DOI: 10.18254/S278229070031784-8 Original paper

Confidentiality of Personal Data in the Situation of Cyber Threats

©2024 Elizaveta Zainutdinova[a]

[a] Novosibirsk State University, Russia
zainutdinovaev@gmail.com

Abstract. Recently, Russia has become one of the leaders in personal data leaks. The year 2023 in Russia became a truly record year for the number of personal data leaks. Personal data is currently not only a valuable resource in the field of business turnover, but it is also the object of various types of cyberattacks and leaks committed by third parties' malicious actions. The right to confidentiality and the right to protection of personal data are not implemented in the digital environment due to the susceptibility to cyberattacks and the lack of appropriate measures and guarantees in this field. Based on the analysis of current legislation and law enforcement practice, we conclude that it is not enough to list the rights of personal data subjects in order to effectively protect them. Guarantees in the cyber space are needed through the implementation of appropriate protective measures, as well as the establishment of the liability of operators related to the amount of harm caused and eliminated in regards to the subjects of personal data.

Keywords: personal data, operator, leak, leakage, personal information, GDPR, turnover fines, protection of personal data, cyber threat, cyberattack

For citation: Zainutdinova E. 2024. Confidentiality of Personal Data in the Situation of Cyber Threats. *Law & Digital Technologies 4(1): 31—38.*

INTRODUCTION

According to the Federal Law of July 27, 2006 No. 152-FZ (as amended on February 6, 2023) "On Personal Data" (hereinafter referred to as the Federal Law on Personal Data), personal data means any information related to a directly or indirectly defined or identified individual (subject of personal data). Such legislative provision 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. It seems that this approach of the Russian legislator is developing in line with the global practice.

Thus, according to the provisions of the General Data Protection Regulation of the European Union (hereinafter referred to as the GDPR), personal data is also any information relating to an identified or identifiable individual. At the same time, 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. It seems that this definition is similar to the Russian one. Moreover, in the current realities of the digital economy, it is impossible to list all personal data; in any case, this is a task of judicial practice.

China's new Personal Information Law, effective November 2021, also defines personal information as broadly as possible to cover the widest possible range of information. Thus, 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. Indeed, this definition enshrines a wide range of information; the only limitation is the indication that when anonymization is used, personal information ceases to relate to a specific or identifiable individual.

Russian judicial practice quite successfully formulates criteria for classifying various types of information as personal data (for example, data left by individuals on the social networks VKontakte, Odnoklassniki, Moi Mir, Instagram (prohibited in the Russian Federation), Twitter; on the Internet portals "Avito", "Avto.ru", which are considered as personal data). Law enforcement practice is based on the principle of maximizing the list of personal data if it allows one to identify a particular individual. Also, expanding the means of legal protection, courts, when considering cases on the use of personal data of citizens, apply the norms of the Law of the Russian Federation "On the Protection of Consumer Rights".

IMPLEMENTATION OF THE RIGHT FOR PROTECTION OF PERSONAL DATA IN THE DIGITAL FIELD

It is interesting to see how the right to protect the rights and legitimate interests of the subject of personal data in the digital field is changing. As a general rule, in accordance with Articles 17.2 and 24 of the Federal Law on Personal Data, the subject of personal data has the right to protect his or her rights and legitimate interests, including in court, and the right to compensation for losses and moral damage.

In general, the approach of the Russian legislator is to establish a legal treatment for personal data through their definition and limitation of the personal data operator's ability to use them (Articles 3, 10, 11, 18, 18.1, 19 of the Federal Law on Personal Data). The unlawful acquisition of personal data constitutes both criminal and administrative offenses. As a rule, violating personal data legislation results in 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). Article 13.14 of the Code of Administrative Offenses applies when a person who received access to personal data in connection with their official or professional duties allows its disclosure, which is often found in practice and frequently leads to personal data leaks.

Two more types of legal liability should also be added. For disclosure of personal data, employees of an organization may be subject to disciplinary action, such as dismissal. For damage caused to the employer by the disclosure of information related to personal data, the employee is fully financially liable (Articles 90, 238, clause 7, part 1; Article 243 of the Labor Code of the Russian Federation).

Criminal liability arises for more serious acts. These acts not only include the disclosure of personal data or other illegal uses but also causing harm to the property or personal non-property rights of the subject. An example of such harm is the sending of personal messages, photos, or videos of a citizen to third parties or posting them in the public domain (in Cassation ruling of the Seventh Cassation Court of the General Jurisdiction dated June 10, 2020 No. 77-889/2020). Such disclosure often takes place by posting information on the Internet (in Resolution of the Plenum of the Supreme Court of the Russian Federation dated December 25, 2018 No. 46 "On Some Issues of Judicial Practice in Cases of Crimes against the Constitutional Rights and Freedoms of Man and Citizen (Articles 137, 138, 138.1, 139, 144.1, 145, 145.1 of the Criminal Code of the Russian Federation Federation)").

