Legal Regulation of Personal Data in the Digital Economy: Leading Problems and Prospects

Tatiana Efimtseva*
Orenburg Institute (Branch) of
The Kutafin Moscow State Law University (MSLA),
Komsomolskaya str. 50, 460000 Orenburg
Russian Federation
e-mail: tve-26@mail.ru

Stanislav Shadrin
The Orenburg State University
Pobedu av. 13, 460018 Orenburg
Russian Federation
e-mail: rusrock.ru@mail.ru

Abstract In the digital economy, information became the major leading commodity that is freely available on the market. However, this type of information, such as personal data, is an essential element of a person's private life, and therefore the state should ensure the protection of such information by means of legal norms.
In the situation when the foreign doctrine issues of legal protection of personal data are developed, the degree of study of this topic in the Russian Federation is very modest and limited. The purpose of this research is to analyze the world experience and apply it on the territory of the Russian Federation for further improvement of legislation. As a result, it is proved that the aspects of privacy in General and the protection of personal data should be taken into account when developing a regulatory framework aimed at regulating relations in the digital economy. At the same time, it is important to find a balance with regard to the processing of personal data and establish rules that allow not only the free provision and use of electronic communications services, but also respect the right to respect for privacy.

Keywords: *legal regulation, personal data, digital economy, leadership prospects*

1 Introduction

Modern technologies, especially in the field of information and telecommunications, are developing so rapidly that legal regulation often does not keep up with this development, and this creates many, both real and potential threats to fundamental human rights and freedoms, and, above all, the right to privacy is subject to violations. With the development of computer technologies and cyberspace (World Wide Web (WWW), social networks, online broadcasts, geo-data transmission, etc.), the most vulnerable part of this right is personal information – personal data. At the same time, the volume of data processed on a global scale is growing at an enormous pace. According to statistics, by 2020, the accumulated volume of data should increase to about 44 zetabytes or 44 trillion gigabytes (for comparison, in 2015 - only12 zetabytes) (see Statista 2020).

Personal data of individuals in States where information flows between them can be transferred without any barriers within international or regional organizations are particularly at risk. Such state associations include the European Union, which is a unique integration entity that has no analogues in the world. At the moment, the closest and freest economic integration in the world is being carried out within the EU, the formation of an economic and monetary Union is continuing, and the transition to the next stage of integration is underway (European Central Bank 2020). Within the framework of this Union, the single digital market of the EU is being formed, the creation of which is one of the priorities of European institutions over the past years. That is why the issue of legal use of personal data is important for economic entities operating in the EU member States, as well as for all partners of the Union around the world (European Commission 2019). However, it should be noted that integration not only creates new opportunities, but also generates new social problems (Kashkin 2019, p. 772).

The high level of economic development of the EU countries stimulates the emergence of problems of personal information security. As the American researcher in the field of information privacy Simson Garfinkel rightly notes: "*over the past 50 years, new types of threats to personal information have appeared, whose roots do not go to totalitarianism at all. These threats have grown on the basis of a free capitalist market, modern technologies and uncontrolled exchange of electronic information*" (Garfinkel 2000).

In the European Union, special legislation on the protection of personal data has been in place for more than twenty years, and in 2018, new legal acts entered into force that revolutionized the European legal regulation of personal data protection.

One of the challenges facing the new EU instruments was how to combine the right to protect information with the right to free access to information and to express opinions. On the other hand, given that the processors (controllers) of personal data are not only individuals and organizations, but also States, it is necessary to maintain a balance between public and private interests. At the same time, much depends on whether we are talking about a public person, close attention to which is a necessary element of a democratic society, or about a private person, the protection of whose personal data the state should approach with special care. This conflict has practically no universal ways of resolution (Talapina 2018, p. 141).

In the process of preparing new legal acts, it became obvious that new methods of data protection, such as profiling and pseudonymization, would need to be introduced, since modern globalization and the digital economy require the active development and improvement of information technologies, the blurring of the boundaries of data transmission, the use of new types of personal data (for example, biometric, genetic) and automated systems for their processing.

The Russian Federation, where a huge number of databases have been created and maintained, faces similar problems. At the same time, it should be taken into account that the Russian industry legislation on personal data protection has existed for a little more than ten years, during which it has not undergone significant changes, and by all indications is in the initial stage of its formation. Currently, issues related to cross-border transfer of information between the Russian Federation and the European Union, as well as within the framework of the Eurasian Economic Union (EEU), require solutions. Thus, one of the issues raised by Russia during its presidency of the organization in 2018 was the development of an agreement on personal data between member States. Personal data protection is one of the priority activities of the Eurasian economic Commission in accordance the digital agenda of the EAEU until 2025 (Eurasian Commission 2020). However, in order to successfully cooperate with the member States of the organization, it is important for Russia to have its own legislation that meets the modern realities of the digital economy, including effective data protection mechanisms and ensuring a high level of protection of the rights and freedoms of individuals and, in particular, the right to protect personal data. In this regard, the need to formulate and develop these problems determines the relevance of this study.

