Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The use of Big Data: A Russian perspective of personal data security

Anna Konstantinovna Zharova [a,*], *Vladimir Mikhailovich Elin* [b]

[a] *Department of Innovations and Business in IT, Faculty of Business and Management, National Research University Higher School of Economics, Moscow, Russia*

[b] *Department of Information Security, National Research University, Higher School of Economics, Moscow, Russia*

Keywords:
Personal data
Privacy
Identifying information
Russia
Personal data security
Russian public authorities
Big Data

A B S T R A C T

This article examines the impact of Big Data technology on Russian citizens' constitutional rights to a private life. There are several laws in the Russian Federation covering data privacy and protection, but these are proving inadequate to protect the citizens' rights in the face of the ever-increasing use of massive data sets and their analysis by Big Data tools. One particular problem in this regard is that datasets of anonymised records currently not covered under personal data laws (because they do not identify individuals) can, in fact, be used to identify data subjects (the individuals to whom the data refers) when combined and analysed using Big Data tools. Furthermore, existing sanctions for misuse of personal data are minor, and often fail to act as a deterrent when the commercial benefits of exploiting user data (e.g. through targeted advertising) are so much greater. From the point of view of companies handling Big Data, a general confusion over definitions and responsibilities is making compliance with the law difficult, leaving most to come up with their own forms of best practice, rather than being able to follow clear industry recommendations. The article examines existing laws and oversight bodies, discusses how the current provisions are inadequate to deal with new developments in Big Data, and proposes recommendations for amending and updating existing laws and policies.

1. Introduction

The development of information technology (IT) has increased the possibilities for personal data to be used in ways that are damaging to the data subject. However, the creation of strong organisational measures and legal regulation can potentially reduce the level of threats and risks. This article focuses on the processing of personal data using what is generally referred to as Big Data technology. We understand "Big Data" as a set of information technology, tools, data and processes that allows the analysis of large sets of structured and unstructured data. A particular difficulty lies in the separation of information into identifying information that relates to specific people, and anonymised data that, in theory at least, gives a general picture without identifying individuals. It has been

* *Corresponding author.* 33 Kirpichnaya Str., Moscow, Russia. Fax: (495) 771-32-38.
E-mail address: ajarova@hse.ru (A.K. Zharova).

http://dx.doi.org/10.1016/j.clsr.2017.03.025

noted that information, which is initially presented as anonymised, can still be used to identify individuals, especially when two or more anonymised databases are combined for analysis with Big Data tools. For example, research of Massachusetts Institute of Technology specified that *"just four fairly vague pieces of information – the dates and locations of four purchases – are enough to identify 90% of the people in a data set recording three months of credit-card transactions by 1.1 million users"*.[1]

This article explores the privacy, security and consumer welfare issues linked with the collection, storage, analysis, processing, reuse and sharing of data within the Russian Federation, with a particular focus on issues that arise with Big Data. It discusses legal issues relating to the management and security of personal data processed by Big Data technology and looks at the role of the state in regulating the industry, exploring existing measures such as legislation and industry guidelines, as well as the role of the courts and of governmental oversight body in enforcing standards. There is a particular focus on the use of data gleaned from the Internet about the activities of users, which can potentially be used to profile individuals for commercial gain (e.g. targeted advertising) to identify good or bad candidates for credit, or to set insurance premiums.

The discussion section explores the effectiveness of Russian legislation in providing clear, usable guidelines for business, adequate protection for individual privacy and appropriate sanctions for organisations that fail to meet these requirements. It examines how in many cases, legislation is contradictory or simply out-of-date when it comes to protecting personal data, especially when datasets created for different purposes are combined for analysis by Big Data tools. The authors furthermore note that administrative sanctions, consisting of minor fines, applicable in the case of abuse of personal data, often fail to deter certain businesses from mining personal data, as the financial benefits of doing so often outweigh the fines.

The article concludes with a set of recommendations for adaptation of current legislation to provide more protection for data subjects, clearer guidelines for companies to help them comply with the legal requirements, and firmer, criminal sanctions in the case of intentional misuse of personal data.

This article seeks to contribute to the literature in two respects. Firstly, it offers insights into how various characteristics of Big Data are linked to privacy, security and consumer welfare issues. Secondly, it shows how the privacy, security and consumer welfare aspects of Big Data are linked to the interrelated issues of information collection, storage, sharing and accessibility.

