Legal regulation of privacy data protection

V.V. Sagitova
Department of Computer Engineering and
Information Security
Ufa State Aviation Technical University
Ufa, Russia
e-mail: sagitovavv@mail.ru

V.I.Vasilyev
Department of Computer Engineering and
Information Security
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vasilyev@ugatu.ac.ru

Abstract[1]

The problem of privacy data (PD) protection with account of their specifics is considered. The state-of-art of legal regulation in the field of PD protection in different countries is analyzed. The requirements to PD protection established by law and normative documents of Federal Service for Technical and Export Control (FSTEC) and Federal Security Service (FSS) of Russia are considered. The main changes of legislation in the field of PD protection are analyzed.

1. Introduction

PD protection takes an important place of information security (IS) maintenance of any company.

According to the federal law FL-152 “On privacy data”, PD is defined as any information related to certain individual (PD subject) [1]. PD as a protection object has the following specifics:

- PD are bound to the PD subject;
- PD are heterogeneous, passing from one category to another;
- PD loss cannot be discovered immediately;
- it is difficult to determine the consequences of the PD loss, it can emerge at the PD subject level and at the state level;
- PD are processed in open systems by different operators together with other information;
- other difficulties are linked with budgetary constraints on PD security ensuring and the lack of qualified personnel.

According to the InfoWatch Analytical Center for 2016, more than three billion PD records in the world were compromised [2]. It is three times more than a year earlier. This situation indicates the need to improve the PD protection systems. In modern legal acts of the Russian Federation, a great attention is paid to PD protection, new documents are appeared, the rules for bringing the privacy data protection system (PDPS) into compliance with the requirements of legislation are specified.

Below main directions of PD protection in different countries are considered. The regulatory documents on the PD protection in the Russian Federation are analyzed, including the latest changes in the Russian Federation legislation of PD.

2. The directions for PD protection

The laws of many countries contain basic principles for privacy protection. Currently, there are two directions in the world for PD protection: American and European PD protection models.

The American model is characterized by the lack of the general federal legislation to PD protection and the department that oversees the privacy protection. There are the following main documents: the Privacy Act (1974) and the Privacy Protection Act (1980) [3,4]. These acts are characterized by the following features:

- they are mandatory only for state organizations;
- the verification of PD operators for compliance with the IS requirements is not carried out;
- the liability for violation comes with the leakage of confidential information;
- if the PD subjects rights are violated, then the practice of case law is applied.

The recommendations for minimizing of data and their depersonalization are widespread in the US regulations. These measures make it easier to PD protection. An "umbrella" approach is used in the US, which is based on the use of general legislation. An "umbrella" approach provides relevant data protection in certain areas.

The European Union countries are characterized by the existence of federal legislation to PD protection, the responsible regulator and the responsibility for non-compliance with the legislation in the field of PD

[1] **Proceedings of the 6th All-Russian Scientific Conference "Information Technologies for Intelligent Decision Making Support", May 28-31, Ufa - Stavropol, Russia, 2018**

protection. The main document in this field is the Europe Council Convention "Convention for the protection of individuals with regard to automatic processing of privacy data" [5]. This document defines the procedure for collecting and processing PD, the principles of storage and access to PD, and ways to PD physically protect.

Table 1 provides a comparative analysis of the PD protection regimes in different countries.

3. PD protection in the Russian Federation

The Russian Federation acceded to the European Convention in 2001. The Russian Federation implements mechanisms for PD protection based on the evolution of previously developed basic approaches to IS. The main normative document regulating the PD protection in the Russian Federation is the federal law dated of July 27, 2006 FL-152 "On privacy data" [1]. This normative act establishes:

- the requirements for ensuring PD protection while them processing in privacy data information system (PDIS);
- the principles and conditions for PD processing;
- rights of the PD subject;
- duties of PD operator;
- rights and responsibilities of the responsible regulator for rights protect of PD subject;
- responsibility for violating the requirements of the law.