Despite the existence of General theoretical and special works in the field of protection and protection of personal data, this topic is currently not sufficiently developed, a number of issues remain debatable, and some of them are left without attention, while their solution largely depends on the further development of legal regulation of privacy-one of the fundamental human needs in the development of the digital economy.

The purpose of the research is to form a holistic scientific understanding of the mechanism of legal regulation of personal data protection in the European Union, to set current problems and develop reasonable proposals for their solution, to identify prospects for the development of EU law in the relevant sphere of public relations in the digital economy, as well as to formulate recommendations for improving Russian legislation on personal data, taking into account the experience of the European Union.

Achieving these goals provides for the following tasks: to consider the system of sources of legal regulation of personal data protection in the European Union at the present stage; to assess the effectiveness of existing legal acts of the European Union in the field of legal regulation of personal data protection of individuals; to identify and disclose the content of the basic rights and obligations of individuals - subjects of personal data; to predict the prospects and main directions of development of legal regulation of personal data protection in the European Union in the digital economy; to conduct a comparative analysis of legal acts on personal data protection of the European Union and the Russian Federation and to formulate proposals for improving Russian legislation on personal data.

2. Problem relevance

Despite the importance and relevance of the problem of legal protection and protection of personal data of individuals is one of the little-studied areas, both in European and Russian legal science. The only work devoted to a comprehensive study of the problems of personal data protection in the EU is a dissertation defended in Kazan on the topic "The system of legal protection of personal data in the European Union".

Some works of Russian authors concern the EU information law in general while only touching on the protection of personal data. Such works include the works of Postnikova (2018). Many other researchers write about the legal regulation of personal data protection in individual EU States. Other researchers conduct a comparative analysis of the legal regulation of personal data protection in Russia and in the individual EU Member States.

Most Russian scientists in their work consider the protection of personal data exclusively in the Russian Federation. Some works concern only selective aspects of legal regulation of personal data protection - issues of data transfer between States, protection of personal data of an employee, technical aspects of personal data protection, use of personal data on the Internet, etc. In addition, certain issues of legal regulation of personal

information protection are considered in the works on the law of the European Union of many domestic Russian scientists.

In foreign scientific literature, including European literature, the legal protection of personal data has been also considered by many scientists. However, the works of these authors have not been studied in relation to the problems of improving the legal regulation of personal data protection in the Russian Federation. This study analyzes the most important international agreements and the latest EU legal acts on data protection.

3. Materials and methods

When writing this article, General scientific and special legal methods of knowledge were used: the method of system-structural analysis of the studied phenomena; the method of comparative law in the analysis of norms of domestic and European sources in the field of protection and protection of personal data of individuals; the method of interpretation of law; formal-logical and some other methods. The use of these methods in the complex allowed to solve the problems set for the researchers.

The European Union has established and operates a comprehensive system of legal regulation of personal data protection. The main element of this system is Regulation (EC) 2016/679 European Parliament and of the Union "On the protection of individuals regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General rules on the protection of personal data)" [8] (hereinafter – Regulation (EC) or Regulation (EC) 2016/679), which promotes the development of innovative digital services, and acts as a cornerstone in the implementation of the European strategy digital Single market, aimed at promoting free access of businesses to the online market in conditions of fair competition and a high level of protection of consumers and their personal data.

In turn, legal acts such as Directive (EU) 2016/680, Regulation (EU) 2018/1725, Directive (EU) 2002/58/EU Supplement Regulation (EU) 2016/679, extending the legal regulation of personal data protection to many areas of public life in the Union. At the same time, it is important to note that EU member States are obliged to harmonize their national legislation with these EU acts.

EU legal acts confer on individuals, as participants in legal relations arising from the protection of personal data, the rights and obligations that constitute the essence of the legal regulation of personal data protection in the EU. Rights and obligations are based on the concept of legal, transparent and controlled data processing, reflected in special principles and meeting the legitimate interests of individuals who provide their personal data.

An analysis of the provisions of the Regulation (EU) allows us to deduce the definition of a personal data subject, which means a person who is either identified, or is currently identified, or can be identified in the future, directly or indirectly, on the basis of personal data relating to it, in particular by reference to a specific identifier, such as a name, identification number, location data, online identifier, one or more other factors unique to the physical, physiological, genetic, mental, economic, cultural or social identity of this individual.

