Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Overcoming Illegal Cross-border Transfer of Personal Data

Dmitry V. Bakhteev ✉
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Anna M. Sosnovikova
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Evgeniy V. Kazenas
Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia

Keywords

communications,
computer network,
cross-border data transfer,
digital technologies,
incident,
information security,
information,
law,
legislation,
personal data

Abstract

Objective: to form of a comprehensive interdisciplinary legal and technological risk management model in the field of illegal cross-border transfer of personal data by eliminating legislative gaps and creating a system for automated control of outgoing information flows, as well as expert response to identified incidents.

Methods: in addition to general dialectical and general scientific methods, special legal and cybernetic methods were used. For example, based on comparative legal analysis, the authors reveal differences between national and international regulation of cross-border flows of personal data. In the second section, the modeling method allows forming an algorithm for identifying information security incidents in the field of cross-border transfer of personal data and responding to them.

Results: the article formulates proposals to optimize legislation in the field under study by introducing specialized protective norms for violating the rules of cross-border transfer of personal data and stipulating the operator's obligation to notify personal data subjects of the intention to transfer the information abroad. The second section describes the concept of a software package designed to detect information security incidents in the field under consideration, as well as a model of action of an authorized representative of the operator after receiving a signal from the automated system.

✉ Corresponding author

Scientific novelty: to solve the set problem, the work combines the knowledge and competencies of legal scientists and specialists in the field of information security, which allows an interdisciplinary approach. At the same time, it is stated that the issues of illegal cross-border transfer of personal data have not received proper coverage in science today, since Russian legislation in this area has changed recently. The authors propose not so much to strengthen the sanction for legislation violation in this area, as to ensure the punishment of persons who commit cyberattacks, and to equip personal data operators with an effective tool to minimize the risks of information leakage.

Practical significance: the research results can be used to improve legislation in the field of cross-border transfer of personal data and the organization of activities of authorized employees of the personal data operator for risk management in this area.

For citation

Bakhteev, D. V., Sosnovikova, A. M., Kazenas, E. V. (2024). Overcoming Illegal Cross-border Transfer of Personal Data. *Journal of Digital Technologies and Law, 2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Contents

Introduction
1. Legal aspects of cross-border transfer of personal data
   1.1. History of the legal relations in the sphere of cross-border transfer of personal data
   1.2. Regulation of cross-border transfer of personal data by the legislation of the Russian Federation and international laws
2. Technical and technological aspects of cross-border data transfer
   2.1. Main technical communication channels through which the cross-border transfer of personal data is carried out
   2.2. Model for identifying the facts of illegal cross-border transfer of personal data through technical means and responding to them
Conclusions
References

Introduction

The rapid development of technology and society as a whole has led to the blurring of borders between countries in the virtual space. This phenomenon entails many positive consequences: the possibility of international communication, the availability of foreign education, the ability to buy goods from abroad, etc. However, it is not without

negative manifestations, one of which is the illegal cross-border transfer of personal data.

Today, Russia has fairly strict rules for such transfers, as a result of which personal data operators are not always able to accurately comply with them. In addition, more and more malicious attacks are carried out every year; as a result, personal data of a wide range of people become publicly available on foreign servers, which violates the constitutional rights of citizens, undermines the national security of the state and results in significant fines for legal entities.

In this regard, our goal was to propose an optimal comprehensive legal and technological model for minimizing the risks of illegal cross-border transfer of personal data, while maintaining a balance of interests of all parties. To achieve this goal, we have solved the following tasks: studied the history of the relations in this area; analyzed the current national and international regulations governing the cross-border transfer of personal data; formulated proposals to optimize these standards; established the main channels through which personal data can be transferred abroad; established the nodes through which it is possible to prevent unauthorized flows; and proposed an algorithm for identifying information security incidents in this area and responding to them.

We believe that the practical implementation of the proposals outlined in this paper and the focus on the issues raised will not only be of interest to the scientific community, but will also reduce illegal cross-border flows of personal data.

1. Legal aspects of cross-border transfer of personal data

1.1. History of the legal relations in the sphere of cross-border transfer of personal data

Today, personal data is a priori associated with “sensitive” information (Ji et al., 2023), the unauthorized access of which by third parties is extremely undesirable. However, this was not always the case: for a long time, the world was dominated by an order in which, on the one hand, the rights of an individual did not matter; on the other hand, there were no globalization phenomena generating active international interaction at the private level. In this regard, the phenomenon of personal data did not refer to legal regulation, and there was no cross-border transfer of such information in principle. Personal data could only get to another state together with the person or their imminent arrival in that state (for example, when traveling or as part of sending diplomatic representatives from one country to another). At the same time, if the “identity” of someone was stolen and illegally used abroad, this fact did not affect the life of the one whose data turned out to be in the possession of the attackers.

At the same time, the development of society gradually led to systemic changes in the field of personal data: for example, during the Great French Revolution, the question of respect for the individual and their freedoms, including the right to personal privacy, was raised.

In the Russian Empire, such rights were legalized on the initiative of the Emperor: Alexander II adopted Postal and Telegraphic Statutes, which enshrined the inviolability of private life and the secrecy of correspondence. The Criminal Code also provided for sanctions for violation of these norms (Balashkina, 2007). Such a guarantee of privacy was excluded from the legal sphere after the Great October Revolution; however, provisions of the inviolability of the person and the secrecy of correspondence reappeared in the USSR Constitution in 1936[1].

However, in a strict sense, the concept of personal human rights was still very far from the well-established understanding of personal data and their protection regime today. The first relevant phenomenon that approximates modern realities was the theory of American legal scientists S. Warren and L. Brandeis, who in 1890 formulated the concept of privacy as the right to "be left alone" (Balashkina, 2007). About half a century later, a judicial interpretation of this category was given, from which it follows that privacy means the inviolability of personal data and this principle follows from the first amendments to the US Constitution.

The concept of personal data was widely developed only in the second half of the 20th century. At about the same time, against the background of incipient digitalization and intensifying globalization, the phenomenon of cross-border transfer of such information arose.

We must make a reservation that by cross-border data transfer we mean the situation when a specific person (operator) transferred data, including without notifying the subject, from the state in which the subject voluntarily provided the operator with certain information that allows identifying them (unambiguously establishing their identity) to another state, and provided access to the information to third parties. Thus, we do not consider the situation when a subject of information independently communicates their data to representatives of another state, for example, in the case of traveling abroad, when a person provides her passport when checking in and her data is entered into the foreign hotel database. The same applies to legislative norms, which will be discussed below.