The requirements of the federal law apply to all state organizations, commercial organizations, individuals who process PD in their information systems. In addition to the federal law FL-152, there are a number of other normative acts on the PD protection:

- Government Decrees;
- orders;
- methodological materials of FSTEC;
- methodological materials of FSS.

Table 2 presents the main regulatory and methodological documents to the PD protection.

Table 1. The PD protection regimes in different countries

Countries	Regulation of PD protection rules (federal or regional levels)	Responsible regulator to monitor compliance with PD protection requirements	Necessity of databases registration	Existence of requirements for leak notification
Russian Federation	At the federal level: FL-152 “On personal data”	Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR)	+	-
Germany	At the federal and regional levels: Federal Data Protection Act “Bundesdatenschutzgesetz” (BDSG) [6]	Each state has its own supervisory authority	-	+
France	At the federal level: “Information Technology, Data Files and Civil Liberty” [7]	National Commission on Information Technologies and Civil Liberties	+	-
USA	No legislation to PD protection at the federal level	Absent	-	+
China	No single system of documents to PD protection	Absent	-	-
Australia	At the federal and regional levels: The Federal Privacy Act, 1988 [8]	The Office of the Australian Information Commissioner	-	-

Table 2. Regulatory and methodological documents to the PD protection in the Russian Federation

Federal law	FL-152 “On privacy data” (27.07.2006)
Government Decrees	№687 “On approval of the regulations on the peculiarities of privacy data processing , carried out without the use of automation facilities” (15.09.2008)
	№512 “On the approval of requirements for material carriers of biometric privacy data and technologies for storing such data outside privacy data information systems” (6.06.2008)
	№1119 “On approval of the requirements to privacy data protection when they are processed in privacy data information systems” (1.11.2012)
	№ 211 “On approval of the list of measures to ensure the fulfillment of the duties provided for by the Federal Law "On privacy data" and regulatory acts adopted in accordance with it, operators that are state or municipal bodies” (21.03.2012)
Orders and other documents	The methods to define actual security threats to privacy data while their processing in privacy data information systems (stated by FSTEC 2008)
	The basic model of privacy data security threats that appear when privacy data are processed in information systems (stated by FSTEC 2008)
	“On approval of the composition and content of organizational and technical measures to ensure the security of privacy data during their processing in the information system of privacy data” (FSTEC Order № 21 of February 18, 2013)
	“On approval of the composition and content of organizational and technical measures to ensure privacy data protection while their processing in privacy data information systems using the cryptographic information security tools necessary to fulfill the requirements set by the Russian Federation government for privacy data protection for each of the protection levels” (FSS Order № 378 of July 10, 2014)

4. Normative documents requirements to PD protection

The Russian Federation Government decree № 1119 dated of November 1, 2012 “On approval of the requirements to privacy data protection when they are processed in privacy data information systems” establishes four PDIS protection levels (PL) and the corresponding requirements for each of them. According to this document, the PDIS protection levels depend on the following criteria:

1. The PD categories:

- special categories of PD including PD that concern race and nation belonging, political views, religious or philosophical beliefs, health conditions, intimate life of PD subjects;
- biometrical PD including data that characterize physiological and biological features of the subject, which make possible a personality identification;
- generally available PD including PD obtained only from public sources;
- other categories of PD not presented in three previous groups.

2. The form of relations between the organization and the subjects:

- processing of operator's employees PD;
- processing of not operator's employees PD.

3. The number of processed PD:

- less than 100 000 subjects;
- more than 100 000 subjects.

4. The groups of threats:

- threats caused by not proclaimed possibilities in system software used in PDIS (the 1st-type threats);
- threats caused by not proclaimed possibilities in applied software used in PDIS (the 2nd-type threats);
- threats not caused by not proclaimed possibilities in software used for PDIS (the 3d-type threats).

The PDIS class in the terms of protection levels is determined in accordance with Table 3.

The order FSTEC № 21 "On approval of the composition and content of organizational and technical measures to ensure the security of privacy data during their processing in the information system of privacy data" establishes:

- PD protection requirements;
- requirements to executors of works to PD protection;
- requirements to assess the effectiveness of measures;
- composition and content of measures to ensure PD protection;

- requirements for the use of computer facilities and IS equipment of certain classes in the PDIS at different protection levels.