Regulation (EC) 2016/679 is a special act aimed at protecting the fundamental rights and freedoms of every individual located in the territory of the Union, including the right to protect their personal data. In comparison with earlier EU regulations, in particular, Directive 95/46 / EC on the protection of individuals in the processing and free circulation of personal data (see EU 1995) (hereinafter-Directive (EU) 1995), it significantly expanded the set of subjective rights of individuals, and their regulation is fully devoted to Chapter 3. The regulation (EU) provides for rights such as the right to delete data (the right to forget), the right to access information, the right to correct, the right to restrict data processing, the right to portability of data, the right to object. However, it should be noted that some of these rights (for example, the right to delete data) are novelties not only at the European level, but also on a global scale.

The set of rights that constitute the fundamental right of an individual to protect personal data has been developed taking into account the current risks to personal information, including on the Internet. All rights are directed to the person's comprehensive control over the processing of their personal data and allow them to participate in operations for the processing of their data. The implementation of rights is facilitated by the emerging jurisprudence of the EU Court of justice. Thus, the right to delete data was originally formulated by the EU Court in its decision on the widely known "Costeja case". In 2010, Spanish citizen Mario Costeja Gonzalez filed a complaint with the Agencia Española de Protecciónde Datos (AEPD - Spanish national data protection Agency) demanding that the newspaper La Vanguardia removed or changed the information published in 1998 about the inclusion of his property in the auction lists in connection with the court proceedings for the recovery of social security debts, payments for which he was overdue. Costeja Gonzalez discovered this information after years of searching for personal data in the Google search engine. It also required that Google Spain (or "Google Inc.") deleted or hid this information and did not display it in search results. As an argument, he argued that the foreclosure proceedings had been completely discontinued several years ago, and the references to this information "are completely irrelevant at the moment." Costeja Gonzalez's complaint against La Vanguardia was rejected, but the AEPD said it had the authority to order Google to remove data from its search indexes and block access to the

data. When the AEPD decision was appealed by Google to the Audiencia Nacional (national High Court of Spain), this judicial body requested a preliminary decision from the EU Court on this issue in accordance with European legal acts. The EU court ruled in favor of the Spanish national Agency for data protection and, accordingly, ordered Google to satisfy the request of Costeja Gonzalez. In its decision, the EU Court ruled that the controllers (in the case of Google, the search engine operator) must remove from the search results links to personal information about an individual at his request, if such information is "illegal, irrelevant, more irrelevant or excessive in relation to the purposes of data processing performed by the search engine operator" (Court of Justice of the European Union 2014).

The subject of personal data is endowed with numerous rights that he can exercise in order to exercise its fundamental right to protect personal data. However, the exercise of their rights should not adversely affect the rights and freedoms of other persons. In this regard, it is necessary to name the duties assigned to the subjects of personal data. They are not directly regulated in the EU legal acts, but follow from the meaning of the provisions of the Regulation (EU) and other acts. First of all, it means that an individual is obliged to comply with the regulations of the Union and the EU member States concerning the protection of personal data. It is the responsibility of individuals to provide only such information as can be used to identify the individual, and such information must be reliable. If these conditions are not met, the processing of data will not fall within the scope of the regulation (EU) and, consequently, the person will not be able to exercise their right to protect personal data. In certain cases, an individual must submit to a decision based solely on automated processing, including profiling.

In addition, the person is obliged to provide additional information for the processing of personal data, when this is provided by the Regulation (EU). In particular, the controller may request the provision of additional information necessary to confirm the identity of the data subject (article 12), as well as the consent of the legal representative, if it is a question of processing the data of the child (article 8). In some cases, in order to exercise their rights, an individual is required to make arguments that the information to be deleted or the processing of which is restricted is illegal, irrelevant, irrelevant or excessive in relation to the purposes of data processing performed by the controller.

Legal regulation of personal data protection on the territory of the EU is implemented through the activities of the competent authorities for the protection of personal data of the European Union and the EU member States. At the same time, their interaction with each other at the level of the Union was previously practically not regulated. Through the adoption of Regulation (EU) 2016/679 and Directive (EU) 2016/680, a large-scale reform of the activities of the authorized bodies was carried out. The aim of this reform was to create a structured and effective system of authorities capable of fully protecting the rights and freedoms of individuals with regard to the processing of their personal data, both at the level of the EU member States and the Union as a whole. The Central part of this system is the European Council for data protection, which has a supervisory, executive, advisory, coordination and interaction function. In turn, the European Commissioner for data protection has information, advisory, organizational, security and control functions, while the National Supervisory Authorities have information, security, executive, control functions and coordination and interaction functions. For the effective implementation of its functions, each body is endowed with authority.

The European Union has an institutional mechanism for the protection of personal data of individuals, based on binding decisions of authorities, both general and special competence. Measures of legal responsibility are aimed at preventing and minimizing the consequences of violations, as well as at punishing violators, which is expressed in the obligation of the guilty person to undergo the adverse consequences provided for by the sanction of the legal norm for the committed offense. These measures may be of a disciplinary, administrative or other nature. The Regulation (EU) does not prohibit EU member States from including criminal liability measures in their legislation.

