REVISTA
SAN GREGORIO

http: 10.36097/rsan.v1i44.1581
Artículo Original

Legal Schemes For The Protection Of Personal Data In The Context Of Digitalization

Regimes Jurídicos Para A Proteção De Dados Pessoais No Contexto Da Digitalização

Authors

Yana V. Gaivoronskaya*[1], Olga I. Miroshnichenko[2], Daria A. Petrova[3], Iryna I. Bodrova[4]

[1] *Far Eastern Federal University Law School, PhD in Law, Associate Professor, Associate Professor, Associate Professor of the Department of theory and history of state and law,690950, Vladivostok, 8 Sukhanova St., Russian Federation, *Email: yanavl@yandex.ru , https://orcid.org/0000-0002-5491-2414*

[2] *Far Eastern Federal University, Law School, PhD in Law, Ll.M. In legal theory, Associate Professor of the Department of theory and history of state and law, Vladivostok, 8 Sukhanova St., Russian Federation, olga-star.05@mail.ru. https://orcid.org/0000-0003-0135-3855*

[3] *Far Eastern Federal University Law School, PhD in political science, Associate Professor of the Department of theory and history of state and law, 690950, Vladivostok, 8 Sukhanova St., Russian Federation, petrova.dan@dvfu.ru https://orcid.org/0000-0001-8751-6402*

[4] *PhD in Law, Vice Director of the Scientific Research Institute of State Building and Local Government of National Academy of Law Sciences of Ukraine Kharkiv, Ukraine, irina_bodrova@ukr.netFederation https://orcid.org/0000-0003-2239-9908*

Fecha de recibido: 2020-11-30
Fecha de aceptado para publicación: 2021-02-01
Fecha de publicación: 2021-03-25

Abstract

The purpose of this article's research is to problematize the legal regulation of work with personal data and other confidential information in the context of large-scale digitization. We sought to systematize the basic concepts used in addressing the topic of information security, such as information, types of protected data, information leakage, types and channels of information leakage. Particular attention is paid to personal data security measures: the legal framework; the specifics of the appointment of sanctions; gaps and collisions in the interaction of legislative acts are determined. The authors concluded that the legal regulation of issues related to personal data and information leakage in Russian legislation is insufficient and inconsistent.

Keywords: information, information security, personal data

Resumen

O objetivo da pesquisa deste artigo é problematizar a regulamentação legal do trabalho com dados pessoais e outras informações confidenciais no contexto da digitalização em grande escala. Procurou-se sistematizar os conceitos básicos utilizados na abordagem do tema segurança da informação, tais como informação, tipos de dados protegidos, vazamento de informação, tipos e canais de vazamento de informação. É dada especial atenção às medidas de segurança de dados pessoais: o quadro jurídico; as especificidades da nomeação de sanções; são determinadas as lacunas e colisões na interação dos atos legislativos. Os autores chegaram à conclusão de que a regulamentação legal de questões relacionadas a dados pessoais e vazamento de informações na legislação russa é insuficiente e inconsistente.

Palabras clave: informação, segurança da informação, dados pessoais

Introduction

The issue of information security has acquired particular relevance in the age of information technology development. Digitizing virtually all data has made it increasingly difficult to preserve meaningful information. The problem is relevant at all levels: state, corporate, and personal. Thus, according to the former Minister of Communications and Mass Media of Russia, the country is exposed 57 million times to cyber-attacks at the state level in just one year (https://tass.ru/politika/1487313). Examples of information leaks from Sberbank (Masalova & Abrekova, 2019), Alfa-Bank,(Chernyshova, 2019). Apple and many others also indicate that corporations are also not protected from virtual hacking. And on a personal level, we have the same: who has not responded with indignation to phone calls with offers to sign up for a free trial procedure for something? We need to define some key concepts before sinking into the analysis of the legal regulation of working with personal data; in particular, what exactly is meant by information and the protection of which information is regulated by Russian law?