Civil liability for leaks of personal data is also implied, but cases are rare and the amounts of compensation are insignificant, as was shown in judicial practice above. Subjects of personal data have the right to recover losses and compensate for moral damage caused, but examples of decent compensation for personal data leaks cannot be found in existing practice. As a result, companies are not so concerned about taking appropriate measures, including compliance, that would prevent personal data leaks in the future. It seems that legislation and practice should more fully regulate how a person who has suffered from a leak of personal data can receive protection from the misuse and dissemination of his or her personal data.

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 fulfillment of its 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 probably not fully developed in the current legal acts, however is of undeniable importance in light of the increasing frequency of personal data leaks.

The legislator in the same article, from December 2020, 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. Since July 2022, a mechanism for this interaction has appeared. Thus, interaction is envisaged with the Federal Security Service of Russia (hereinafter referred to as the FSB of Russia), 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.

The Order of the of the Federal Security Service (Bureau) of the Russian Federation dated February 13, 2023 No. 77 "On Approval of the Procedure for Interaction of Operators with the State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks on Information Resources of the Russian Federation, including Informing the FSB of Russia about Computer Incidents that resulted in Unlawful Transfer (Provision, Distribution, Access) of Personal Data" stipulates the operator's obligation

to inform the FSB within 24 hours from the moment of detection of a computer incident that entails the specified above consequences, if the operator directly interacts with the National Coordination Center for Computer Incidents. Otherwise, the operator informs Roskomnadzor no later than 24 hours from the moment of detection of a computer incident that entailed the specified consequences, and no later than 72 hours from the moment of the computer incident - fills out a notice of the results of the internal investigation, sending it to Roskomnadzor (Federal Service for Supervision in the field of Communications, Information Technologies and Mass Communications). That is, in essence, the specified standards established internal compliance and work with computer attacks as measures to combat personal data leaks.

A more recent innovation in Russian legislation, in our opinion, based on the experience of the European GDPR, namely the Part 3.1 of the Article 21 of the Federal Law on Personal Data, regulates the operator's procedure in the event of a personal data leak and his 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 Roskomnadzor website has a special electronic form for submitting notification of personal data leakage. This was intended to increase the level of protection of personal data of Russian citizens from possible leaks, as well as to allow Roskomnadzor to more quickly respond to such incidents. However, has this goal actually been achieved?

Article 33 of the European GDPR act establishes the obligation of the controller (operator), if possible, no later than 72 hours after the discovery of this violation, to notify the competent supervisory authority about it, except in cases where it is unlikely that it will lead to any risk to the rights and freedoms of individuals. If notification is not made within 72 hours, it must be accompanied by an explanation of the reasons for the delay. It is noteworthy that in the comments to this law it is stated that it is necessary to verify whether all measures have been taken to immediately establish the fact of a leak of personal data, as well as to determine whether all measures, including technical measures, have been taken before the leak to ensure effective protection of the rights of personal data subjects. The GDPR also mandates personal data protection impact assessment, specifying when this is necessary. However, the latter is important even before personal data leaks for taking preventive measures, primarily of an organizational and technical nature.

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. Based on this, Roskomnadzor established rules for assessing the harm that may be caused to subjects of personal data. These rules make it possible to determine the degree of probable harm, which is reflected in the corresponding leak report. 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.

In Chinese legislation on personal data (personal information) there are similar provisions as well as completely unique legal norms aimed at minimizing cases of personal data leaks in the digital environment. Article 51 of the Chinese law 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. Article 54 of the law also provides for external checks (audits) of compliance with legislation on personal information. Article 55 also 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." Specific deadlines for notifying the Chinese supervisory authority about incidents in the field of personal data are not established, and such notification shall include categories of personal information that were leaked, the reasons and possible harm, the measures taken by the operator.

Most interesting and noteworthy is the Article 58 of the Chinese law. This article obliges operators of personal information providing important platform Internet services: 1) create a system for monitoring the protection of personal information and form an independent body, consisting primarily of external persons, to oversee the protection of personal information; 2) in the platform rules formulate their obligations to protect personal information; 3) stop providing a service or product that seriously violates law on personal information; 4) regularly publish reports on the protection of personal information and allow public control (Savodnikov 2021). Indeed, these provisions are very noteworthy, establishing specific measures to prevent personal data leaks, taking into account Chinese legal specifics (publicity and accountability to authorities).