In particular, for violations related to the processing of personal data, the controller or processor may be subject to liability measures by the competent Supervisory authority of the EU member state in whose jurisdiction it is located. The European data protection Commissioner may impose liability measures on controllers who are bodies of the Union. Authorized bodies for the protection of personal data have the right to take such measures, both independently and at the request of an individual or his representatives. In addition, the authorized bodies of the EU and EU member States themselves may be held liable for failure to perform their duties. Claims against authorized EU authorities are sent to the EU court of Justice, and against national Supervisory authorities - to the competent court of the relevant EU member state. However, EU legislation does not provide for any liability for personal data subjects.

The right to personal data protection in the European Union is a dynamic social phenomenon. With the advent of new technologies and awareness of new security challenges and to improve economic performance, the current rules are periodically reviewed. Thus, the right to protect personal data is always in development, which is facilitated by the activities of the authorized data protection bodies and institutions of the EU and, mainly, the European Commission. In addition, this process is influenced by the Supervisory authorities and other public authorities of the EU member States, both directly and through participation in the activities of the European Council for data protection.

Theoretically, EU citizens can also influence the development of the right to protect personal data by using the right of legislative initiative, since the Lisbon Treaty of 2007 gave citizens of the Union the right to request the Commission to draft new EU legal acts. This right is called "civil initiative" and is recognized as one of the democratic principles of the EU (Section II "Provisions on democratic principles" of the Treaty on European Union (DES) (European Union1992). However, until now, no civil initiative to adopt specific acts on the protection of personal data has come directly from EU citizens. Only civil rights associations, such as the non - governmental organization European digital rights (EDRi), participate in the dialogue with EU institutions (EDRI 2012).

The most active development of legal regulation of data protection is expected in the field of electronic communications. An important and necessary step is the development and adoption of new Regulations of the European Parliament and the Council on respect for privacy and protection of personal data in electronic communications and the repeal of Directive 2002/58/EC (privacy and electronic communications Regulation or "ePrivacy" Regulation) (European Parliament 2002) and the Directive establishing the European electronic communications code ("EECC Directive") (European Commission 2016). The drafts of both documents, which are complementary to each other, are currently being discussed in the EU institutions.

Based on the analysis of the draft "ePrivacy" Regulations, we can draw several conclusions. Thus, the Regulation will establish rules concerning the protection of the fundamental rights and freedoms of individuals and legal entities in the provision and use of electronic communications services, and, in particular, the right to respect for the privacy and protection of individuals in relation to the processing of personal data. This document will also ensure the free and secure circulation of electronic communication data and electronic communication services within the Union, which should not be restricted or prohibited for reasons related to respect for the privacy and communication of individuals and legal entities and the protection of individuals in relation to the processing of personal data. It is planned that the "ePrivacy" Regulation will not apply to:

- activities that go beyond the law of the Union;
- activities of member States falling within the scope of Chapter 2 of Section V of the Treaty on European Union;
- electronic communication services that are not publicly available;
- the activities of the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offences or the execution of criminal penalties, including the protection and prevention of threats to public safety.

The "ePrivacy" Regulation should not restrict the application of Directive 2000/31/EC on certain legal aspects of information society services, including e-Commerce on the domestic market (the "e-Commerce Directive") (European Parliament 2000), which establishes rules on the liability of service providers and intermediaries. The "ePrivacy" Regulation does not repeal the provisions of Directive 2014/53/EC on the harmonization of the laws of EU member States relating to the provision of access to the radio equipment market. Finally, the "ePrivacy" Regulation will not apply to data processing activities by Union bodies and institutions, since the principles and obligations that such bodies should follow when processing data by electronic means of communication have been included in Regulation (EU) 2018/1725.

According to the draft "ePrivacy" Regulation, EU member States will be able to maintain or create national data storage systems, if such structures comply with the law of the Union. In this regard, EU member States need to take into account the case law of the EU Court of justice regarding the interpretation of Directive 2002/58/EC and the Charter of fundamental rights of the EU and, in particular, the case "Digital Rights Ireland and Seitlinger and Others" and the case "Tele2 Sverige AB and Secretary of State for the Home Department" (Home Department 2016).

The same data protection authorities that are responsible under the General data protection Regulation (Regulation (EU) 2016/679) will be responsible for compliance with the privacy rules that will be provided for in the "ePrivacy" Regulation.

It is important to note that the scope of the "ePrivacy" Regulation will be closely related to the scope of legal acts regulating other issues of EU information law. This document will be part of the regulatory framework for the regulation of electronic communications. In particular, the draft "ePrivacy" Regulation will be based on the definitions given in the draft Directive establishing the European code of electronic communications ("EECC Directive"), including the definition of "electronic communication services". Thus, it is planned that these two legal acts will complement each other, since the "EECC Directive" will have to provide additional security for electronic communications services, through which personal data will be transferred.