According to Federal Law No. 149-FZ dated July 27, 2006 "On Information, Information Technologies and Information Protection", information is knowledge (messages, data) regardless of the form of their presentation, including in digital format. Depending on the category of access, information is divided into public and restricted, access to which is restricted by federal laws (restricted information) (Arutyunov, 2017; Begishev et al., 2019).

Materials. The normative base of the study was made up of framework normative legal acts regulating confidential information by its types: Federal Law dated July 29, 2004 No. 98-FZ "On Commercial Secrets", Presidential Decree No. 188 of March 6, 1997 "On Approval of the List of Confidential Information" as framework document, Federal Law "On Personal Data" dated July 27, 2006, No. 152-FZ, On personal data: Federal Law No. 152-FZ dated July 27, 2006 (as amended on December 31, 2017); On information, information technology and information protection: Federal Law No. 149-FZ dated July 27, 2006 (as amended on December 2, 2019) (as amended and supplemented, and entered into force on December 13, 2019). The factual material that became the basis of the analysis was studied on the basis of periodicals and news data of information and analytical media (Law & Rights, 2006; law No, 2006).

Methods

There are several current concerns concerning the security of information systems, as mentioned above. Spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft are some of these problems; each of these concerns fits under one of two headings: computer misuse or computer crime. The research is based on such methods as the system and structural analysis, which allows differentiation of types of confidential information, as well as a systematization of the main concepts used in coverage of the topic of information security, such as information, types of protected data, information leakage, types and channels of information leaks; formal and legal method, with the help of which regulations governing relations using digital technologies are analysed.

Main part

At the moment, federal legislation protects two types of information: information constituting state secrets, and confidential information.

State secrets are information protected by the state in the field of military, foreign policy, economic, intelligence, counterintelligence and operational and search activities, the dissemination of which may harm the security of the Russian Federation (Tambovtsev, 2014). The legal regime of state secrets is regulated by the Law of the Russian Federation dated 21.07.1993 No. 5485-1 "On state secrets", Decree of the Government of the Russian Federation dated 22.08.1998 No. 1003 "On approval of the Regulations on the procedure for admittance to state secrets of persons with dual citizenship, stateless persons, and persons from among foreign citizens, emigrants and re-emigrants", etc.

In accordance with Federal Law No. 149-FZ dated July 27, 2006 (as amended on December 2, 2019) "On Information, Information Technologies and Information Protection" (as amended and entered into force dated December 13, 2019), confidential information includes the following information (see Table).

Table 1. Confidential information

Type of confidential information	Designation	Clarifying normative legal act
Secrecy of investigation	The data of the preliminary investigation are not subject to disclosure without the sanction of a prosecutor, investigator and inquiry officer	Art. 161 of the Criminal Procedure Code of Russia
Trade secret	Information of any nature (production, technical, economic, organizational, etc.), including on the results of intellectual activity in the scientific and technical sphere, as well as information on the methods of carrying out professional activities that	Federal Law dated July 29, 2004 No. 98-FZ "On Commercial Secrets."

	have actual or potential commercial value due to their unknown third party persons to whom third parties do not have free access on a legal basis and in respect of which the owner of such information has introduced a trade secret regime	
Service secret	Service information, access to which is restricted by state authorities in accordance with the Civil Code of the Russian Federation and federal laws	Decree of the President of the Russian Federation dated 06.03.1997 No. 188 "On approval of the List of confidential information" as a framework document
Personal data	Any information relating to a directly or indirectly identified or identifiable natural person (the subject of personal data)	Federal Law "On Personal Data" dated July 27, 2006, No. 152-FZ

This list is not exhaustive; the law provides for the existence of other types of confidential information. With respect to all this information, restricted access must be observed, but often some of the information goes beyond the permissible boundaries of information storage. In this case, they talk about information leakage.

The leakage of data is the unregulated or unauthorized delivery to the outside of classified information. As the cost of incidents continues to increase, it poses a serious issue for businesses. To provide data protection, many software solutions have been created. Information leakage is the uncontrolled spread of information outside the organization, premises, building, any territory, as well as a certain circle of people who have access to this information (Akhmetzyanova et al., 2018; Sizov et al., 2020).