The international community's interest in the described phenomenon took shape only after the beginning of the "computer age" (Romansky Noninska, 2020; Zheng, 2021), since at that time many risks associated with the lack of uniform standards for interstate turnover of personal data and their protection in the process of such turnover became apparent.

On the one hand, obtaining various rights and privileges and implementation of the natural interests of people in the era of widespread Internet is almost impossible without cross-border flows of various personal data (Fuentes, 2020). This is due to the development of international business, when a founder is located in one state, and

[1] Glushkova, S. I. (2002). Human rights in Russia: theory, history, practice: tutorial. Yekaterinburg.

its branches and representative offices operate in many countries. Other examples include remote registration of foreign business trips by an internal personnel service; the referral of a seriously ill person to another state for treatment and many other, often quite routine situations (Artemova, 2023). Separately, it is necessary to describe the practice that was widespread in Russia before 2015 and related to the use of foreign databases located outside the Russian Federation for storing personal data obtained by domestic companies. Such use of third-party resources was due to their cheapness and existence as such (Smolensky & Levshin, 2016), since earlier in Russia, there was no demand for its own reliable and accessible databases of various sizes capable of processing significant amounts of information and withstanding malicious attacks. Similar problems are also considered in foreign publications (Abdulrauf et al., 2023).

On the other hand, personal data is a very valuable resource in the modern world. Their legal processing allows commercial companies to produce products more adapted to the interests of the target audience, create targeted advertising, attracting new customers and increasing profits. For states, personal data is necessary in order to combat crime and various kinds of offenses (using cameras with automatic face recognition, conducting genomic and fingerprint identification, etc.), aggregate statistical data on the population (health status, standard of living, etc.), forecast political decisions that will receive support of the population, etc. At the same time, personal data is also of interest for intruders, since they enable them to perform various kinds of theft, discredit a specific person in the media space, encrypt their own identity when carrying out illegal actions, etc.

Thus, a multilateral conflict of interests is formed even within one state: citizens advocate for the inviolability and secrecy of their own personal data (Abramova, 2020); commercial organizations seek to increase the profitability of their business by using customer information; intruders try to steal personal data in order to facilitate or ensure commitment of criminal acts; and the state strives for sole control over the maximum amount of information about its citizens.

The situation is aggravated if we add a cross-border factor, since the subjects of personal data have significantly reduced control over information about themselves. In the commercial sector, competition increases which means the increased demand for large amounts of personal data of potential consumers. It becomes easier for attackers to remain unpunished and unidentified if they distribute various stages of criminal activity in different countries with different legal regimes, conditions for the protection of personal data and rules for the extradition of criminals. States, on the other hand, lose some control over the personal data of their citizens and at the same time acquire the potential ability to obtain relevant information about residents of other countries, which can become an instrument in international counteraction and political pressure.

Legislative and international norms are designed to find a balance between the private interests of individual freedom, the commercial interests of companies and the desire of states to ensure security. It seems that modern legal norms fully provide a compromise in these relations, but they are based on the presumption of good faith of all parties to interaction; hence, the criminal element is omitted. At the same time, the greatest threat to the natural rights of citizens, to the commercial interest of organizations, and to the national security of states is the malicious theft of personal data or violation of their secrecy, as a result of which information about people gets into an open network.

For example, in 2023 alone, 168 leaks of personal data were identified, the largest of which were:

– from the Sberbank "Spasibo" loyalty program – 52.5 million entries;
– from the "Sportmaster" sportswear sales network – 46 million entries;
– from the zdravcity.ru online pharmacy – 8.9 million records;
– from the "Kassy.ru" service – 4.5 million records;
– from the "Zoloto585" jewelry store – 9.9 million records;
– from the "Sogaz" insurance company – 8.3 million records.

The situation of obtaining unauthorized access to the personal data of 1,000,000 MTS Bank users deserves special attention. In total, three files with personal information of clients were unlawfully made public. The first one included a million lines with names, phone numbers, gender, INN, and citizenship. The second one had three million records with types, part of the 16-digit card numbers and their release dates. The third file included 1.8 million phone numbers, 50 thousand e-mails and user IDs[2].

One of the most large-scale incidents occurred in the summer of 2024, when information processed by the Moscow Department of Information Technology, as of September 2023, became publicly available. The published file contains 13,462,446 lines with the following information about Muscovites and guests of the capital who used digital services:

– last name, first name, patronymic;
– phone number (7.2 million unique numbers);
– email address (4.8 million unique addresses, more than 16 thousand of which are on the @mos.ru domain);
– address of registration and actual place of residence;
– date of birth;
– series, number of passport or birth certificate;
– place of birth;
– number of a Muscovite's social card;
– number of the compulsory health insurance policy[3].

---

2 Talash, A. Leakage of personal data: high-profile scandals, who was fined last year and how will they be punished in 2024? Rosco. https://clck.ru/3EmK8s

3 Nefedova, M. The Moscow Department of Information Technology stated that the data published by hackers is a compilation. Khaker. https://clck.ru/3EmK9J

We point out that, at the time of writing, the Moscow Government does not confirm the fact of leakage, reporting the compilation of data freely available on the network due to the fault of the citizens or as a result of a security breach by other operators.

In all the described situations, the personal data of Russians also got to the information resources of foreign countries, i.e. there was an obvious illegal cross-border data transfer based on the broken dam principle. However, the covert transmission of this kind of information abroad is no less dangerous[4].

In total, in 2023, more than 300 million records with personal data of Russian citizens became publicly available, which resulted in fines for businesses totaling over 4.6 million rubles[5]. These are statistics for the Russian Federation only, whereas the problem is global (Jurcys et al., 2022). However, it seems that tightening the liability of legal entities for ongoing violations of the confidentiality of users' personal data is not an optimal measure, since it is aimed at resolving symptoms, but not combating the root cause – hackers carrying out cyberattacks. This situation is connected, in our opinion, with the difficulty of detecting leaks when confidentiality has already been violated, but the data has not yet become widely available, as well as with the fact that criminals belong to other states and use high-tech means of encrypting their own identity and actions. In this regard, it seems necessary, on the one hand, to develop international and national legislation in terms of punishing those really guilty of violating the inviolability of personal data, and on the other hand, to create and implement special technological means of detecting and blocking illegal cross-border transfer of personal data into the activities of the Russsian Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor). This work is devoted to analyzing the current legislation in the field under consideration and describing the models of such technological solutions.