4. Legal regulation and personal data protection in the digital economy

Currently, Russia has created a regulatory framework designed to ensure the effective implementation of individuals ' right to protect their personal data. The main element is the Federal law of 27 July 2006 N 152-FL

"On personal data" (Federal Law 2006a) (hereinafter - the Federal law "On personal data"), whose adoption is due to increasing influence on the Russian legal system of international and European law, including the agreements and conventions developed by the Council of Europe and the world trade organization (WTO).

In order to assess the extent of such influence, it is necessary to conduct a comparative analysis of Russian and European legislation regulating public relations in the field of personal data protection of individuals.

First, it is obvious that Directive 95/46/EC, which was in force in the European Union at the time of its adoption, had a great influence on the content of the Russian Federal law "On personal data". As an example, we can cite several provisions of the Russian Law that are similar in content to the norms enshrined in the Directive. Thus, article 22 of the Federal law "On personal data" obliges the operator to notify the authorized body for the protection of the rights of data subjects of its intention to process personal data before the start of processing. The obligation to notify the authorized body of the start of data processing was initially only enshrined in European Directive 95/46/EC. Further, part 2 of article 22 of the Federal law "On personal data" defines a number of cases where the legislator allows processing without prior notice to the authorized body for the protection of the rights of data subjects. This rule is similar to the provision set out in Directive 95/46/EC (article 18).

Secondly, the Federal law "on personal data" regulates the processing of data in several areas of public life, while in the EU there are various legal acts. This division of areas seems justified, since it is quite difficult to provide for all data processing requirements in one document, both by individuals and by state and municipal authorities. The specifics of personal data processing in state or municipal personal data information systems are contained in article 13 and other provisions of the Russian law.

The Federal law "On personal data" also contains rules that in European law fall within the scope of the special "police" Directive (EU) 2016/680. In accordance with article 6 of the Federal law "On personal data", processing of personal data is allowed, including in the following cases: in connection with the participation of a person in constitutional, civil, administrative, criminal proceedings, proceedings in arbitration courts; for the execution of a judicial act, an act of another body or official, subject to execution in accordance with the legislation of the Russian Federation on enforcement proceedings, etc. It should be noted that these rules are related to paragraph 1 of article 1 and other provisions of the Directive.

Third, the relatively small terminological base of Russian legislation in the field of personal data protection is noteworthy. The list of definitions used in EU law is much broader and includes 26 basic concepts. At the same time, the concepts given in article 3 of the Federal law "On personal data" (namely: "personal data", "operator", "processing of personal data", "blocking of personal data", "depersonalization of personal data", "information system", "cross-border transfer of personal data") are related to similar concepts enshrined in Regulation (EU) 2016/679.

However, the Federal law "On personal data" operates with such concepts that are not used in European acts, such as "automated data processing", "distribution of personal data", "provision of personal data", "destruction of personal data". The concept of "biometric personal data" in the Russian law is included in a separate article 11, which regulates in detail the circumstances under which the processing of such data can be carried out without the consent of the subject of personal data.

We believe that given the current level of development of information systems, as well as the emergence in recent years of technical capabilities for the implementation of numerous operations for processing information, some of the concepts used in the Regulation (EU) can be adapted for the purposes of legal regulation of data protection in the Russian Federation.

Fourth, the regulation of the legal status of personal data subjects, which includes their inalienable rights and obligations, is important from the point of view of effective legal regulation of the protection of personal data of such persons. The rights of the subject of personal data is entirely devoted to Chapter 3 of the Federal law "On personal data". After analyzing the legal status of personal data subjects in the Russian Federation and the EU, we have to acknowledge that the Russian legislation is much inferior to European acts in terms of volume and content of fundamental rights of the data subject in Chapter 3 of Regulation (EC) 2016/679. For example, the Russian legislation does not provide for the right to portability of data, does not regulate in detail the right to notification of correction, the right to delete data and the right to restrict the processing of personal data.

In accordance with Federal law N 264-FL of July 13, 2015, from January 1, 2016 in the Russian Federation, everyone has the right to be forgotten by the search engine, which in content is the same as the right to be forgotten (or the right to delete data) introduced in the EU. This Federal law introduces into the Federal law "On information, information technologies and information protection" of July 27, 2006 N 149-FL (Federal Law 2006b) (hereinafter - the Federal law "On information") article 10.3, according to which the operator of a search engine on the Internet at the request of an individual is obliged to stop issuing information about the index of the site page (link) on the Internet, allowing access to information about the applicant. Analysis of article 10.3 of the Federal law "On information" makes it possible to determine that it is the personal data of an individual.