ENFORCEMENT OF PROVISION ON THE PROTECTION OF PERSONAL DATA

As for European practice, of course, 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 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[36]. Based on the results of an analysis of the implementation of organizational and technical measures for protection of personal data, the Irish Personal Data Protection Authority discovered a violation of Article 25 of GDPR, and the 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.

An 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 real. The Russian doctrine notes that, in general, a leak, which constitutes an administrative offense, can be a consequence of both the deliberate actions of the personal data operator or his employees and a hacker attack on the operator's information systems in situations where the operator has not taken sufficient and reasonable measures.

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 (Savelyev 2021).

Thus, a recent 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 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.

A more well-known situation is the leak of Yandex.Food users' data, as a result of which personal data of 58 thousand users became publicly available. 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 (In 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. It should be noted that 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.

An analysis of judicial practice leads to the conclusion that, as a rule, no one is looking for the culprit; the 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 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. Thus, by a resolution of the magistrate's court of the court district No. 374 of the Tagansky district of the city of Moscow, 1C-Bitrix LLC was brought to administrative liability in the form of an administrative fine in the amount of 60 thousand rubles, which, apparently, is typical for this category of cases. In each case considered, a fine is applied in the specified amount, regardless of the consequences of the leak of personal data and the number of affected personal data subjects, and the damage caused to them. The court found the unlawful access to personal data information systems

36 Meta Platforms (social networks Facebook and Instagram) are prohibited in Russia

of the "Applicants" database, which resulted in the dissemination of personal data of registered users of the 1C-Bitrix LLC website to an unlimited number of people by posting them on the Internet. The court is limited to the conclusion that the operator must ensure the security of access to the personal data of its clients; however, the measures taken by the operator are not examined in detail. It is noteworthy still that in this case the court, when imposing a punishment, took into account the behavior of 1C-Bitrix LLC after the offense was committed, and the fact that the company strengthened measures to protect clients' personal data. At the same time, this did not change the sanction applicable in the case (In 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).

In another case regarding Laboratory Gemotest LLC, the court did not take into account the fact that the cause of the leak of personal data was the unlawful actions of third parties. The court only took into account that the fact of committing an administrative offense is confirmed by the totality of evidence in the case: a protocol on an administrative offense, an act of an unscheduled on-site inspection, a copy of the order to eliminate the identified violation, a certificate of the results of an unscheduled on-site inspection, a survey protocol, screenshots of the information database, screenshots of the website with a list of clients, a conclusion of an internal audit, a report from Kaspersky Lab JSC, and other case materials (In Decision of the Perovsky District Court of Moscow dated September 8, 2022 in Case No. 12-2741/2022).

This position of law enforcement officials may be assessed twofold. On the one hand, there is indeed a subject who can be held accountable and must ensure the measures taken necessary for the confidentiality of personal data. On the other hand, persons who, in reality, through their malicious actions, have unlawfully accessed personal data, go unpunished, and leaks continue to occur.

In Russia, the activities of exchanges of personal data and darknet forums (Trends.rbc.ru n.d.) where you can leave a request to purchase certain personal data are known. Certain risks for personal data leakage are posed by new services, such as the cloud storage service for users' data and ChatGPT, an artificial intelligence service on which individuals post their personal data and which is also not protected from possible cyber-attacks and the unlawful receipt and use of personal data. All this affects the daily life of citizens and hinders the effective application of legislation on personal data, the right to confidentiality and the protection of personal data.

In modern Russia, there are several large digital ecosystems: Sberbank, Tinkoff, Ozon, Yandex, VK, MTS, and some others, that provide users with diverse products: from taxi to banking services. The issues of protecting personal data of users of digital ecosystems include the following: the legality of requesting a single consent from the user for all platforms of the digital ecosystem, synchronization of ecosystems with the Unified Portal of State and Municipal Services, access of the owner of the digital ecosystem to a wide range of data of users (Burova 2023). Problems with the confidentiality of personal data also arise abroad. Recent cases include a hacker hack of the Microsoft-owned Outlook email client (Bleepingcomputer.com 2023).

Thus, the question arises of how it is possible to ensure and improve the confidentiality of personal data in the current situation: cyberattacks and cyber threats, in the situation in which personal data can become publicly available on the Internet and used by attackers.

CHANGES IN LEGISLATION REGARDING PERSONAL DATA LEAKS

In accordance with the part 3.1 of the 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 the interaction with operators within its jurisdiction (part 10 of the 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 and 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 are expressed and bills are proposed to improve the current legislation on personal data. By analogy with the European data protection regulation GDPR, it is proposed to establish turnover fines against operators who have committed unlawful or accidental transfer (provision, distribution, and

access) of personal data, that is, in essence, is a leak of personal data. It is proposed 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. These were noted in the List of Instructions of the President of the Russian Federation following the meeting of the Council for the Development of Civil Society and Human Rights, held on December 07, 2022. Thus, the Government of the Russian Federation was instructed to consider establishing turnover fines in relation to companies that leak personal data, strengthening responsibility for their illegal trafficking and other violations of legislation in the field of personal data, and submit proposals for introducing appropriate changes to the legislation of the Russian Federation. In this regard, the proposal on the minimum amount of a turnover fine for operators who compensated for the damage from the leak of personal data to the majority of victims seems interesting (Rbc.ru 2022).

