International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Digital Technologies of the European Union in Personal Data Protection

Elena Olegovna Tchinaryan, Maria Sergeyevna Lavrentieva, Evgeny Sergeevich Kuchenin, Alla Andreevna Neznamova

Abstract*: The purpose of the article is to consider issues related to the legal protection of personal data in the European Union (EU). Based on a systematic approach and the method of comparative law, it is determined that the legal mechanisms of the EU most extensively regulate their scope, create a rigid framework for European and foreign companies and world corporations, and introduce independent regulatory authorities. This system of personal data protection is the most progressive at the moment. It is revealed that in the 20th-century mankind has experienced a rapid breakthrough of its development when the vector of technology progress was a reoriented towards information infrastructure, huge in its scale and universal coverage. Digital technologies led to the third industrial revolution, and they have entered into everyday life, both professional and domestic. Finally, the authors came to the conclusion that personal data protection rules are increasingly expanding. The world community has already realized the need to protect personal information, prevent its uncontrolled use, and the need to take sufficient measures to ensure the protection of information about the private life of everyone. Issues of cross-border transfer of personal data have become particularly important, and the trend towards the implementation of regulations on the personal data protection of an extraterritorial nature can be clearly seen.

***Keywords*: personal data, cross-border data transfer, European Union law.**

I. INTRODUCTION

A huge number of new ideas and inventions in the line of information technology have raised new challenges for the post-industrial society, namely, the issues of special control over the direct activities that are carried out through such developments. Among the significant number of legal aspects that arise in the course of involving a person in an objectively functioning digital infrastructure, it is necessary to identify the most vulnerable issue, which is the human rights protection.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Elena Olegovna Tchinaryan*, Russian State Social University (RSSU), Moscow, Russian Federation
Maria Sergeyevna Lavrentieva, Russian State Social University (RSSU), Moscow, Russian Federation
Evgeny Sergeevich Kuchenin, Russian State Social University (RSSU), Moscow, Russian Federation
Alla Andreevna Neznamova, Russian State Social University (RSSU), Moscow, Russian Federation

This concerns the protection of the individual's right to privacy in interaction with information technology, as well as personal data protection.

Due to its unique technological structure, the Internet is a critical element of information and communication technologies, which acquires significant importance in the modern life of man, society and the state. Indeed, at present, the activities of state bodies and institutions, public and private sector companies, as well as individual entrepreneurs are somehow related to the use of personal data. Many technical devices and technological processes, such as the Internet of things (IoT), Internet voting, Internet training, etc. are associated with the use of personal data [1]. The use of personal data of individuals is necessary when applying for a job, opening a bank account, or obtaining a loan, buying tickets, etc. The Internet has radically changed the cross-border interaction of individuals, expanding their communication capabilities, and the scope of their digital presence, which objectified the diversification of regulation of a number of relations and, in particular, led to the fact that personal data (personal data/personal information) have become an independent subject of legal regulation. Issues of comparative analysis of personal data protection in European legislation and in the Russian Federation are considered in the work of A.P. Zhukov [2], S.V. Chernyaev [3], the problems of the impact of European legislation on Russian personal data operators are raised in the works of M.B. Kasenov [4] and A.A. Zavedenskaya [5]. Some aspects of the personal data regulation in Europe are addressed in the work of S. Gutwirth and P. Hert [6].

II. PROCEDURE FOR PAPER SUBMISSION

A. General description

The cross-border nature of the Internet objectively requires international legal cooperation of states, especially when dealing with issues of cross-border data exchange and access. Today, incomplete, fragmentary regulation of legal issues regarding personal data protection has an obvious negative effect, and this is primarily manifested in the field of ensuring the smooth cross-border exchange of information in the global world. Many states and regional associations have already developed an understanding of the need to revise most legal acts in the field of privacy protection and personal data exchange. However, the process of overcoming the conservative regulatory environment proved to be a very difficult task.