At the same time, despite the fact that Russia has a special law regulating the processing of personal data, these amendments were made to the Federal law "On information". For unknown reasons, the Russian legislator decided not to link the right to be forgotten with personal data. This situation, in our opinion, complicates the

uniform interpretation of the legislation of the Russian Federation in relation to situations related to the deletion of personal data of users on the Internet. In addition, the Federal law "On information" does not establish objective criteria for dividing information into relevant and irrelevant. On the contrary, it emphasizes the subjective nature of such a qualification, referring to the loss of value for the applicant. Moreover, the Federal law "On information" does not oblige the user to prove this irrelevance, that is, the degree of "relevance and significance for the applicant" should be determined by the search engine operator. How he will be able to explain to the citizen the significance of the information about himself remains unclear. In addition, in a similar situation, another law - the Federal law "On personal data" - in article 14 obliges a citizen to prove the irrelevance of his data in order to delete them by the operator.

Fifth, the Federal law "On personal data" gives broad powers to law enforcement agencies in terms of the collection and subsequent processing of personal data. For example, processing of special categories of personal data received in cases established by the legislation of the Russian Federation is allowed in connection with the implementation of prosecutorial supervision by the Prosecutor's office.

In addition, in accordance with article 19 of the Federal law "On personal data", draft regulations and draft decisions adopted by associations and organizations of operators are subject to approval by the Federal service for technical and export control (FSTEC of Russia) and the Federal security service (FSB of Russia). Control and supervision over the implementation of organizational and technical measures to ensure the security of personal data during their processing in the state information systems of personal data are carried out by the FSTEC of Russia and the FSB of Russia within their powers.

The rules of the Federal law "On personal data" give broad powers to collect personal information without the consent of the subject of state security agencies. Given that the regulations do not provide for the responsibility of such bodies, such a General formulation, in our opinion, may lead to abuse of authority by the relevant state bodies and their officials (in personal interests, with violations of the established terms and methods of processing and storage, etc.). Such situations have already been repeatedly considered by the European Court of human rights. As an example, we can cite the case "Roman Zakharov v. Russia", related to the access of the security services to the data on the user's telephone conversations and the uncontrolled use of the received personal data (European Court of Human Rights 2015).

Sixth, national Supervisory authorities for the processing of personal data in the Russian Federation and the EU have different legal status. The provisions of Regulation (EC) 2016/679 state that each Supervisory authority of an EU member State must act independently in the performance of its tasks and in the exercise of its powers in accordance with EU legal acts.

In the Russian Federation, the Federal service for supervision in the field of communications, information technology and mass communications (Roskomnadzor) is the competent authority for the protection of the rights of data subjects, which is charged with ensuring control and supervision over the compliance of personal data processing with the requirements of the law (Government of the Russian Federation 2009). Roskomnadzor is a Federal division (service) of the Ministry of communications of Russia - a Federal executive authority under the Government of the Russian Federation, and therefore it is impossible to talk about the independent status of this service. Analysis of the Federal law "On personal data" confirms this thesis, since its provisions do not say anything about the fact that the competent authority of the Russian Federation has an independent status.

Thence, despite a certain influence on the legislation of the Russian Federation on personal data the European legal acts, however, significant differences in the approaches of EU and RF legal regulation of protection of personal data of individuals. The legislation of the Russian Federation on personal data is not developing as dynamically as required by the realities of the time. Thus, comparing the provisions of Russian legislation and EU legal acts on cross-border transfer of personal data, it can be noted that the domestic legislation does not regulate the transfer of personal data to international organizations, both governmental and non-governmental.

The analysis of the current state of legal regulation of personal data protection in the Russian Federation, taking into account the level of development of information technologies, allows us to state that it needs serious improvement. The most effective step, in our opinion, will be the adoption of special regulations that regulate a specific area of legal regulation of data protection. First of all, we are talking about the processing of personal data by law enforcement agencies in order to prevent, investigate, detect criminal offenses and threats to public safety, as well as the execution of penalties. In addition, it is necessary to adopt a regulatory act regulating the processing of personal data by electronic means of communication, including the transfer of data via the Internet. Of course, the development of these documents can take quite a long time. However, in any case, the legislator should consider this issue in order to ensure that in the future Russia has an effective legislative framework that is not inferior to foreign ones.

The reform of the legal regulation of personal data protection in the Russian Federation will bring Russian legislation closer to high European standards, more effectively protect the basic rights and freedoms of citizens, including the fundamental right to protect personal data, to carry out mutually beneficial cooperation with the EU on data protection issues and to provide a mutually acceptable regime for data transfer that will meet the requirements of the legislation of the Russian Federation and legal acts of the European Union. The reform should

begin with amendments to the Federal law "On personal data", which will allow to proceed to the adoption of special Federal laws in the future.