Table 3. Criteria for PDIS classification

PD categories	1st-type threats	2nd-type threats	3d-type threats
Special categories of PD	1 PL	1 PL* 2 PL**	2 PL* 3 PL**
Biometrical PD	1PL	2 PL	3 PL
Generally available PD	2 PL	2 PL* 3 PL**	4 PL
Other categories of PD	1 PL	2 PL* 3 PL**	3 PL* 4 PL**
Special categories of operator's employees PD	–	2 PL	3 PL
Generally available PD of operator's employees	–	3 PL	–
Other categories of operator's employees PD	–	3 PL	4 PL

Note. PL – protection level; * more than 100 000 PD subjects; ** less than 100 000 PD subjects.

5. Recent changes in Russian Federation legislation on PD protection

Protecting PD is a complex process because it is subject to stringent requirements. There is a need to take into account PD specificity associated with heterogeneity, attachment to PD subject, difficulty of damage assessment from the implementation of PD security threats. There is a need to take into account the normative documents requirements for PD protection which, in their turn, often are contradictory, often change, do not contain certain recommendations for PD protection and require an improvement. In addition, on July 1, 2017 there were changes in the "Code of the Russian Federation on administrative offenses" [17] on violations of PD protection legislation and on increasing fines for these violations. The article 13.11 of the Code of administrative offenses contains seven sets of offenses with corresponding fines. Therefore, in the current changes in IS legislation, a great attention is paid to PD protection. Normative acts and methodological recommendations regulating the features of PD processing in one or another field are appeared, that greatly simplifies the task of the practical implementation of the law.

An example of such a normative act is a new version of the Bank of Russia branch standard STO BR IBBS-1.0-2014 "Information security providing of Banking System Organizations of the Russian Federation" [18]. In the standard, much attention is paid to PD processing and PD protection. The new version specifies the need to define the criteria for classifying automated banking systems as PDIS.

The Standard has a new term "PD resource" - a PD set, which processed in the banking system organization of the Russian Federation with or without the use of automation. The requirements associated with processing the PD are formed for each PD resource. Issues related to the PD destruction are separately examined: organizations are given the opportunity to delete PD not immediately, but on a periodic basis 1 time in 6 months. It should be ensured that such data is blocked until it is deleted. In addition, the changes touched on the approach to indicator value estimate "General requirements for PD processing ".

Now it is calculated according to the general scheme, and not as a minimum of the values of the incoming private indicators.

New version of Bank of Russia standard takes into account both the specifics of PD, which is processed in automated banking systems, and the latest legislative changes in the field of PD protection.

Another important document on the IS, which has undergone recent changes, is "Doctrine of information security of the Russian Federation" of December 5, 2016 [19]. The document pays much attention to the citizens privacy protection of the Russian Federation when processing PD using information technology. In accordance with the new Doctrine, one of the aspects of privacy protection should be to increase information systems security and other information infrastructure facilities involved in the citizens PD processing. Due to the fact that the current situation is characterized by low awareness of citizens in matters of ensuring privacy IS, one of the main areas of IS in the field of education should be the formation of privacy IS culture of citizens.

6. Conclusion

On the basis of the analysis, it can be concluded that in our country the regulation of the PD protection issues is sufficiently developed. However, there are still weak points. The requirements for PD protection are rigidly defined and the fines size is not proportional to the possible damage to the PD subject that occurs when large leaks occur. In addition, there are fines for violating legal requirements, and not for data leakage. In this case, the operator should pay attention not only to protection against regulators sanctions, but also to protect the data from leakage. Therefore, there is a need to create techniques and methods that will allow PD operators to protect data from leakage in a particular area of the company's operations.

References

1. On privacy data: The Russian Federation Federal Law, dated of July 27, 2006 № 152-FL (with changes from 29.07.2017) [Electronic resource] URL: http://ivo.garant.ru/#/document/12148567:0 (the date of visit 14.09.2017). (In Russian).