1.2. Regulation of cross-border transfer of personal data by the legislation of the Russian Federation and international laws

In the Russian Federation, the basic provision defining the procedure for the cross-border transfer of personal data is Article 12 of Federal Law No. 152-FZ of July 27, 2006 "On personal data"[6] (hereinafter – 152-FZ), which has undergone four revisions since 2006. Initially, it had only three parts; today, with the latest amendments of July 14, 2022, it consists of 15 parts. This clearly confirms the trends, on the one hand, towards the

[4] Explanatory note to the draft Federal Law "On amendments to the Federal Law 'On personal data' and other legislative acts of the Russian Federation on the protection of the rights of personal data subjects". System of ensuring legislative activity (SOZD). https://clck.ru/3EmKC8

[5] Roskomnadzor recorded 168 data leaks in 2023. Право.ru. https://clck.ru/3EmKCx

[6] On personal data. No. 152-FZ of 27.07.2006. (July 31, 2006). Collection of legislation of the Russian Federation, No. 31 (part I), Art. 3451.

intensification of globalization processes, and on the other hand, towards an increase in cases of such cross-border data transfer, which, without being directly prohibited by law, violates the legitimate rights and freedoms of citizens and the interests of the state as a whole. We will not delve into the historical comparison, focusing on the current regulation of the issue.

The modern edition of the Article regulates in detail the procedure for the cross-border transfer of personal data, according to which:

1. The list of states to which personal data may be transferred from Russia is conditionally limited to those countries that are either members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, or provide high standards of personal data protection under national legislation.

2. This rule is not absolute, since in extreme cases it is possible to transfer personal data to other states.

3. Any operator of personal data is obliged to send to the authorized body – Roskomnadzor[7] – a separate motivated notification of the intention to transfer personal data abroad, indicating the purpose of the transfer, the country and specific recipients of this information.

4. Roskomnadzor may decide to ban the transfer of personal data to a certain state or in a certain situation.

5. This possibility is not absolute, but the range of grounds is very wide, including:

– protection of the constitutional system of Russia, morality, health, rights and legitimate interests of citizens;

– ensuring the country's defense and state security;

– protection of the economic and financial interests of the Russian Federation;

– ensuring diplomatic and international-legal means of protecting the rights, freedoms and interests of citizens of the Russian Federation, sovereignty, security, territorial integrity of the Russian Federation and its other interests in the international arena.

6. If a decision is made on the inadmissibility of the personal data transfer when such transfer has already taken place, then the transferred personal data must be destroyed, for which the original operator is responsible.

It should also be noted that Article 12 of 152-FZ provides that the cross-border transfer of personal data is carried out in accordance with the above-mentioned Federal Law and international treaties of the Russian Federation, which, under the Russian Constitution, cannot be adopted if their provisions or interpretation contradicts the Constitution. In this regard, when analyzing international acts, we consider it advisable to focus only on documents ratified in the Russian Federation.

---

7 Resolution of the Government of the Russian Federation No. 228 of 16.03.2009. https://clck.ru/3EmKGN

The central international treaty applied to solve the issues of cross-border transfer of personal data is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[8] (further – Convention). This convention was adopted in 1981 and slightly modernized in 2018 (there were included norms regulating the use of systems based on artificial intelligence technology for automated processing of personal data). Initially, 44 states signed the document; today 55 states are its members on an equal basis with Russia: Albania, Andorra, Argentina, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Burkina Faso, Cape Verde, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Great Britain, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Turkey, Ukraine, and Uruguay.

This act regulates the relations arising from the storage of personal data, i.e. any information about a certain or identifiable natural person: the implementation of logical and/or arithmetic operations with this data, their modification, destruction, search or dissemination, if these actions are carried out in whole or in part using automated means. In general terms, the Convention provisions are similar to the norms and guarantees enshrined in 152-FZ, since it was on the basis of the Convention that the Russian law was adopted. However, as is natural for international agreements, the Convention has a more dispositive character, leaving wide scope for the discretion of the contracting parties. We will not dwell on the review of this Convention, but will highlight only the norm that directly relates to the topic of this study.

Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regulates the specifics of cross-border transfer of personal data, establishing as a general rule that the Parties may not prohibit or restrict cross-border flows of personal data between themselves only for the reason of protecting privacy. However, there are two exceptions to this rule – in the following situations, the Parties are free to prohibit or restrict the transfer:

1) the legislative regulation of the processing of a particular category of personal data on the side of the outcome differs from similar norms in the receiving state;

2) personal data will be transferred from the territory of the receiving state to a country that is not a Party to the Convention.

Thus, despite the seemingly strict rule guaranteeing the free transfer of personal data between the Parties to the Convention, there are two rather broad exceptions to it.

[8] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (Strasbourg, January 28, 1981). (February 3, 2014). Collection of legislation of the Russian Federation, No. 5, Art. 419.

Moreover, it is not as strict as it may seem upon a superficial analysis. While prohibiting restrictions based on the privacy protection, the provision in question does not prohibit states from using other grounds for such restrictions. For example, in Russia it is stipulated that cross-border data transfer may be restricted or prohibited in order to ensure national security and for other equally valid and weighty reasons. From this one may conclude that the provisions of Article of 152-FZ and Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data do not contradict each other; national legislation only regulates issues in more detail, providing greater protection for the personal data of its citizens.

We believe this approach to be correct, because, as it was shown above and noted by researchers, personal data is sensitive information, the access of which by intruders can significantly harm both a particular citizen and society as a whole (Akulin et al., 2020). However, the current normative and organizational regulation of cross-border transfer of personal data is far from perfect. There is an opinion that the most correct model is free transfer of personal data between countries, while conditional or prohibitive regulation negatively affects the processes of international interaction (Ferracane van der Marel, 2024). However, in our opinion, this viewpoint focuses exclusively on the interests of business and ignores the issues of human rights, national security and the risks of criminal activity in this area. Therefore, it is necessary to develop a more consensual protective model.

First of all, it should be noted that, as is known, a rule of law should consist of three elements: a hypothesis (describing public relations subject to regulation), a disposition (indicating required or prohibited behavior in these public relations) and a sanction (providing punishment for violation of requirements (prohibitions) to behavior). If any of these parts is missing, then the norm is "dead" and will not actually be applied, losing its regulatory force. In this regard, for the strict rules for the cross-border transfer of personal data established by Article 12 of 152-FZ to be observed, a liability for their violation should be provided. The situation with latter is not so clear. Article 13.11 of the Administrative Code of the Russian Federation, consisting of nine parts, provides for liability for various violations of the legislation on personal data. However, there is no special rule regarding the cross-border transfer of such information; hence, it is necessary to turn to the general part.