5. Results

At the present stage of development of legal regulation of personal data protection in the EU in the digital economy, there is a review of existing legal acts, as well as the adoption of new documents is planned. Given that the EU is implementing The Digital Single Market strategy ("DSM Strategy"), which aims to increase confidence in digital services and their security, data protection reform and, in particular, the adoption of Regulation (EU) 2016/679 were key actions in this direction. Further development implies a high level of privacy protection for users of electronic communications services and equal conditions for all participants of the Single digital market.

In accordance with the requirements of the "best regulation" concept, the EU Commission has implemented the Regulatory Fitness and Performance Program ("REFIT evaluation") in relation to Directive 2002/58/EC. Its assessment shows that the goals and principles of the existing system remain sound. However, since the last revision of the Directive in 2009, there have been important technological and economic changes in the market. Consumers and businesses are increasingly relying on new Internet services that provide interpersonal communication, such as voice over IP, instant messaging, and Internet connectivity. These ultra-modern communications services (Over-the-Top communications services - "OTTs") are generally not subject to the legal acts regulating the field of electronic communications in the EU, including Directive2002/58/EC.

In this regard, a draft "ePrivacy" Regulation has been developed, which is currently under consideration. The format of the regulation is due to the fact that the regulation is a binding document in all EU member States, and thus its consistency with Regulation (EU) 2016/679 will be ensured. For example, the "ePrivacy" Regulation will specify Regulation (EU) 2016/679 with regard to data transmitted by electronic communication devices.

The analysis of the current state of legal regulation of personal data protection in the Russian Federation, taking into account the level of development of information technologies and the digital economy, allows us to state that it needs serious improvement. In this regard, it is necessary to amend the current legislation of the Russian Federation on the protection of personal data. This should be guided by the latest legal acts of the EU, and first of all the General data protection Regulations, which are the most progressive documents for the protection of personal data to date. This requires not direct copying of the norms of European acts, but their adaptation taking into account the Russian experience and traditions in this area, the current level of development of technical means to ensure the security of personal data in the Russian Federation.

In order to improve the effectiveness of measures to ensure the protection and protection of the rights and freedoms of individuals with regard to the processing of their personal data, it is proposed to make the following amendments to the Federal law of July 27, 2006 N 152-FL "On personal data":

- supplement article 3 of the Law with definitions of the following concepts: "subject of personal data", "violation of personal data", "processor", "threats to the security of personal data", "levels of protection of personal data", "biometric data";
- to allocate part of Chapter 3 article "the Right of the data subject to delete their personal data", article "the Right of personal data subject to the correction of personal data", article "the Right of the data subject for limiting the processing of personal data", article "the Right of personal data subject to object to processing of personal data" and article "the Right of personal data subject to data portability". In addition, it is necessary to transfer the provisions of article 10.3 of the Federal law "On information, information technologies and information protection" to a separate article "The right of the subject of personal data to oblivion", which is also allocated under Chapter 3 of the Federal law "On personal data". In the content of these articles, it is necessary to define the conditions under which the operator will be obliged to fulfill the requirement of the data subject, and provide an exhaustive list of cases of restriction of these rights;
- supplement article 9 with part 9, where it is necessary to establish that the processing of personal data of a minor will be considered legal if at the time of data collection he was at least 14 years old. If the person is under 14 years of age, such processing is legal only if and to the extent permitted by the special consent given by the person who is the legal representative of the child. To reduce the risks of collecting and processing personal data from minors, part 7 of article 14 of the Federal law "On personal data" must be applied;
- to establish at the federal level the position of the Commissioner for the protection of personal data in the Russian Federation, giving it an independent status. In this regard, it is necessary to introduce a separate Chapter in the Federal law "On personal data", the provisions of which will be fully devoted to the conditions for the creation and operation of an independent competent authority, and which will replace the current article 23. In this Chapter, it is necessary to regulate in detail the powers, functions, tasks of such a authority, the procedure for appointing its officials, etc. For the effective implementation of the

activities of the authority, it is necessary to provide special legal guarantees that will ensure the real independence and impartiality of its officials and employees.

Therefore, according to Giovanni Butarelli, who previously served as the European Commissioner for data protection, "the European Union currently enjoys a privileged position as a reference point for most of the world in the field of privacy and data protection. But for the EU to continue to be a leader in the digital age, it must act on its own fundamental principles of privacy and data protection and act quickly" (Buttarelli 2019). Of course, not all researchers agree with the privileged position of the EU in this area, but it should be noted that the European legislation at this stage is really ahead of many countries, including Russia. This is largely due to the reform of the legal regulation of personal data protection, which began with the adoption of the General data protection Regulation (Regulation (EU) 2016/679).

In conclusion, we would like to cite the words of Giovanni Butarelli, succinctly describing the goal that every democratic state should strive for: "*It is extremely important to make data protection simpler, more understandable and less bureaucratic, so that it lies at the heart of the digital world now and in the future*" (Buttarelli 2019).