Thus, the development of ICT is far ahead of the ability of international law to regulate it. In the course of study, the authors used a systematic approach and the method of comparative law (Table 1). This contributes to the convergence and unification of legislation in the field of personal data regulation, as well as the possibility of developing proposals to improve the Russian system of legislation in the field of personal data protection. Appeal to the approaches of legal regulation of personal data in the European Union, of course, is now of great practical importance for many states, including the Russian Federation.

Table 1. Methods used to achieve the purpose of the study

Research method	Purpose of use	Obtained result
System approach	allows considering the system of personal data protection as a system-based concept	it is revealed that this system consists of a set of interconnected elements having certain internal links
Method of comparative law	the general development patterns of the institution of personal data protection are revealed	it is revealed that this system consists of a set of interconnected elements having certain internal links

B. Algorithm

The study of digital technologies of the European Union in the field of personal data was based on a branching algorithm.

During the study, the authors processed and analyzed the international legislation in correlation to the Russian legislation, as well as the authors' viewpoints.

In the course of the study, the authors identified the following stages that allowed conducting the study according to a certain scheme (Fig. 1):

1. Formulating the research topic.
2. Setting the research goal and objectives.
3. Studying the theoretical basis of the research.
4. Constructing the research hypothesis.
5. Choosing research methods.
6. Identifying gaps in legislation.
7. Processing and analyzing research results.
8. Formulating the research findings.

C. Flow chart

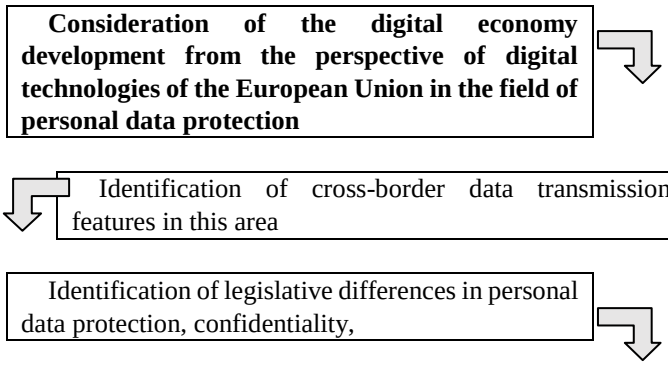

Fig. 1: Research flow-charts.

III. RESULTS

It is revealed that in the context of digital economy development legal regulation of the spheres associated with the privacy protection acquire special economic importance and commercial value. Today, the regulation of cross-border data transmission takes place at different levels. Most states have enshrined the right to privacy at the legislative level.

It is determined that the legislation of different states has significant differences in terms of its effectiveness, adequacy, consistency, dynamics, as well as trends in further development, which, certainly, is due to the difference in the choice of ways and methods of solving the multiplying number of issues related to the potential conflict between intensification of the use of such data and ensuring their protection, confidentiality, security, etc. The national approach to the regulation of the personal data sphere was implemented several decades ago, and, therefore, could not take into account the modern features of the global information system.

It is established that there are several prerequisites justifying the application of international law to transnational legal relations in the field of privacy protection. First of all, it is the lack of universal international legal protection of privacy, which entails a violation of basic human rights such as illegal storage of personal data, storage of inaccurate personal data, as well as unauthorized use or publication of such data. And the second – significant differences in national approaches to the regulation of the issue under study that creates serious obstacles to the free exchange of personal data between different states.

The study of approaches to the legal regulation of personal data in the European Union, of course, is now of great practical importance for many states, including the Russian Federation.

4. **Discussion**. The European Union law is an independent system, whose functioning is ensured by the integrity of its regulatory and institutional mechanisms. European law is a special legal system, whose norms regulate social relations emerging in the course of integration processes in the framework of the European communities and the European Union [7]. It is the totality of the national legal systems of European States, despite their very significant, sometimes fundamental differences, associated with the transfer of a number of sovereign powers by the members of the integration community to supranational institutions – the Council of the European Union, and the European Parliament [8].