Part 1 of Article 13.11 of the Administrative Code of the Russian Federation says that "processing of personal data in cases not provided for by the legislation of the Russian Federation in the field of personal data, or processing of personal data incompatible with the purposes of collecting personal data, entails the imposition of an administrative fine on citizens in the amount of 2,000 to 6,000 rubles; on officials – from 10,000 to 20,000 rubles; on legal entities – from 60,000 to 100,000 rubles"[9].

[9] Administrative Code of the Russian Federation of December 30, 2001, No. 195-FZ. (January 7, 2002). Collection of legislation of the Russian Federation, No. 1 (part I), Art. 1.

However, the application of this rule seems difficult due to the very vague wording of the disposition. On the one hand, almost any operator's action may fall under cases not provided for by law or incompatible purposes; on the other hand, one may easily imagine a situation when formally legal, but in fact illegal cross-border transfer of personal data is carried out. In addition, the sanction of this norm, if imposed on the situation of illegal cross-border transfer of personal data, turns out to be very insignificant, because the profit from these illegal actions can exceed the amount of fines by tens or even hundreds of times.

At the same time, Roskomnadzor's practice follows a different path: for such violations organizations involved are suited under Part 9 of Article 13.11, which provides that "the failure of the operator collecting personal data, including via the Internet information and telecommunications network, to fulfil the obligation provided for by the legislation of the Russian Federation in the field of personal data to ensure the recording, systematization, accumulation, storage, clarification (updating, modification) or extraction of personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation, entails the imposition of an administrative fine on citizens in the amount of 30,000 to 50,000 rubles; on officials – from 100,000 to 200,000 rubles; on legal entities – from 1,000,000 to 6,000,000 rubles"[10].

Undoubtedly, the sanction in this case is much more significant, but formally, the cited norm introduces liability only for one particular case of illegal cross-border transfer of personal data – non-use of domestic databases, which violates the rule introduced in 2015. However, this regulation appeared only in 2019. A similar situation can be observed today – introduced in 2022, the complicated procedure for the cross-border transfer of personal data is currently not provided with a sanction for violating its rules, which negatively affects the regulatory mechanism. We believe that there is an urgent need to elaborate and adopt a special protective norm aimed at preventing illegal cross-border transfer of personal data. At the same time, we believe that the disposition of such a rule should fix an intentional form of guilt so that personal data operators are not subject to punishment for a cyberattack committed on them. This will reduce the latency of such incidents, ensure the cooperation of operators with law enforcement agencies and the implementation of the sanction fairness principle, as it will be directed against the really guilty persons. Simultaneously, especially in an unfriendly international atmosphere, we consider it necessary to introduce an additional qualifying feature in Articles 272, 273, and 274.1 of the Criminal Code of the Russian Federation, for them to enshrine the consequences in the form of obtaining unlawful access to legally protected computer information by persons located outside the Russian Federation.

[10] Administrative Code of the Russian Federation No. 195-FZ of 30.12.2001 (ed. of 23.11.2024). (2024). SPS KonsultantPlyus. https://clck.ru/3ExqcF

The next problem is related to the requirement of Article 12 of 152-FZ, according to which, if Roskomnadzor decides to ban or restrict the cross-border transfer of personal data, "the operator is obliged to ensure the destruction by a foreign state authority, a foreign individual, or a foreign legal entity of the personal data previously transferred to them"[11]. It seems unlikely that the government of a foreign, especially unfriendly, state will delete personal data previously received from Russia on the instructions of any commercial company from our state. There is no mechanism by which this requirement can be implemented. Thus, taking into account the notification procedure for the cross-border transfer of personal data to states that are Parties to the Council of Europe Convention or provide an adequate level of personal data protection (34 more states)[12], as well as the possibility in exceptional cases to carry out cross-border transfer to other states, there appears a very significant risk of leakage of personal data of Russians and their abandonment on hostile territory, after Roskomnadzor decides that the transfer should not have taken place.

Apart from special norms, we can identify another possibility for citizens to protect their personal data from cross-border transfer. As enshrined in paragraph 8, part 7 of Article 14 of 152-FZ, the subject of personal data has the right to receive information about the implemented or proposed cross-border transfer of their data. The systematic interpretation of Part 2 of Article 9 and Part 1 of Article 14 of 152-FZ provides that the subject of personal data may at any time withdraw their consent to their processing and may require the operator to delete their personal data. If a person does not agree with the cross-border transfer of their personal data, they may prohibit the operator from carrying out such actions. However, all the described processes must be initiated by the subject, as the operator is not obliged to report on the planned or ongoing cross-border transfer of personal data until a request for the relevant information is received from the subject. At the same time, most citizens, not having a properly developed legal culture, may not be aware of these features, and therefore they are unable to protect their interests in practice. In addition, even being aware of the above legal provisions, a person is not able to track down all operators potentially carrying out or planning to carry out cross-border transfer of her personal data, since there are many such operators per one subject.

In this regard, we consider it necessary to supplement Article 12 of 152-FZ with a rule providing for mandatory notification of the personal data subject of the intention to make a cross-border transfer of information referring to them, as well as to provide them with the opportunity to limit such transfer to a certain state or in specific situations.

---

11 On personal data. No. 152-FZ of 27.07.2006 (ed. of 08.08.2024). (2024). SPS KonsultantPlyus. https://clck.ru/3Exr2K

12 Order of the Federal Agency for Supervision of Communications, Information Technology and Mass Communications No. 128 of 05.08.2022. https://clck.ru/3EmKNQ

Despite all of the above, it should be recognized that comprehensive measures are being taken in Russia to ensure maximum protection of personal data of persons residing in the state. For example, one has to mention the Federal Law "On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing personal data in information and telecommunications networks" dated July 21, 2014, No. 242-FZ (the so-called Localization Law). It amended 152-FZ, stipulating that the recording, systematization, accumulation, storage, clarification (updating, modification), and extraction of personal data of the Russian Federation citizens must be carried out using databases located on the territory of the Russian Federation[13].

This requirement seems to be very effective for protecting the personal data of the Russians, minimizing the risks of information leaks, ensuring state control over information about their citizens, and eliminating the risk of situations where the personal data of Russian citizens will be inaccessible to domestic companies and the state due to blocking of certain foreign services or disconnecting Russian users from foreign databases, or will be used to commit crimes. However, not everyone adheres to this position – for example, in 2015, when the described norm was just coming into force, scenarios were developed to circumvent it in order to minimize business losses (Veselitsky, 2015). In this regard, today we can expect a wide spread of shadow schemes that actually allow storing personal data of Russian citizens abroad.