Amendments to the legislation have been adopted in the first reading, the purpose of which is to tighten liability for personal data leaks, as well as eliminate their consequences. Thus, in order to fulfill these instructions, the State Duma of the Russian Federation is considering Bill No. 502104-8 "On Amendments to the Code of the Russian Federation on Administrative Offences", which, in general, tightens responsibility, differentiates it depending on the number of personal data subjected to leakage, and the affected subjects of personal data. In case of repeated violation of the duty of confidentiality of 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 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 ways.

The issue of insurance against personal data leaks is also being considered in the doctrine and practice. The idea is in concluding agreements with an insurance organizations or creating 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 (Ratushny 2024), 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.

DOCTRINAL APPROACHES TO RESOLVING SITUATIONS WITH CYBER TREATS

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. It is also important to use anti-virus programs and not to download any data from questionable sites, which could lead to a leak of personal data (Barkov and Kiselev 2022). In this sense, the emphasis is on the need for subjects of personal data to take some kind of self-defense measures, which allows them to ensure the safety of their own personal data.

Nowadays a person, without even realizing it, provides a huge amount of information about himself or herself to a variety of companies every minute. Moreover, even the smallest particles of such information can recreate the complete image of a person (Gribanov 2018). The more personal data about a person is collected and processed, the higher the risks of violation of his or her rights to the protection of personal data (Savelyev 2015). All this is a prerequisite for personal data leaks and gives rise to different problems in law enforcement. However, it seems that much in taking measures to protect personal data should also depend on personal data operators and on what measures to prevent and eliminate personal data leaks they take. Accordingly, it seems illogical to assign the full legal consequences solely to the subjects of personal data who act as consumers.

Another author, V.V. Arkhipov (2018), correctly points out that recognizing personal data not as goods, as some in the doctrine indicate (Nokhrina 2013), but as an intangible benefit, will help to combat violations in this field. M.A. Rozhkova and V.N. Glonina (2020) acknowledging the existence of the concept of personal data as a commodity, 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 (Uroshleva 2018). 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 (Soldatova 2023), 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 (2023) also notes that we should avoid uniform user consent for the processing of his or her 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. 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.

CONCLUSION

It seems that in 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 what was the exact cause of the leak of personal data and how it can be prevented in the future.

Only an integrated approach, consisting of both preventing harm and assessing an operator's activities for violations, can change the current situation with the circulation of personal data. It seems that 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 as well as in other countries and minimize the negative consequences of the state, business and society.

REFERENCES

1. 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.
2. Barkov, A.V., and A.S. Kiselev. 2022. Legal Support of Information Security: Tools to Counter Cyber Threats. Zhurnal Prikladnyh Issledovanij. Pravo 5: 91-96.
3. Burova, A.Yu. 2023. Digital Ecosystem as a Way of Doing Business: a Legal View. Current Issues of Russian Law 11: 111-117.
4. Gribanov, A.A. 2018. General Data Protection Regulation: Ideas for Improving Russian Legislation. Zakon 3: 149-162.
5. Nohrina, M.L. 2013. The Concept and Signs of Intangible Benefits: Legislation and Civil Science. Izvestiya Vysshih Uchebnyh Zavedenij. Pravovedenie 5: 143-160.
6. Rozhkova, M.A., and V.N. Glonina. 2020. "Personal and Non-Personal Data as Part of Big Data". In Pravo Cifrovoj Ekonomiki. Ezhegodnik-Antologiya. Ser. «Analiz Sovremennogo Prava / IP & Digital Law», edited by M.A. Rozhkova, 271-296. Moscow: Statut.
7. Savel'ev, A.I. 2021. Scientific and Practical Article-by-Article Commentary on the Federal Law "On Personal Data". Moscow: Statut.

8. Savel'ev, A.I. 2015. Problems of Application of Legislation on Personal Data in the Era of "Big Data". Pravo. Zhurnal Vysshej Shkoly Ekonomiki 1: 43-66.
9. Soldatova, V.I. 2023. New Legislative Measures to Protect Personal Data. Pravo i Ekonomika 3: 25-30.
10. Uroshleva, A. 2018. "Commercialization of Personal Data and the Concept of "Big Data" are Topical Issues in the IT Field". https://www.garant.ru/article/1229761/
11.