The following research questions guided this article:

1. Is Big Data a unique information technology that requires the development of new legal and practical approaches to the security and management of personal data?
2. Is the Russian legislative system ready to regulate the security of personal data in Big Data?
3. Can businesses adapt their activities to existing legal principles?
4. Do the principles of the legal requirements satisfy the business environment?
5. How can recommendations be formulated to address the problems identified?

2. Legal background

The following section explores the legal definitions pertaining to data privacy and Big Data, the state bodies that have responsibility for ensuring data security and individual rights to privacy, and the existing laws in the Russian Federation that govern the responsibilities of data handlers. One particular point to bear in mind is that the existing Russian Federation laws described below were designed to establish and uphold principles of privacy in the handling of personal data, but that these laws[2] are not fully equipped to ensure these principles are upheld in the case of Big Data analysis. These shortcomings are explored further in the Discussion section, and recommendations for updating existing laws are presented in the Conclusions.

2.1. *The concept of Big Data*

Big Data technology allows the collection and processing of large amounts of data, including personal information or information that can identify an individual. In this regard, Russia faces a number of challenges in terms of protecting confidentiality in the provision of services reliant upon personal data such as online purchases, social networks and banking. These challenges include ensuring personal data is secure from theft or leaks, balancing companies' ability to access to personal data with individuals' right to privacy, and ensuring that the protection for anonymity provided by law is extended to data processed using Big Data tools.

No widely accepted definition of Big Data technology exists. In Russia, at the conference "Big Data and Business Intelligence 2012", research manager Alexander Prokhorov pointed out that four Vs determine Big Data: volume, variety, velocity and the numerical values of infrastructure,[3] as does the European Union Agency for Network and Information Security (ENISA).[4] Gartner 2013 defined Big Data in terms of three Vs: volume, variety and velocity. However, by 2015 Gartner did not include Big Data in his report "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations that Organizations should Monitor",[5] explaining that the concept

[1] Privacy challenges. Analysis: It's surprisingly easy to identify individuals from credit-card metadata. Available from: http://news.mit.edu/2015/identify-from-credit-card-metadata-0129 [Accessed 17 February 2017].

[2] Federal Law № 149 "On information, information technologies and protection of information", Federal Law № 152-FZ "On Personal Data", etc.

[3] Naidich A, "Bolshiye dannyie: naskolko oni bolshiye? [Big Data: How big it is]" (2012) 12 *Kompyuter Press*. Available from http://compress.ru/article.aspx?id=23469. [Accessed 1 June 2016].

[4] Naydenov R, Liveri D, Dupre L, Chalvatzi E and Skouloudi Ch, "Big Data Security" (European Union Agency for Network and Information Security 2015). doi: 10.2824/13094.

[5] "Gartner's 2015 Hype Cycle for Emerging Technologies identifies the computing innovations that organizations should monitor". Available from http://www.gartner.com/newsroom/id/3114217. [Accessed 1 June 2016.

of "Big Data" includes a variety of technologies that are relevant to other popular areas and trends which have become everyday working tools.

In Russia, there is no official definition of Big Data either at the legislative level or within the IT industry. This is confirmed by the study "100 profiles of top Russian companies about the strategy in Big Data" conducted by TAdviser analysts in 2014. Their survey uncovered the "multiplicity of interpretations of the term and the plurality of its definitions" within the industry. Furthermore, as this report points out, *"the public sector uses Big Data relatively weakly"* despite it being used by several government agencies, including the Federal Tax Service, the analytical centre of the Russian government, the Pension Fund, the Government of Moscow, the Mandatory Health Insurance Fund, the Federal Security Service, the Investigative Committee and the Foreign Intelligence Service.[6]

Ziora[7] cites the McKinsey Global Institute report of 2011, which identified four sectors in which Big Data technology may be used, namely the health sector, public administration, retail trade, and the production and use of location data. In Russia, in addition to the above, this technology is also used in the banking sector.

According to Russian research conducted by CNews Analytics, "banks are actively considering the use of Big Data technologies to search for debtors and to facilitate the more efficient operation of collection services. In 2015, representatives of 11 financial institutions said that their banks use modern technology to analyze Big Data. Five [other] banks plan to implement these technologies".[8] Monitoring clients' personal data to assess risk or stimulate demand seems an attractive idea for a company but not, generally, for consumers, since such data can be used in ways that are not in their interest, for example by restricting borrowing based on their past behaviour or financial records.