First of all, speaking about information leakage, they analyse the channels of its leakage. An information leakage channel is a collection of a source (information carrier), information receiver (violator), as well as a physical medium through which information is disseminated from a source to a receiver.

Based on the methods of implementing threats to information security, the channels of information leakage can be classified as follows:

- Technical channels of information leakage;
- Unauthorized access to information;
- Channels of information leakage without the use of technical means.

Information leakage through a technical channel is an uncontrolled distribution of information from a protected information carrier through a physical medium to a technical means that intercepts information. Unauthorized access to information is carried out in violation of the established rights and (or) rules of access to information using standard means of the information system or means similar to them in their functional purpose and technical characteristics (Akhmetzyanova et al., 2018; Sizov et al., 2020).

According to Article 14 of the Federal Law "On State Protection", one of the duties of state security bodies is to implement measures to counter information leakage through technical channels in cooperation with the bodies of the federal security service.

It is not possible to cover all types of confidential information and their security modes in one paper; therefore, we will further focus on this work on ensuring the safety of personal data.

If information constituting state, official and commercial secrets has always been the target of interested parties, then attacks on user data records have become especially relevant after entering the practice of Big Data. With the emergence of a new practice, new players have also emerged: information brokers, or data brokers, companies specializing in the collection and sale of personal data. Data brokers are especially popular in the United States, where there is no dedicated law on personal data protection. Companies compile a dossier on a person from various sources, reflecting in it the level of income, food preferences, frequently used sites, the circle of acquaintances on social networks, etc., and then transfer this information to interested organizations.

The work by A.I. Savelyev contains clear illustrations of the practice implemented by information brokers. In particular, one of the most illustrative examples may be the activities of a Singapore bank, which services monitored banking transactions and made conclusions about the tastes of clients and sent them an individual proposal. For example, a client paid at lunchtime with a bank card next to a street with an Italian restaurant. The bank and the restaurant have entered into a partnership agreement. Knowing that the client prefers Italian food, the bank sends an SMS notification with a special offer in this institution (Savelyev, 2015).

Brokers often use private data on mail accounts. According to Info Watch, in 2019, 14 billion user data records were in the public domain, which is twice as much as in 2018. At the beginning of December 2019, in the Asian segment, Yahoo and Gmail were hacked and placed on a remote server 2.7 billion email addresses; half of these addresses also had a password (The largest dump in history: 2.7) billion accounts Since it is often the practice among users to use one password for several accounts, the information and data of various companies from around the world are under attack.

All well-known social networks have experienced personal data leaks. In 2019, the loudest scandal happened with Facebook, Twitter, LinkedIn and GitHub. According to forecasts of experts from the InfoWatch expert and analytical centre, in 2020, the share of intentional information leaks will only grow. The main reason for these leaks is the too fast pace of digitalization (Baek et al., 2008; Kratov, 2019) and therefore, companies do not have time to develop an effective data protection mechanism.

The problem of stalkers in China is also gaining relevance in connection with the construction of "smart cities", the infrastructure of which is based on the latest technological developments (Baig et al., 2017; Sookhak et al., 2018).

In Russia, the activities of information brokers are limited by the Law on the Protection of Personal Data, which requires the written consent of owners to process their information. However, when filling out the consent to such processing when receiving a discount card, or when subscribing to the store's new items, the client may find an item in the consent form that allows the transfer of data to third parties. This line will allow brokers to use client data in the future.

What are the sanctions provided for the theft of personal data?

With regard to personal data, the legislator has chosen a blanket method of setting out legal norms governing liability for violation of the law on the protection of personal data. Therefore, we can determine the scope and measures of responsibility by referring to the Code of Administrative Offenses and the Criminal Code.

The Code of Administrative Offenses distinguishes between the collection of data in an automated form and a non-automated one. Failure by an operator to fulfil its obligations to store, organize and accumulate information according to paragraph 8 of Article 13.11 entails the imposition of fines, which for citizens are from 30 to 50 thousand roubles, from 100 to 200 thousand roubles for officials, and from 1 to 6 million roubles on legal entities.