6. Conclusions

Overall, there are interesting European legal practices and experience that can be implemented into the Russian practice. According to Postnikova (2018), the adoption of Regulation (EC) and Directives (EU) is a big step forward in respect of the right of individuals to protection of personal data which should positively affect the functioning of the EU internal market (see Postnikova 2018, p. 248].

Petrykina (2007) proposes to fix alternative sanctions in the Russian civil legislation for violations in the sphere of turnover and protection of personal data of citizens in the form of an apology and compensation for moral damage in agreement with the victim (Petrykina 2007, p. 165). The use of an apology as a form of sanction is interesting, but it is closely related to the inner conviction of the person.

In our opinion, it would be more rational to establish in the legislation the right of the subject to demand the termination of processing of personal data, their correction, blocking and deleting, especially in social networks, on sites, etc. It is dictated by conditions of functioning of the digital economy based on operations with personal data. The presence of personal data in a variety of information systems can put the subject to various risks and lead to unpredictable consequences. Therefore, the subject must make sure that his personal data will be used only for his benefit and not for harm.

References

Buttarelli G (2019) Strategy 2015-2019. https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf Accessed 26 March 2020.

Court of Justice of the European Union (2014) Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Case C-131/12, Court of Justice of the European Union (Grand Chamber). http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 Accessed 25 March 2020

EDRI (2012) Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available via: https://edri.org/files/1012EDRi_full_position.pdf Accessed 26 Feb 2020

EU (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11, pp. 31-50

EU (2016) Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ. L 119:9. 4th of May 2016, pp. 1-89

Eurasian Commission (2020) EAEU 2025 Digital Agenda: Prospects and Recommendations. http://www.eurasiancommission.org/ru/act/dmi/Pages/digital_agenda.aspx Accessed 25 Feb 2020

European Central Bank (2020) Official website of the European Central Bank.https://www.ecb.europa.eu/ecb/history/emu/html/index.en.html Accessed 25 March 2020

European Commission (2016) Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM/2016/0590 final-2016/0288 (COD)

European Commission (2019) Digital Single Market. https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market Accessed 25 March 2020

European Court of Human Rights (2015) Roman Zakharov v. Russia, Grand Chamber judgment. https://www.echr.coe.int/Documents/Press_Q_A_Roman_Zakharov_ENG.PDF Accessed on 26 March 2020

European Parliament (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8th of June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"). OJ L 178, 17.7.2000, pp. 1-16

European Parliament (2002) Document 52017PC0010: Proposal for a Regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, Regulation on Privacy and Electronic Communications. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 Accessed 26 Feb 2020

European Union (1992) Treaty on the European Union (Maastricht, February 7, 1992) (as amended by the Lisbon Treaty of 2007). The Treaty entered into force on 1 November 1993. Consolidated Version of the Treaty on European Union. Official Journal of the European Union, C 326/13

Federal Law (2006a) Federal law of 27.07.2006 N 152-FL (ed. of 31.12.2017) "On personal data", Collection of legislation of the Russian Federation, No. 31(1), Article 3451

Federal Law (2006b) Federal law No. 149-FZ of 27.07.2006 (ed. of 02.12.2019) "On information, information technologies and information protection" (with ed. and extra, Intro. in force from 13.12.2019). Collection of legislation of the Russian Federation, N 31(1), Article 3448.

Garfinkel SL, Database Nation; the Death of Privacy in the 21st Century, 1st edn. (O'Reilly and Associates, CA, 2000), 338 p.

Government of the Russian Federation (2009) The decree of the RF Government dated 16.03.2009 No. 228 (edited on 05.12.2019) "On the Federal service for supervision in the sphere of Telecom, information technologies and mass communications" (together with the Regulations on the Federal service for supervision in the sphere of Telecom, information technologies and mass communications). Collection of legislation of the Russian Federation, 2009. No. 12, Article 1431

Home Department (2016) Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970

Kashkin SYu, European Union Law, Volume 2: special part: textbook for bachelor students, 4th edn. (Moscow: Yurayt Publishing house, 2019), 1023 p.

Petrykina NI, Legal regulation of personal data turnover in Russia and EU countries: comparative legal research: thesis for the degree of candidate of legal sciences, 1st edn. (Moscow, Law Press, 2007), 173 p.

Postnikova EV (2018) Some aspects of legal regulation of personal data protection within the internal market of the European Union. Law: Journal of the Higher School of Economics 1:234-254

Statista (2020) Volume of data/information created worldwide from 2005 to 2025 (in zetabytes). https://www.statista.com/statistics/871513/worldwide-data-created Accessed 25 March 2020

Talapina EV (2018) Protection of personal data in the digital age: Russian law in the European context. Proceedings of The Institute of State and Law of the Russian Academy of Sciences 13(5):117-150