Given the increasingly widespread analysis of personal data by means of Big Data technology, we consider the possible legal problems of ensuring personal data is processed according to the principles of confidentiality and privacy, and of ensuring the accountability of companies and public sector agencies that collect and analyze such data. We also explore the solutions companies provide when problems arise.

In Russia, there are no special "cyberlaws" regulating these new kinds of relationships between individuals and the institutions that collate and make use, by means of IT, of personal information about them. Because of this, the current system of legal norms, was formed on the basis of sectoral laws (see "On Telecommunications", Federal Law № 149 "On information, information technologies and protection of information" [hereinafter the Federal Law "On information"], Federal Law № 152-FZ "On Personal Data" [hereinafter the Federal Law № 152] and others), on the analogy of the law, including on international law.[9]

These Acts introduced a number of provisions determining how personal data may be processed through information and telecommunications networks.[10] They specify that any data operator collecting personal data, including network Internet, be obliged to use servers located on Russian Federation territory.[11] Responsibility for compliance with Federal Law № 152 lies with the operator (service provider). Article 15.5 of the Federal Law "On Information" defines measures the state can take if these requirements are violated, including the creation of a "Register of violators of the rights of personal data subjects" and the adoption of measures to restrict access to information.

When it comes to the secure and confidential processing of big data sets which hold information on private individuals, the complex problems of legal regulation, the novelty of legal relations in this area, and a general lack of sufficient legal and sectoral practice in Russia are proving challenging to resolve.

2.2. *Public bodies involved in personal data protection*

There are a number of public bodies in the Russian Federation involved with personal data protection, including the Federal Service for Technical and Export Control (FSTEC),[12,13] the Federal Security Service (FSS)[14,15] and the Federal Service for Supervision of Communications, Information Technology and Mass Communications (Roscomnadzor). Additionally, regulations have been implemented by the Central Bank of the Russian Federation and others, since personal data can include any information that is related to banking, personal tax details

[6] TAdviser. (2015). "100 profiles of top Russian companies about the strategy in Big Data" [Report]. Available from http://www.tadviser.ru/index.php. [Accessed 3 June 2016].

[7] Ziora ACL, "The Role of Big Data Solutions in the Management of Organizations. Review of Selected Practical Examples" (2015) 65 Procedia Computer Science 1006 DOI:10.1016/j.procs.2015.09.059.

[8] Kiryanova A, "Bolshiye dannyie ne stali meinstrimom v rossiyskikh bankakh [Big Data will not become mainstream in Russian banks]" (CNews.ru 2015). Available from http://www.cnews.ru/news/top/bolshie_dannye_ne_stali_mejnstrimom. [Accessed 18 June 2016].

[9] Zharova A, Elin V, Dem'yanets M, Entrepreneurial activity on the Internet (Yurcompany 2014).

[10] Federal Law of 21.07.2014 No 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation to clarify the processing of personal data in the order of information and telecommunications networks" //Rossiyskaya gazeta, No 163, 07.23.2014.

[11] Federal Law № 152-FZ "On Personal Data".

[12] Federal Service for Customs and Export Control (2013a). On approval of the composition and content of organisational and technical measures to ensure the security of personal data being processed in information systems. FSTEC RF 18.02.

[13] Federal Service for Customs and Export Control (2013b). On Approval of the requirements for the protection of information, not including state secrets, contained in state information systems. FSTEC RF 02.11.

[14] Federal Security Service. (2009). Model rules of the authority regarding measures for control (supervision) over compliance with the requirements established by the Russian Government to ensure the security of personal data while being processed in information systems. Approved by the Federal Security Service of Russia 08.08. No. 149/7/2/6–1173.

[15] Security Service of Russia (2008). Methodical recommendations for personal data security by using cryptographic processing in information systems. Approved by Federal Security Service of Russia. 21.02.2008 No. 149/54–144.

and other categories of restricted information.[16] Sectoral approaches are based on the use of industry standards, for example, those governing the requirements for protecting information systems holding personal data in the non-state pension fund.[17] Bank of Russia designs their own standard[18]: other legal entities of various industries have their own standards.