Three main functional principles of EU law can be distinguished:

1. The principle of the rule of law of the European Union (EU), which means that in case of conflict between national law and the EU law, the latter will prevail.

2. The principle of the direct action of EU law. It is understood as the direct effect and mandatory applicability of EU law throughout its territory and with respect to all subjects of law of the EU.

3. The principle of integration of EU law, according to which the EU law is considered as integrated automatically into the national system of law of the EU member states. It also means that all EU rules of law are automatically incorporated into the national legal systems of the member states of this integration organization. The rules of EU law are subject to unconditional application by the national administration and the courts in the same manner and scope as the relevant rules of domestic law [9].

The EU legal system consists of sources of *primary law*, i.e. rules that have supreme legal force, *secondary law*, and *precedent law*. The sources of the primary law are primarily the Treaty on European Union [10] (the Maastricht Treaty), Treaty on the Functioning of the European Union [11], and the Charter of Fundamental Rights of the European Union [12](CFR). These sources enshrine the right of every individual to the protection of personal data relating to him, including the free movement, as well as cross-border movement. This right is defined by the specified acts as the basis one in the system of a person's rights and freedoms. The processing of an individual's personal data must be carried out in good faith, for the established purposes, and with the consent of the person concerned, or other lawful grounds provided by law, as well as the right to access the data collected in respect of him, and to seek to eliminate errors in these data. Both, the Treaty of Rome and the Maastricht Treaty, as well as the Charter of Fundamental Rights of the European Union, are based on the fact that compliance with the rules on personal data protection should be under the control of independent authorities [5]. The sources of secondary law are the regulations of the governing bodies of the EU. This is the EU Parliament or the EU Council, which adopt acts in the form of regulations, directives, decisions, recommendations, and conclusions. These are legally binding legislation however they differ in their legal force. The normative legal act adopted by the EU Parliament and the Council in the form of regulations is at the top of the hierarchy of sources. The regulation has binding force and is directly applicable in all EU member states, all EU bodies, and by physical persons. The *de jure* regulation does not imply the adoption of an implementing national act, excludes the effect of national legal acts in cases of conflict between national law and the regulation (priority effect of application). In addition, the regulations are directly applicable by the EC Court, whose decisions are case-law, as well as by national justice authorities. In terms of their legal force, case law sources occupy an intermediate position in the hierarchy of EU law. Precedent law always complements and builds upon provisions of the founding treaties (i.e. the norms of primary law), and cannot cancel them. As for the secondary law, its norms are not only supplemented but also abolished by decisions of the EU judicial bodies.

The Convention on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [4] [13] was the act that established the formal legal framework for the formation of a general legal regime of personal data in the EU and EU member states. It was adopted in 1995 by the EU Parliament and the Council. For more than twenty years of existence of this document, there have been many changes of technological and social nature, especially since the EU member states, observing the Directive as an act of nondirect action, adopted on its basis their own legislation, which led to differences in legislative regulation and law enforcement practice of the personal data use and protection in the EU member states. To strengthen control of personal data circulation and processing, the EU member states began to apply a new normative legal act since May 25, 2018, namely, EU Regulation 2016/679 "On protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repeal of Directive 95/46/EC (General provisions on data protection)", adopted on April 14, 2016.

The regulations are specifically focused on the private law sphere of personal data regulation. They do not regulate the use and protection of personal data for the purpose of preventing, investigating, or adjudicating criminal offenses, or the enforcement of criminal penalties, including the protection and prevention of threats to public security, and the free movement of such data. They also exclude from their scope the issues concerning interaction of law enforcement and judicial bodies in criminal cases and proceedings.

The concept of *personal data*, in comparison with the earlier noted document, underwent certain changes. In Regulation No 2016/679, they mean any information relating to a particular or identifiable natural person (data subject); defined person is the one, who can be identified, directly or indirectly, in particular, through an identification number or through one or more features, specific to his or her physical, psychological, mental, economic, cultural, or social identity" [14]. This approach is more detailed and allows talking about the established tradition of respect for privacy and personal information.