From all of the above, we can conclude that the regulation of the issue under study cannot adequately protect the personal data of Russians. However, preventing cases of illegal cross-border transfer is a fundamental task of the Russian state, on which the security the country's population and the stability of state power rely. In this regard, it is necessary not only to improve legislation, but also to develop technological mechanisms that would effectively identify and block suspicious flows of personal data outside the territory of the Russian Federation until all the circumstances are clarified and a qualified decision is made.

2. Technical and technological aspects of cross-border data transfer

2.1. Main technical communication channels through which the cross-border transfer of personal data is carried out

Before we describe the technical means of preventing illegal cross-border transfer of personal data, it is necessary to identify the channels of potential information leakage. Currently, the transfer of personal data, which may pose a threat, is carried

[13] On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing personal data in information and telecommunications networks. No. 242-FZ of 21.07.2014. (2014). https://clck.ru/3EmKSW

out via computer networks. Certainly, many companies keep paper personal files of employees, for example. However, it seems unrealistic that identifiable information, entirely in analog form, will be obtained from them in large quantities, stored, transferred across the border and published to be accessible to a wide range of people, including for the purpose of their subsequent criminal use. That is why we will consider the technical communication channels represented by computer networks.

To predict the level of threat from illegal access to information, as well as to determine the possibilities of minimizing cyberattacks and leaks, it is important to accurately determine the territory within which the communication channel operates. The following can be distinguished:

Global networks. The most famous of them is the Internet; they encircle the whole world. Global networks also include intra-national networks operating within a particular country or region. It is almost impossible to ensure full protection of information in such networks due to the principle of openness and accessibility underlying their operation.

2. City networks. It is obvious from the name that they exist within a city. However, more often this level includes only networks serving megacities or urban agglomerations. It was at the level of city networks that the special Web software was initially organized.

3. Corporate networks (networks of organizations and enterprises). Networks of this level, on the one hand, are smaller than city ones, since they are aimed at servicing enterprises; but, on the other hand, such networks operate cross-border, i.e. they connect branches and divisions located in different cities, regions and countries.

It should be noted that corporate networks are the most vulnerable from the viewpoint of information security and protection from cyberattacks. The reason is, they cover a significant territory, but are serviced by the private sector, which is limited in resources for constant updating of security protocols and is not bound by strict information protection rules, like state-owned enterprises.

At the same time, departmental communication channels also belong to corporate networks. Their security level is the highest, since they transmit restricted information.

4. Local networks are concentrated in a small area (usually within a radius of 1-2 km). They operate on the territory of one enterprise (factory, hospital, educational institution, etc.). Usually such networks are well protected, as they are organized in a sector where the turnover of legally protected information is carried out in a limited area and through identified terminal equipment, with sufficient resources to set up and maintain security systems.

5. Personal networks are designed for the interaction of devices belonging to the same owner (family members), at a short distance (usually up to 10 m). Despite their low territorial distribution, an individual may not pay enough attention to compliance with the rules of information security and digital hygiene, which puts this infrastructure at risk.

As is obvious from the above classification, cross-border transfer of personal data can be carried out exclusively via global and corporate networks. However, in the latter case, such information is protected and, if an incident occurs, security is violated, then the information is transmitted to global networks, where it becomes available to a wide range of people, including representatives of other states. In this regard, an intermediate conclusion can be drawn that the control of illegal cross-border transfer of personal data is most effective at the border of a secure communication channel and a global network. This approach minimizes the risks of false positive errors when legal internal flows (between government agencies, between divisions of a legal entity, between devices of the same user) are blocked.

To substantiate this thesis, it is necessary to focus in more detail on the characteristics of global computer networks. Their main characteristic feature is that they have a decentralized architecture, are distributed across continents, countries, and can physically be located not only on the Earth's surface, but also above it or underwater – anywhere. Some segments of global networks can be duplicated, including via satellite communications. This, together with the previously mentioned fundamental principle of open access, allows creating a system in which any device with access to the global network can interact with any other connected equipment.

Most often, global computer networks rely on dedicated lines, at one end of which a router is connected to the local network, and at the other end a switch is connected to the rest of the global network. These elements will be discussed in more detail later, as they are important for identifying the facts of unauthorized transfer of personal data.

Note that modern computer networks have inherited a lot from their predecessors – telephone lines. The main technological innovation that the former brought was the rejection of the principle of channel switching, in which interaction requires the physical connection of two devices and allocation of a separate channel for their communication. It was replaced by the technology of multi-level packet switching, when information is divided into small blocks that are transmitted to the addressee along different routes.

Due to such structure of global computer systems, it is impossible to control the flow of information (including personal data) when they are inside the system (Ivanova et al., 2010). Therefore, all measures to block the data transmission channel must be carried out at the local level, amenable to centralized administration.

For the issue of preventing unauthorized flows of personal data, it is important to determine, besides the network level, the media through which information is transmitted. It can be:

– optical fiber;
– copper wires;
– infrared channel;
– radio channel (Wi-Fi, LTE, Bluetooth, etc.).

It is the easiest to intercept, and therefore block, information transmitted through material media – optical fiber and copper wires. In this case, as will be shown below, a technical device that detects unauthorized flows of personal data can be installed directly on the channel. However, in this case, it is very difficult to determine the type of data being transmitted – for this, it is necessary to decrypt them, which requires additional time and special equipment. Therefore, it is much more useful to have access to the so-called infrastructure nodes – local network equipment, which can be active or passive.

Active equipment is the devices directly connected to networks and therefore providing data transmission and routing. They allow a full cycle of data processing: receiving, systematizing, storing, managing, and transmitting. For this purpose, such devices are equipped with their own processor and RAM.

Passive equipment can be called auxiliary: it is characterized by the absence of its own power source and therefore cannot have any effect on the passing data streams. One can draw a metaphorical analogy with a bridge over a river, when traffic lights and signs regulating the order of movement are installed on both sides of it, but the bridge itself is only a section of road on which it is impossible to obtain new information and modernize behavior under its influence. Similarly, passive equipment only creates an environment for data transmission, without managing traffic or processing data. Passive equipment includes, in particular:

– cables (e.g. twisted pair or fiber optic cable) used to connect devices and transfer data between them;

– connectors, patch panels and cross fields used to connect cables and devices;

– splitters or splice boxes used to separate or unite fiber-optic communication lines.

Thus, the role of passive network equipment is reduced to ensuring more efficient and reliable network operation; therefore, it is difficult to block the flow of personal data on it.

Active network equipment is very diverse and performs a variety of functions:

– distribution of traffic between networks;

– connecting local networks at different levels (from intra-organizational to global);

– providing wireless communication between devices within a local network;

– determining the target direction of data packets.