The standards of the Bank of Russia viz. methods of assessing the conformity of the information security organisations of the Russian banking system specify methods for determining the fulfilment of the requirements to ensure the information security of organisations of the Russian banking system, and the final level of information security (IS) compliance of banking organisations with the standards of the Bank of Russia. These methods define the standard approaches and methods of the assessment in key areas[19]:

- the current level of information security of the organisation;
- information security management in the organisation;
- the level of the information security awareness in the organisation.

The standard defines group and individual IS indicators, methods of assessment of these indicators and the degree of the information security compliance in the organisation, the formula of assessment of the current level of information security of an organisation of the Russian Federation banking system. Requirements and formula of assessment of the information security management of an organisation of the Russian Federation banking system are defined.

Group and individual IS indicators in the following areas are used to evaluate the degree of compliance with IS requirements of the Central Bank of Russia ensuring IS:

- in assigning and allocating roles and ensuring confidence in personnel;
- at the stages of ABS life cycle;
- in access and registration control;
- by antivirus protection tools;
- when using Internet resources;
- when using data encryption tools;
- of bank payment technological processes;
- of bank information technological processes;
- personal data processing in a RF BS organisation;
- banking technological processes used for personal data processing.

The assessment of the group indicator is calculated as an arithmetic mean of the assessments of individual indicators included in this group indicator. Group indicators form the structure of assessment areas by providing the details on the assessment of the current IS level in an organisation, IS management and level of IS awareness.

The assessment of the current IS level of a bank is determined by IS group and individual indicators.

Individual indicators are divided into two types. The first type includes individual indicators, which are mandatory for compliance; the second type includes recommended individual indicators. The assessment of the individual indicator is based on the degree of compliance with the requirements identified by the auditing team through expert assessment. The assessment of the mandatory individual indicator shall be accompanied by entering a symbol or value assignment. For the recommended individual indicator "1" is indicated in compliance and "0" – in the absence.

The assessment of the individual IS indicator should be based on evidence. It is recommended to use the following as the main sources of evidence:

- internal documents of the audited organisation and, when necessary, third party documents relating to ensuring IS of the organisation;
- verbal statements from employees of the audited organisation made during interviews;
- results of observations on the activities of employees of the audited organisation made by the members of the auditing team.

During interviews of employees of the audited organisation and observations on the activities of these employees, the members of the auditing team should make a conclusion on the degree of conformity of the audited activities to the requirements of internal documents of the audited organisation.

The evidence obtained for the assessment of IS conformity and its sources shall be documented.

In this case, Russia follows ENISA's recommendation that "standardisation bodies should adapt existing standards or create new security standards to include Big Data".[20]

In this case, Russia shares the proposition European Union Agency for Network and Information Security (ENISA), namely that "T bodies should adapt existing standards or create new security standards to include Big Data".[21]

International recommendations[22] regarding personal data protection include the following:

[16] For example: art. 102 of the Tax Code of the Russian Federation "Rossiyskaya Gazeta" No 148–149, 06.08.1998; art. 139 of the Family Code of the Russian Federation "Rossiyskaya Gazeta" No 17, 27.01.1996; art. 26 of the Federal Law 02.12.1990 No 395-1 "On banks and banking activity" "Rossiyskaya Gazeta", No 27, 10.2.1996, etc.

[17] Official website of the non-state pension fund. Available from http://napf.ru/14154.

[18] Russian Standard of Russian Bank STO BR IBBS-1.2-2014 "Information security organisations the Russian banking system. Methods of assessing the conformity of the information security organisations of the banking system of the Russian Federation, the requirements of STO BR IBBS-1.0-2014". Adopted and put into effect the order of the Bank of Russia of 17 May 2014 No. R-399.

[19] Ibid.

[20] D' Acquisto G, Domingo-Ferrer J, Kikiras P, Torra V, de Montjoye Yv and Bourka A, "Privacy by design in big data" (European Union Agency For Network and Information Security Privacy 2015). doi: 10.2824/641480.

[21] D' Acquisto G, Domingo-Ferrer J, Kikiras P, Torra V, de Montjoye Yv and Bourka A, "Privacy by design in big data" (European Union Agency For Network and Information Security Privacy 2015). doi: 10.2824/641480.

[22] RRI Opportunities in Horizon 2020. Science with and for Society relevant topics in the Horizon 2020. Work Programme 2016-17. The project funded by the European Commission. Available from https://www.hse.ru/data/2015/12/11/1133574498/RRI_opportunities_in_%20Horizon%202020_151208.pdf. [Accessed 1 June 2016].

