, 14 p. https://doi.org/10.1016/j.clsr.2024.106033

[6] Burova, A.Yu. (2023). Digital Ecosystem as a Way of Doing Business: a Legal View. Current Issues of Russian Law, 11, 111-117. https://doi.org/10.17803/1994-1471.2023.156.11.111-117

[7] Jingyu F. (2023). Legal Policies Failing on Data Breaches? Legal Policies Failing on Data Breaches? An Empirical Study of U.S. Information Security Law Implementations. Procedia Computer Science, 221, 971-978. DOI: 10.1016/j.procs.2023.08.076

[8] Nohrina, M.L. (2013). The Concept and Signs of Intangible Benefits: Legislation and Civil Science, Izvestiya Vysshih Uchebnyh Zavedenij. Pravovedenie, 5, 143-160.

[9] Ratushnyj, M. (2024). Overview of Key Changes in Personal Data Legislation. Available at: https://pravo.ru/opinion/251783/ (last visited 01.02.2025).

[10] Rozhkova, M.A., & Glonina, V.N. (2020). Personal and Non-Personal Data as Part of Big Data, Law of Digital Economy. Yearbook-Antology. Series "Analisys of the Modern Law / IP & Digital Law", ed. by M.A. Rozhkova. Moscow: Statut, pp. 271-296.

[11] Rupp, V., & Grafenstein, M. (2024). Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection. Computer Law & Security Review, 52, 25 p. https://doi.org/10.1016/j.clsr.2023.105932

[12] Savel'ev, A.I. (2021). Scientific and Practical Article-by-Article Commentary on the Federal Law "On Personal Data". Moscow: Statut, 468 p.

[13] Savel'ev, A.I. (2015). Problems of Application of Legislation on Personal Data in the Era of "Big Data". Pravo. Zhurnal Vysshej Shkoly Ekonomiki, no. 1, pp. 43-66.

[14] Soldatova, V.I. (2023). New Legislative Measures to Protect Personal Data. Pravo i Ekonomika, no. 3, pp. 25-30.

[15] Uroshleva, A. (2018). Commercialization of Personal Data and the Concept of "Big Data" are Topical Issues in the IT Field." Available at: https://www.garant.ru/article/1229761/ (last visited 01.02.2025).

[16] Wenlong, L., & Jiahong, C. (2024). From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China. Computer Law & Security Review, vol. 54, 14 p. https://doi.org/10.1016/j.clsr.2024.105994

[17] Xiaodong, D., & Hao, H. (2024). For Whom is Privacy Policy Written? A New Understanding of Privacy Policies. Computer Law & Security Review, 55, 13 p. https://doi.org/10.1016/j.clsr.2024.106072

[18] Xiongbiao, Y., Yuhong Y., Jia, L., & Bo J. (2024). Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: Chinese Perspective. Telecommunications Policy, (48)10, 15 p. https://doi.org/10.1016/j.telpol.2024.102851

[19] Zinovieva, V., Shchelokov, M., & Litvinovskya, E. (2023). Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks. Transportation Research Procedia, 68, 461-467. https://doi.org/10.1016/j.trpro.2023.02.062

[20] Ziwei, S. (2024). Personal data Security and Stock Crash Risk: Evidence from China's Cybersecurity Law. China Journal of Accounting Research, (17) 4, 23 p. https://doi.org/10.1016/j.cjar.2024.100393

ABOUT THE AUTHOR

Elizaveta Zainutdinova – Ph.D., Department of Business Law, Civil and Arbitration Proceedings, Novosibirsk National Research State University, Novosibirsk, Russia
e-mail: zainutdinovaev@gmail.com
ORCID ID: https://orcid.org/0000-0002-9522-890X
Google Scholar ID:
https://scholar.google.com/citations?pli=1&authuser=1&user=93Iuvd8AAAAJ

ABOUT THIS ARTICLE

Conflict of interests: The author declares no conflicting interests

PROTECCIÓN DE DATOS PERSONALES CONTRA CIBERAMENAZAS

RESUMEN

Los datos personales se han convertido en un valioso recurso empresarial, pero cada vez son más blanco de ciberataques y filtraciones. Este estudio utiliza análisis jurídico comparativo y métodos legales formales para examinar cómo se pueden proteger mejor los derechos de los ciudadanos sobre sus datos en la era digital. Centrándose en la responsabilidad y las filtraciones de datos, el documento compara el marco de protección de datos personales de Rusia con los enfoques europeos y estadounidenses. Los hallazgos sugieren que una protección eficaz requiere más que simplemente enumerar los derechos de los titulares de los datos; exige garantías exigibles en el ciberespacio. El estudio propone medidas de cumplimiento normativo y control posterior destinadas a prevenir las filtraciones y abordar sus causas fundamentales. También recomienda asignar responsabilidad a los operadores de datos proporcional al daño causado y reparado. El análisis de la legislación vigente y las prácticas de aplicación revela que fortalecer la responsabilidad legal e implementar mecanismos preventivos son pasos esenciales para salvaguardar los datos personales en un mundo cada vez más digital e interconectado.

Palabras clave: datos personales, protección de datos personales, filtración de datos, ciberataque, operador de datos personales

保护个人数据免受网络威胁

摘要

个人数据已成为宝贵的商业资源，但日益成为网络攻击和泄露的目标。本研究运用比较法律分析和正式法律方法，探讨如何在数字时代更好地保护公民的数据权利。本文聚焦责任和数据泄露，将俄罗斯的个人数据保护框架与欧美的做法进行了比较。研究结果表明，有效的保护不仅仅需要列举数据主体的权利，还需要在网络空间提供可执行的保障。本研究提出了合规和事后控制措施，旨在预防数据泄露并解决其根本原因。研究还建议根据造成的损害和补救措施，向数据运营者追究责任。对现行法律和执法实践的分析表明，在日益数字化和互联互通的世界中，加强法律问责和实施预防机制是保护个人数据的关键步骤。

关键词：个人数据、个人数据保护、数据泄露、网络攻击、个人数据运营者

https://doi.org/10.54934/ijlcw.v4i3.143