The latter is of particular interest for this study, since in this way it is possible to establish that certain sensitive data is being sent abroad (to a device whose MAC address is registered abroad).

Based on the above features, it follows that in order to effectively prevent unauthorized cross-border flows of sensitive information, minimize the risks of false

positive and false negative errors in determining the direction of information movement, it is necessary to use specialized technical devices to influence active network equipment.

At the same time, there are many different types of network devices, each with its unique features, characteristics and purpose. Therefore, we will give just a brief description of those that should be influenced in order to prevent unauthorized cross-border flows of personal data.

1. A switchboard. This device, which has temporary (intermediate) memory, connects a finite number of devices into a single network. The number of devices that a switchboard can connect depends on the number of ports it has.

The general principle of its operation can be represented as follows: at the first stage, the switchboard receives data that is transmitted to all ports, while the sender's MAC address is identified and assigned to one specific port. Further, if packets are received intended for a device with an identified MAC address, they are transmitted only to the port assigned to it. Otherwise, the data is transmitted to all ports. Over time, all devices interacting on the network are identified.

In terms of the risks of unauthorized cross-border transmission, the switchboard can be useful for detecting their source (i.e. determining the guilty employee), as well as for identifying the very fact of the personal data transfer.

Similar functions, but on a different, broader scale, are performed by hubs, which differ from switchboards by being more vulnerable to information security threats due to less "intelligence".

2. A router is designed to transfer data packets between different computer networks. To do this, it uses a routing table that contains the MAC addresses of the end devices and the communication paths to them. The router matches the MAC address of the recipient specified in the data packet with the specified table and transmits the information to the recipient. At the same time, the router is a moderated system that operates according to the rules set by the administrator, who can indicate the need for traffic filtering, encryption (decryption) of certain data, and other processing.

Thus, it is best to detect incidents of unauthorized cross-border data transmission at the router level, automating this process by introducing several additional rules at the stage of its installation and configuration. However, the router is not specifically designed for such control, unlike the next element of the network infrastructure.

3. Firewall is a software or hardware-software complex that specifically functions to protect a computer network from unauthorized access, malicious attacks, data theft and other threats from the external environment. The main tasks solved by the firewall are as follows:

– traffic filtering;

– blocking attempts to log into the network from unknown or untrusted sources;

– blocking the transmission (reception) of certain types of traffic (for example, traffic with malicious content or personal data), etc.

Undoubtedly, any of the described devices can be used to detect personal data flows, prevent or at least detect not only their free transfer abroad, but also malicious theft. However, such measures will be most effective when they are applied on routers and firewalls. In the next section, we will consider a somewhat generalized scenario of these protective measures.

2.2. Model for identifying the facts of illegal cross-border transfer of personal data through technical means and responding to them

Before proceeding to the description of the proposed model, we make a reservation that this part of the study will be objectively limited to actions within a legal entity or government agency that serve as personal data operators. Also, we will not consider methods of preventing attacks aimed at stealing personal data, as they are generally reduced to constant updating of security protocols and equipment, compliance with all requirements of technical regulations and Roskomnadzor in this area, and using certified and licensed software. However, these measures do not safeguard against any malicious attacks. Hence, we consider it important to create a mechanism for detecting illegal cross-border flows of personal data, regardless of the reason for which they occurred: as a result of an external breakthrough of the security circuit or as a result of illegal (or erroneous) actions on the part of the operator. This said, since the main problem today is centered on large personal data operators represented by corporations and government agencies, we will focus specifically on detecting flows from local, city and corporate networks, which will be generically referred to as local networks for simplification.

We would like to point out that the basic measure to detect and prevent unauthorized cross-border transfer of personal data is control. Assumingly, it should not only be provided for in local acts and instructions as an obligatory element of network management, but also consist of joint efforts of technical, including automated, devices and humans.

Control of network operation is usually divided into two stages: monitoring and analysis. However, preliminary preparation is of great importance, which implies the development of local acts of the organization, the normative consolidation of the procedure for identifying and processing information about information security incidents and responding to them (Rowe, 2003).

At the monitoring stage, primary data is collected, which will be necessary in the future to analyze the situation and make an informed decision (Pascual et al., 2024). Monitoring, especially in large personal data operators, can (and rather must) be carried out using

technical means. Moreover, we consider it necessary to develop a hardware-software module that can be integrated into the equipment of a specific organization, government agency, adapted to the specifics of the operator's activities and its technical and technological resources, ensuring the effective accumulation of all relevant information. Such a device should work according to the following algorithm:

1. Registering the fact that (any) data is flowing out of the local network.
2. Filtering personal data flows (their detention).
3. Determining the direction of these flows.
   3.1. If the stream is directed abroad, it is blocked.
   3.2. If the flow is internal, it is skipped.
4. Informing the authorized person of the operator about the identified flow, transmitting all the accompanying information (time, source, direction, etc.) to this employee.

At the same time, one can use a software solution, similar to the one that has already proven effective in identifying and processing digital traces of the user (Daniela Amélie, 2022). It should also be noted that, if necessary, such a device can be configured to block any flows of personal data or other information before their preliminary verification by an authorized person.

Next, the authorized employee performs an analysis – comprehension of the information collected at the monitoring stage, comparing it with profile (target) templates and subsequent management decision-making. At this stage, a person should evaluate the following in terms of cross-border flows of personal data:

1) whether they are transferred to a state that is a Party to the European Convention or provides adequate protection of personal data;

2) whether the operator is authorized to carry out cross-border transfer of personal data;

3) whether the notification of this transfer was sent to Roskomnadzor;

4) whether the information specified in the notification correspond to the circumstances and content of the personal data being transferred;

5) whether there is a ban or restriction on the transfer of this personal data to a particular state under existing conditions;

6) whether there was any objection from the personal data subject to transfer their information abroad;

7) whether the purposes of the personal data transfer violate the legislation of the Russian Federation;

8) who is the initiator of the personal data transfer (employees of the organization or an external entity that violated the security of the local network).

After answering all these questions, the authorized person decides whether to allow the cross-border transfer of personal data or inform the head (or law enforcement agencies) about the identified and timely prevented information security incident.

The described model is shown in a general form in Fig. 1.