Article 272 of the Criminal Code would establish sanctions for persons concerning illegal access to protected information, if the access entailed the destruction, blocking, and modification or copying of computer information. The crime is punishable by a fine (up to 200 thousand roubles), or correctional labour for up to one year, or restraint of liberty for up to two years. In the case of the use of official position, the fine rises to 500 thousand roubles, and the restriction of freedom is changed for up to four years.

Thus, we can say that sanctions for violations of the law on the protection of personal data are rather tangible for citizens and the middle segment of companies that do not have a significant amount of data. We also see at least two significant problems in the implementation of the Law in case of personal data leaks.

Firstly, state use of a photo or other image of a citizen on the grounds of Article 152.1 of the Civil Code of the Russian Federation falls out of the scope of the law. So, this article states that the consents of citizens to the publication and further use of their individual images (including their photographs, as well as video recordings of works of fine art where they are depicted) is not required in cases where:

1. The use of the image is carried out in the state, social, or other public interests.
2. The image of a citizen was obtained during filming, which is carried out in places open to free visits, or at public events (meetings, congresses, conferences, concerts, performances, sports competitions, etc.), except for cases when such an image is the main object use.

The second case is of fundamental importance in the light of the development of information technologies, since it is in the places of free attendance where video recording with the function of face recognition is conducted (Kirichenko & Asetov, 2019). It is logical to assume that since the technology recognizes a face comparing it with the image on video, there is a certain base of images of citizens somewhere. There is little information about it, and citizens did not give consent to both the processing of images and their storage. Thus, a whole layer of data is removed from the law on the protection of personal data. Also, the question remains as to what is the reliability of the image storage location.

An interesting statement from the point of view of personal data protection is the statement of the Governor of Primorsky Krai O.N. Kozhemyako on the use of thermal imagers to identify citizens who violate the regime of self-isolation (Drones with thermal imagers will detect mass concentrations of people.). According to the explanation of Roskomnadzor, (Roskomnadzor clarifications “Features of the use of thermal imagers by employers — operators of personal data — in order to prevent the spread of coronavirus”.). information obtained with the help of a thermal imager (temperature) also refers to personal data, and citizens must give their written consents to the processing of this information. The temperature measurement cases do not fit the list of cases where written consent is not required. It is also unclear if this information would be stored and how. Therefore, the legality of such orders is quite controversial from a legal point of view.

The dissatisfaction of citizens with the state's policy regarding the use of personal data has already caused a trial. On October 7, 2019, in Moscow, a citizen Popova challenged the actions of the Moscow Government on the use of face recognition technology in the video surveillance system of the Russian capital. The citizen demanded that the actions of the Moscow

Government should be declared illegal. The court dismissed the claim but made a reservation that the system compares the image from the video camera with the photo that the police have. The case was sent to the appellate instance.

Secondly, the Law on Personal Data has no extraterritorial effect. In conditions where information leakage occurred through the fault of a foreign operator (such as Facebook or Twitter), the mechanism for protecting the rights of citizens will not work. The Russian law on personal data still stipulates its effect in relation to foreign companies. Federal law obliges foreign companies to store information about Russians on Russian servers. A fine of 3,000 roubles was initially assumed for refusal to localize the databases, and at the moment it is 4 million roubles. Thus, Facebook and Twitter were fined (Cory, 2017; Nasretdinova et al., 2020). The amount of the fine, in our opinion, rather looks like a legal fee for collecting data, since it is in no way comparable to the income of these companies. The blocking of a foreign operator for violation of the law on the territory of Russia is not even provided. This policy creates a paradox: the rules for Russian companies are being tightened, but the green light is given to foreign companies.

A different practice has developed in the European Union. The General Data Protection Regulation adopted in 2018 applies to all operators who process personal data of EU citizens, even if these companies are not located in the Union. The US companies such as Google, Uber and Facebook were fined 50 million euros for each operator for breach of data privacy under the General Regulations.