An important condition for the personal data processing is an unambiguous (explicit) consent of the person to such actions. The novelty of this right is the possibility of revoking this consent at any time. Naturally, the operator is responsible for ensuring the confidentiality and security of the information processed [15]. At the same time, in case of hacking or other violation of information confidentiality, the operator is obliged to declare this fact no later than 72 hours from the moment when the compromise of personal data became known. According to the Regulations No 2016/679, information about the rules of data processing must be provided to the data subject in an understandable and accessible way. Consent to the processing of personal information should not be an immediate procedure by just pressing the "Agree" button.

This confirmation should be an affirmative act expressed in writing or orally. In addition, the inaction of the user, for example, when performing certain actions on the site cannot be considered as consent. In this case, the user must be able to refuse to transfer data without prejudice to the commission of the action. The processing process itself should become transparent: the user should be able to track what is happening with his personal information, be able to delete it.

The company, which stores personal data, must ensure that they are adequately protected against leakage. The collection procedure should include depersonalization of information: the data should be associated with an alias rather with their owner. Moreover, the data must be encrypted and only authorized parties must have the key to the code. The transfer of data to third parties is prohibited, and the company is obliged to inform citizens about any leakage of information, including those in the case of hacker attacks. Companies that process personal data systematically and on a large scale must have an employee responsible for data security.

According to paragraphs 23-24 of the Regulation, its rules will also affect the activities of non-EU personal data operators in case if:

1. The processing of personal data is related to the offer of goods or services to the subjects of personal data located in the EU, regardless of whether such processing is related to the payment of these services or not. In this case, the following may evidence about the offer of goods or services:
   - offering goods or services of the language of one or more EU member states, providing the possibility to order these goods or services using this language;
   - giving the opportunity to pay currency, which is used in one or several EU member states;
   - mentioning in the offer of goods or services of consumers or users in the EU.
2. The processing of personal data is related to the monitoring of actions or behavior of personal data subjects in the EU if these actions are committed in the EU. The implementation of such actions may be evident by the fact that individuals carry out activities on the Internet, including the potential opportunity for consistent use of personal data processing technology, etc.

Thus, operators processing personal data of other states, including Russia, can fall under the rules of the new Regulations. Yet, the mechanism of accountability is not worked out. In the territory of the Russian Federation, personal data operators must follow the adopted law "On personal data" [8], while the requirements of Regulation No 2016/679 do not apply to them, since Russia is not an EU member state and a party to international treaties with the EU establishing the procedure and conditions for processing personal data by Russian operators. However, Russian companies operating in the EU, for example, when processing personal data in the provision of goods and services are required to take into account the requirements of Regulation No 2016/679. Noncompliance with Regulation No 2016/679 leads to administrative fines of up to €20 million or 4% of annual turnover. To date, the only global international treaty in the field of personal data protection that is legally binding is the Convention on protection of personal data at international level, which was amended on October 10, 2018, aimed at strengthening control over the circulation of personal data, the processing of special type of data, such as biometrics or genetic data, as well as the regulation of cross-border exchange and international cooperation. The document aims at ensuring respect for rights and fundamental freedoms of each individual in the territory of each country, in particular, the right to privacy, with respect to the automated processing of personal data. The Russian Federation has joined this document and the member states of the Council of Europe have agreed with the Russian proposal on cross-border transfer of personal data. The document should facilitate data transfer across national borders, while ensuring effective protection in their use in accordance with various national and international legal frameworks, including the new legislation of the EU, namely, Regulation No 2016/679 on the regulation of cross-border data flows. To this end, the legal framework for international cooperation in this field is to be expanded.

IV. CONCLUSION

Having considered the mechanisms of legal regulation of personal data protection at the present stage, it can be stated that the European system is the most progressive at the moment. The legal mechanisms of the EU most extensively regulate their scope, create a strict framework for European companies, and are mandatory in all 28 EU member states.