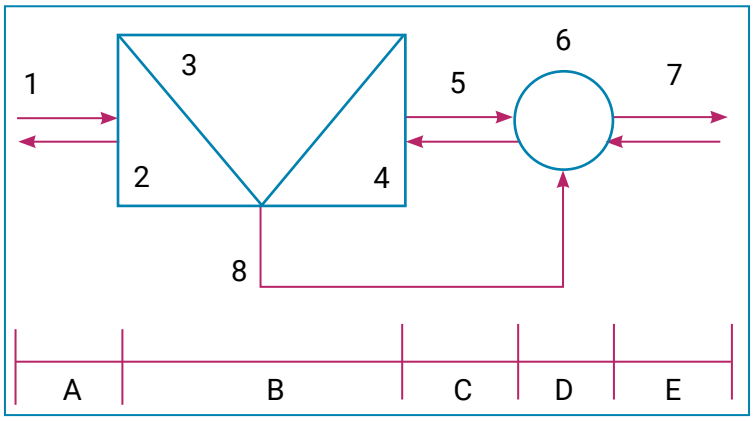

Fig. 1. Graphical representation of the model for identifying the fact of cross-border transfer of personal data and making a managerial decision

In section A, the number 1 shows incoming and outgoing data flows of the physical, network, channel, transport, session, representative, and application levels. Obtaining information from all seven levels of the ISO/OSI model in simple, hierarchical, route, aggregate and other forms for subsequent analysis is necessary, as incoming data, including personal data, may have other than textual representation.

In section B, module 2 shows the identification of the information recipient by analyzing their IP address, domain name, and other similar information and comparing it with official data on the registration of these IP addresses.

Information about the IP address belonging to a geographical (country) location and to a legal entity or individual can be obtained from the official resources of domain name registrars[14]. Obviously, in the model under consideration, the highest priority of trust will belong to domain name registrars operating in Russia (due to the norms of current legislation and regulatory norms of the Federal Service for Technical and Expert Control, the Federal Security Service of the Russian Federation, the Federal Agency for Supervision of Communications, Information Technology and Mass Communications, etc.).

If the recipient is located within the Russian Federation, then no further analysis of the package is performed and it is passed unchanged to section D of module 6. If the recipient is located outside the Russian Federation, then the package is further processed by module 3.

In section B, module 3 collects and normalizes the information (data) intended for recipients outside the country. It is here that the work of an authorized employee of the organization (state body) is supposed to take place.

The data normalization consists of software and mathematical transformations (including, but not limited to: TLS/SSL, HTTPS, HTTPX, E1/T1, ATM and others) of any data representations into text form.

[14] Coordination center for domain names.RU/.РФ. https://clck.ru/3EmLBZ

In section B, module 4 analyzes the normalized data for compliance with the attributive and substantive features of the personal data that fall under the definition.

To do this, the organization must define a list of processed personal data at the level of a local act or instruction and develop appropriate templates (for example, regular expressions), according to which the procedure for detecting target information is carried out. We point out that, depending on the specific tasks of the personal data operator, module 4 may be located before module 3, i.e., precede human analysis.

If the analyzed traffic contains matches with patterns of information that is unacceptable for transmission, then a control action (element 8) is sent to the section D of module 6 about the destruction (discarding) of a specific packet and logging of this event. In the considered model, such command can be submitted by an authorized employee; however, the fully automated operation of the proposed software module is not excluded.

In section D, module 6 is a corporate firewall, which, in addition to its main functions, decides on destroying (discarding) a specific package and logging an information protection event when a control action (command) comes from section B.

Elements 5 and 7 are standard information flows within the local network and the module for automated processing of outgoing data flows.

Similar algorithms were also proposed by foreign research teams (Liu et al., 2024; Pascual et al., 2024; Guaman et al., 2021; Yan et al., 2023). Therefore, we consider it useful to establish international cooperation in this area in order to most effectively achieve the goals of protecting sensitive information.

We have to make a reservation that the monitoring and analysis we have considered are only parts of a more detailed algorithm, which includes related organizational measures (creation of local acts in the field of information security, cooperation with regulatory authorities, implementation of general and private prevention, etc.). However, this study does not claim to be complete and exhaustive, and therefore we consider it sufficient to highlight only those stages of management within which specialized technical means can be involved, as it was initially stated.

Conclusions

Summarizing the above, we would like to emphasize the following.

1. Relations in the sphere of cross-border transfer of personal data could develop only in the digital age, when global information flows beyond the borders of any state became commonplace, and therefore the legal and political regulation of this area is just being formed.

2. Personal data are a valuable resource: they contain information about personal life that a person wants to keep secret; they are necessary for business development; they are required for effective fight against crimes and offenses; they are an important component

of criminal and other illegal activities; they can be a factor in interstate and inter-political struggle.

3. Illegal cross-border flows of personal data pose a serious threat to individual rights, national security and financial well-being of organizations; however, current national and international legal norms do not provide a mechanism sufficient to prevent them.

4. To resolve this problem, it is necessary to introduce a special prosition for violating the established procedure for the cross-border transfer of personal data to the Administrative Code of the Russian Federation; to supplement the qualifying signs in the Articles of the Criminal Code of the Russian Federation devoted to the violation of the security of computer information; to oblige the operator of personal data to inform their subject of their intention to carry out cross-border transfer of such information.

5. Simultaneously with the legislation optimization, it is necessary to introduce specialized technical means for detecting unauthorized cross-border flows of personal data into the information security systems of organizations and government agencies acting as personal data operators.

6. The use of these tools should be carried out according to the following algorithm: constant automated background control of all outgoing information flows, determination of their direction; identification of flows moving abroad; attribution of information in this flow to personal data; blocking of the flow corresponding to the two above-specified signs; notification of an authorized employee of the organization (state body) about the identified flow; human assessment of the permissibility of cross-border data transmission; decision-making on skipping or final blocking of the stream; in the latter case, informing about an identified and prevented information security incident.

We believe that the implementation of the described algorithm, as well as the improvement of legal regulation in the field of cross-border transfer of personal data, will reduce the number of thefts and unintentional leaks of such sensitive information. This will help to protect the rights of citizens, ensure the political stability of the Russian Federation, reduce the number of crimes using other people's personal data, and achieve financial well-being for commercial organizations.

References

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Abramova, A. G. (2020). Contemporary issues of personal data protection in the network: fundamental principles of personal data protection. *Region i mir*, *11*(4), 21–25. (In Russ.).

Akulin, I. M., Chesnokova, E. A., Guryanova, N. E., Presnyakov, R. A., & Letova, A. D. (2020). Possibility of transboundary transfer of health-personal data within the EAEU: reality, prospects. *Menedzher Zdravookhranenia*, *7*, 65–73. (In Russ.). https://doi.org/10.37690/1811-0185-2020-7-65-73

Artemova, A. N. (2023). Legal regulation of cross-border personal data transfer. *Yuridicheskaya nauka i praktika*, *19*(3), 9–16. (In Russ.). https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Balashkina, I. V. (2007). Features of the constitutional regulation of the right to privacy in the Russian Federation. *Pravo i politika*, *7*, 92–105. (In Russ.).