2. Infowatch analytical center reference on privacy data leaks which citizens voluntary provide to organizations [Electronic resource] URL: https://www.infowatch.ru/analytics/leaks_monitoring/18095 (the date of visit 14.09.2017). (In Russian).

3. Privacy Act of 1974: United States Federal Law, dated of December 31, 1974 [Electronic resource] URL: https://www.justice.gov/opcl/file/844481 (the date of visit 14.09.2017). (In English).

4. Privacy Protection Act of 1980: United States Federal Law [Electronic resource] URL: https://www.justice.gov/usam/criminal-resource-manual-661-privacy-protection-act-1980 (the date of visit 14.09.2017). (In English).

5. Convention for the protection of individuals with regard to automatic processing of privacy data: Europe Council Convention, dated of January 28, 1981 [Electronic resource] URL: http://www.conventions.ru/view_eng.php?id=1097 (the date of visit 14.09.2017). (In English).

6. Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG): Germany Federal Law, dated of January 14, 2003 [Electronic resource] URL:http://www.gesetze-im-internet.de/englisch_bdsg (the date of visit 14.09.2017). (In English).

7. Information Technology, Data Files and Civil Liberty: France Federal Law, dated of January 6, 1978 (with changes from 17.03.2014) [Electronic resource] URL:https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf (the date of visit 14.09.2017). (In English).

8. Privacy Act 1988: Australian Law [Electronic resource] URL: https://www.oaic.gov.au/privacy-law/privacy-act/(the date of visit 14.09.2017). (In English).

9. On approval of the regulations on the peculiarities privacy data processing, carried out without the use of automation facilities : The Russian Federation Government Decree № 687// Rossiyskaya gazeta, 2008. (In Russian).

10. On the approval of requirements for material carriers of biometric privacy data and technologies for storing such data outside privacy data information systems : The Russian Federation Government Decree № 512// Rossiyskaya gazeta, 2008. (In Russian).

11. On confirmation of requirements to privacy data protection under their processing in privacy data information systems : The Russian Federation Government Decree № 1119// Rossiyskaya gazeta, 2012. (In Russian).

12. On approval of the list of measures to ensure the fulfillment of the duties provided for by the Federal Law "On privacy data" and regulatory acts adopted in accordance with it, operators that are state or municipal bodies" : The Russian Federation Government Decree № 211// Rossiyskaya gazeta, 2012. (In Russian).

13. The methods to define actual security threat to privacy data when the data is processed in privacy data information systems [Electronic resource] : Method. document : [stated by FSTEC of Russia February 14, 2008] URL: http://fstec.ru (the date of visit 14.09.2017). (In Russian).

14. The basic model of privacy data security threats that appear when privacy data are processed in information systems [Electronic resource]. : Method. document : [stated by FSTEC of Russia 2008] URL: http://www.zki.infosec.ru (the date of visit 14.09.2017). (In Russian).

15. On approval of the composition and content of organizational and technical measures to ensure the security of privacy data during their processing in the information system of privacy data : [stated by FSTEC of Russia February 18, 2013] URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (the date of visit 14.09.2017). (In Russian).

16. On approval of the composition and content of organizational and technical measures to ensure privacy data protection when processing them in privacy data information systems using the cryptographic information security necessary to fulfill the requirements set by the Russian Federation government for personal data protection for each of the protection levels : [stated by FSS of Russia July 10, 2014] URL: http://base.garant.ru/70727118/ (the date of visit 14.09.2017). (In Russian).

17. Code of the Russian Federation on administrative offenses (with changes from 29.07.2017) [Electronic resource] URL: http://koapkodeksrf.ru/ (the date of visit 14.09.2017). (In Russian).

18. Information security providing of Banking System Organizations of the Russian Federation : STO BR IBBS-1.0-2014, dated of May 17, 2014 [Electronic resource] URL: http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf (the date of visit 14.09.2017). (In Russian).

19. Doctrine of information security of the Russian Federation : The Russian Federation Doctrine, dated of December 5, 2016 [Electronic resource] URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (the date of visit 14.09.2017). (In Russian)