In conditions when innovative digital technologies and algorithmic systems know much more about us today than we do about them, their impact on our public and everyday life is colossal, and the state policy of Russia with regard to the protection of personal data is contradictory (Baranov et al., 2016; Mamychev et al., 2018). The first contradiction is that the state restricts the operation of the Personal Data Law. The safety of the public storage of personal information raises more questions than the storage of data in commercial companies. The second contradiction is related to the provision of carte blanche to foreign intelligence gathering companies. While weakly controlling the activities of foreign firms to prevent information leaks, the Law on Personal Data does not have any clear mechanisms for bringing foreign violators to justice.

References

Akhmetzyanova, L. R., Alekseev, E. K., & Smyshlyaev, S. V. (2018). *Security bound for CTR-ACPKM internally re-keyed encryption mode*.

Arutyunov, V. V. (2017). Clustering of information-security standards of the Russian Federation. *Scientific and Technical Information Processing*, *44*(2), 125–133.

Baek, E., Kim, Y., Sung, J., & Lee, S. (2008). The design of framework for detecting an insider's leak of confidential information. *Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop*, 1–4.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., & Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13.

Baranov, P. P., Mamychev, A. Y., & Ovchinnikov, A. I. (2016). Institutionalization of the Human Rights Management, Economic and Social Community in the XXI Century: The Global and Eurasian Trends. *International Journal of Economics and Financial Issues*, *6*(8S).

Begishev, I. R., Khisamova, Z. I., & Mazitova, G. I. (2019). Criminal legal ensuring of security of critical information infrastructure of the Russian Federation. *Revista Gênero & Direito*, *8*(6), 283–292.

Cory, N. (2017). *Cross-border data flows: Where are the barriers, and what do they cost?* Information Technology and Innovation Foundation.

Kirichenko, Y. A., & Asetov, S. A. (2019). The Facial Recognition Technology. *Студент: Наука, Профессия, Жизнь*, 249–252.

Kratov, S. (2019). About Leaks of Confidential Data in the Process of Indexing Sites by Search Crawlers. *International Andrei Ershov Memorial Conference on Perspectives of System Informatics*, 199–204.

Law, F., & Rights, F. (2006). On Personal Data. *Hereinafter Referred to as the "Personal Data Law," 152-FZ*.

law No, F. (2006). 152-FL from July 27, 2006 "On Personal Data"(edition of 04.06. 2011)[Federal'nyi zakon ot 27 iyulya 2006 g. № 152-FZ «O personal'nykh dannykh»(red. Ot 04.06. 2011)]. *SZ RF–Collection of Laws of the Russian Federation*, *31 part 1*.

Mamychev, A. Y., Okorokov, A. V., Bespalova, T. V., Sviridkina, E. V., & Chertakova, E. M. (2018). Civilizational modeling of political and legal development of the society in the XXI century. *Amazonia Investiga*, *7*(15), 49–57.

Masalova, A. A., & Abrekova, A. M. (2019). Prospects For The Development Of The

Cyber Insurance Market In Russia. *Современные Научные Исследования и Разработки*, 182–186.

Nasretdinova, D., Kazina, E., Agnew, M., Rodriguez, P., & Nabil, R. (2020). Strengthening the Russian Digital Economy for Long Term Prosperity. *Stanford US-Russia Forum Journal*, *12*(1).

Savelyev, A. I. (2015). Problemy primeneniia zakonodatel'stva o personal'nykh dannykh v epokhu «bol'shikh dannykh»(big data)[Problems of application of legislation on personal data in the era of «big data»]. Pravo. *Zhurnal Vysshey Shkoly Ekonomiki [Law. Journal of the Higher School of Economics]*, *1*, 43–66.

Sizov, V. A., Malinichev, D. M., & Mochalov, V. V. (2020). Improvement of the Regulatory Framework of Information Security for Terminal Access Devices of the State Information System. *Открытое Образование*, *24*(2), 74.

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2018). Security and privacy of smart cities: A survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1718–1743.

Tambovtsev, A. I. (2014). Interaction Of Internal Affairs Bodies With The Media: Advantages And Shortcomings Of The Current Normative Legal Acts. *The Topical Issues of Public Law*, *1*, 90–104.