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ivanova, O. V., Ivanov, P. V., & Smelov, M. N. (2010). Problems and algorithms of information retrieval in global computer networks. *T-Comm*, *4*(3), 23–2. (In Russ.).

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Smolenskij, M. B., & Levshin, N. S. (2016). Localization of personal data of Russian citizens as a component of Russia's economic and national security. *Nauka i obrazovanie: khozyajstvo i ekonomika, predprinimatelstvo, pravo i upravlenie*, *2*(69), 111–114. (In Russ.).

Veseliczky, O. I. (2015). Issues of cross-border transfer of personal data in accordance with the requirements of 242-FZ. *Collections of conferences of the Sotsiosfera SIC*, *53*, 275–279. (In Russ.).

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Authors information

Dmitriy V. Bakhteev – Dr. Sci. (Law), Professor, Department of Criminalistic named after I. F. Gerasimov, Head of Laboratory of Digital Technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Anna M. Sosnovikova – probation researcher of the Laboratory for digital technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Evgeniy V. Kazenas – student, Ural Federal University named after the first President of Russia B. N. Yeltsin
Address: 19 Mira Str., 620002, Yekaterinburg, Russia
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research was funded by Russian Science Foundation, grant No. 23-78-10011, https://rscf.ru/project/23-78-10011/

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 28, 2024
Date of approval – July 12, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Преодоление нелегальной трансграничной передачи персональных данных

Дмитрий Валерьевич Бахтеев ✉
Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Анна Михайловна Сосновикова
Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Евгений Владимирович Казенас
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

Ключевые слова

законодательство,
информационная безопасность,
информация,
инцидент,
компьютерная сеть,
персональные данные,
право,
связь,
трансграничная передача данных,
цифровые технологии

Аннотация

Цель: формирование комплексной междисциплинарной юридико-технологической модели управления рисками в сфере незаконной трансграничной передачи персональных данных посредством ликвидации законодательных лакун и создания системы автоматизированного контроля исходящих потоков информации, а также экспертного реагирования на выявленные инциденты.

Методы: в работе, помимо всеобщего диалектического и общенаучных, используются специально-юридические и кибернетические методы. Так, на основе сравнительно-правового анализа выявляются различия между национальным и международным регулированием трансграничных потоков персональных данных, а метод моделирования, положенный в основу второго раздела исследования, позволяет сформировать алгоритм выявления инцидентов информационной безопасности в сфере трансграничной передачи персональных данных и реагирования на них.

Результаты: сформулированы предложения по оптимизации законодательства в рассматриваемой сфере посредством введения специализированных охранительных норм за нарушение правил трансграничной передачи персональных данных, закрепления обязанности оператора уведомлять субъектов персональных данных о намерении осуществить передачу информации за рубеж. Во второй части работы описана концепция программного комплекса, предназначенного для детекции инцидентов информационной безопасности в рассматриваемой области, а также модель действия уполномоченного представителя оператора после получения сигнала от автоматизированной системы.

✉ Корреспондирующий автор

Научная новизна: для решения заявленной проблемы в работе объединяются знания и компетенции ученых-юристов и специалистов в сфере информационной безопасности, что позволяет предложить междисциплинарный подход. Одновременно с этим вопросы незаконной трансграничной передачи персональных данных на сегодняшний день не получили должного освещения в науке, поскольку российское законодательство в данной сфере изменилось не так давно. Авторы настоящей работы предлагают не столько усилить санкцию за нарушение законодательства в рассматриваемой сфере, сколько обеспечить наказание лиц, совершающих кибератаки, и вооружить операторов персональных данных действенным инструментом минимизации рисков утечки информации.

Практическая значимость: результаты исследования могут быть использованы для совершенствования законодательства в сфере трансграничной передачи персональных данных и организации деятельности уполномоченных сотрудников оператора персональных данных по управлению рисками в рассматриваемой сфере.

Для цитирования

Бахтеев, Д. В., Сосновикова, А. М., Казенас, Е. В. (2024). Преодоление нелегальной трансграничной передачи персональных данных. *Journal of Digital Technologies and Law*, *2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Список литературы

Абрамова, А. Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: Основополагающие принципы защиты персональных данных. *Регион и мир*, *11*(4), 21–25. https://www.elibrary.ru/eveayh

Акулин, И. М., Чеснокова, Е. А., Гурьянова, Н. Е., Пресняков, Р. А., Летова А. Д. (2020). Возможность трансграничной передачи связанных со здоровьем персональных данных в рамках ЕАЭС: реальность, перспективы. *Менеджер здравоохранения*, *7*, 65–73. https://doi.org/10.37690/1811-0185-2020-7-65-73

Артемова, А. Н. (2023). Правовое регулирование трансграничной передачи персональных данных. *Юридическая наука и практика*, *19*, 3, 9–16. EDN: https://www.elibrary.ru/cgfugw. DOI: https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Балашкина, И. В. (2007). Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации. *Право и политика*, *7*, 92–105. https://www.elibrary.ru/hzyhnn

Веселицкий, О. И. (2015). Вопросы трансграничной передачи персональных данных в соответствии с требованиями 242-ФЗ. *Сборники конференций НИЦ Социосфера*, *53*, 275–279. https://www.elibrary.ru/vbvgev

Иванова, О. В., Иванов, П. В., Смелов, М. Н. (2010). Проблемы и алгоритмы поиска информации в глобальных компьютерных сетях. *T-Comm: Телекоммуникации и транспорт*, *4*(3), 23–25. https://www.elibrary.ru/ophpnz

Смоленский, М. Б., Левшин, Н. С. (2016). Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России. *Наука и образование: хозяйство и экономика, предпринимательство, право и управление*, *2*(69), 111–114. https://elibrary.ru/item.asp?id=25423352

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Сведения об авторах

Бахтеев Дмитрий Валерьевич – доктор юридических наук, доцент, профессор кафедры криминалистики имени И. Ф. Герасимова, заведующий лабораторией цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия Федерация, г. Екатеринбург, ул. Комсомольская, 21
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765

Сосновикова Анна Михайловна – стажер-исследователь лаборатории цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1196069

Казенас Евгений Владимирович – студент, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Адрес: 620002, Россия, г. Екатеринбург, ул. Мира, 19
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77 / Уголовное право
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 28 июня 2024 г.
Дата одобрения после рецензирования – 12 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.