Legal mechanisms of the European legal system in the field of personal data protection impose obligations on foreign companies and global corporations to implement independent regulatory bodies to monitor the movement of personal data.

Today, the cross-border nature of the Internet objectively requires international legal cooperation of states, primarily in addressing issues of cross-border data exchange and access. The legal norms of the European community not only call for and encourage, but also oblige to develop international cooperation in the field of data protection in today's globalized world.

REFERENCES

1. L.B. Sitdikova, S.J. Starodumova, “Cloud technology services in information security”, *International Journal of Innovative Technology and Exploring Engineering*, vol. 8(1), 2019, pp. 3209-3211.
2. A.P. Zhukova, “K voprosu o novyh pravila obrabotki personal'nyh dannyh v Evrope Sravnitel'naya harakteristika Evropejskogo i rossijskogo zakonodatel'stva v sfere zashchity dannyh” [On the issue of new rules of personal data processing in Europe: Comparative characteristics of the European and Russian legislation in the field of data protection], *Fundamental and Applied Research of the Cooperative Sector of the Economy*, vol. 3, 2018, pp. 159-165.
3. S. V. Chernyaev, “Razvitie instituta zashchity personal'nyh dannyh v Evropejkoj soyuze i Rossijskoj Federacii” [Development of the institution of personal data protection in the European Union and the Russian Federation]. *Proceedings of the Orenburg Institute (branch) of the Moscow State Law Academy*, vol. 38, 2019, pp. 85-91.
4. M. B. Kasenova, “Nekotorye zamechaniya otnositel'no diversifikacii pravovogo regulirovaniya zashchity personal'nyh dannyh: podhod evropejskogo soyuza” [Some comments on the diversification of legal regulation of personal data protection: The approach of the European Union] [Text]. *Moscow, Legal Science*, vol. 2, 2018, pp.17-26.
5. A.A. Zavedenskaya, “Vliyanie GDPR na rossijskih operatorov personal'nyh dannyh” [Impact of GDPR on the Russian operators of personal data protection]. *Information Protection. Insider*,vol. 5(83), 2018, pp. 59-63.

6. S. Gutwirth, P. Hert, *Regulating profiling in democratic constitutional taste in profiling the European citizen: Cross-disciplinary perspectives*. Ed. by M. Hildebrandt . Dordrecht: Springer, 2008.
7. S.Yu. Kashkin, *Pravo Evropejskogo Soyuza* [European Union Law] [Text]. Textbook. Moscow, 2005.
8. L.M. Entin, *Evropejskoe pravo. Pravo Evropejskogo soyuza i pravovoe obespechenie zashchity prav cheloveka* [European law. European Union law and legal protection of human rights] [Text]. The college textbook, 2nd ed. revised and amended. Moscow, 2005.
9. A.Ya. Kapustina, Pravo Evropejskogo Soyuza: uchebnik dlya vuzov [European Union law] [Text]. A textbook for universities. Moscow: Yurayt Publishing House, 2017.
10. The Treaty on European Union. (Signed in Maastricht, 07.02.1992. Rev. and amended on 13.12.2007). Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:xy0026&from=EN
11. Treaty on the Functioning of the European Union, TFEU. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF
12. The Charter of Fundamental Rights of the European Union. European Convention, Strasbourg, December 12, 2007.
13. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Directive 95/46/EC of the European Parliament and the Council of October 24, 1995, (Adopted in Luxembourg on 24.10.1995. Rev. and amended on 29.09.2003). Official Journal of the European Union, L 281, 1995, p. 31.
14. The EU Regulation 2016/679 concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General provisions on data protection). *Official Journal of the European Union*, vol. 119, 2016, pp. 1-88.
15. S.J. Starodumova, M. A. Volkova, A.A. Neznamova, G.N. Kuleshov, R.R. Lenkovskaya, "The problems of responsibility for violation of legislation regulating information security on the Internet", *Revista Espacios*, vol. 39(45), 2018, p. 25.