- Policy makers should provide guidance for the secure use of Big Data systems in critical information infrastructures (such as those involved in defence, security and the rule of law).
- Big Data providers or vendors should invest in compliance with security standards for their products (devices, cloud services, etc.).
- The appropriate authorities overseeing critical sectors should encourage vendors to offer security authentication mechanisms and protocols in their products.
- Standardisation bodies should adapt existing or create new security standards for Big Data.

Industry players and vendors should invest more in enhancing the technical security skills of staff who use Big Data through training and certifications.

There is a diverse range of industry standards designed to deal with the obligations on the operator handling personal data to "*independently determine [its] composition and [create] a list of legal, organisational and technical measures for ensuring [its] security*" (Article 18.1, Federal Law № 152).[23] The lack of a uniform Russian approach has both positive and negative aspects. On the one hand, diversity in standards may create a situation where technologies that might be useful in combination for data protection are not interoperable. On the other hand, diversity makes it easier to protect data, because measures based on various security models are harder to hack than a system based on a single model.

According to Article 23 of the Federal Law of (27 July 2006 № 152-FZ) "On personal data", the body authorised to protect the rights of personal data subjects is Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Communication). Roskomnadzor determines the appropriate treatment of personal data according to the specific content of the data being collected and the methods of processing it.

President Putin determined that measures relating to the security of personal data should be enforced by FSTEC, the federal executive authority responsible for the implementation of state policy.[24] FSTEC's role includes the control of information relating to national security, protecting information with restricted access, preventing leaks through technical channels, guarding against unauthorised access, and undertaking specific actions to against information carriers aiming to obtain, destroy or distort sensitive information or block access to the territory of the Russian.[25] The Federal Security Service (FSS) not only secures state secrets, but also determines procedures for encryption for the protection of non-state secrets, such as personal data.[26,27]

According to Articles 1, 21 and 26 of the Federal Law "On the Prosecutor's Office of the Russian Federation",[28] the Prosecutor General's Office supervises the observance of the Constitution of the Russian Federation and compliance with the law. The Prosecutor General's Office is therefore empowered to check Roskomnadzor's performance in overseeing the laws on data protection.

In 2012, Roskomndazor created an Advisory Council to protect the rights of personal data subjects (20 June 2012, № 621). Its functions included harmonising Russian Federation legislation on the protection of personal data and ensuring compliance with it, analysing both public opinion and the experiences of legal practitioners in this area, and providing methodological support for enforcement of the legislation. Roskomnadzor also cooperates on compliance with international standards with the authorities of foreign states and international organisations (Para. 5.15. Government Decree № 228).

Roskomnadzor's activities also relate to the package of "anti-terror" laws[29] adopted in 2016, which ensure access to information by law enforcement officials for the investigation and suppression of crime. This package complements Russian legal definitions such as "the organizer of the dissemination of information on the Internet".

However, this requirement on localisation information was enshrined in law in 2005. According to p. 12 of the "Rules for interaction of operators with authorized state bodies engaged in operational-search activities",[30] approved by the Russian Government:

> "The operator is obliged to update information contained in the databases of subscriber service providers and provide them with services. This information should be kept by the operator for 3 years". In our opinion, here we can see the

[23] Federal Law № 152-FZ "On Personal Data" "Rossiyskaya gazeta", No 165, 29.07.2006.

[24] Presidential Decree, "Issues of the Federal Service for Technical and Export Control" No. 1085. (2004) 34 "*Collection of the legislation of the Russian Federation*" 3541.

[25] Federal Service for Customs and Export Control (2013a). On approval of the composition and content of organisational and technical measures to ensure the security of personal data at their processing in information systems of personal data. FSTEC RF 18.02.

[26] Federal Security Service. (2009). Model rules of the authority regarding measures for control (supervision) over compliance with the requirements established by the Russian Government to ensure the security of personal data while being processed in information systems. Approved by the Federal Security Service of Russia 08.08. No. 149/7/2/6–1173.

[27] Security Service of Russia (2008). Methodical recommendations for personal data security by using cryptographic processing in information systems. Approved by the Federal Security Service of Russia. 21.02.2008 No. 149/54–144.

[28] The Federal Law "On Prosecutor's Office of the Russian Federation" of 17.01.1992 № 2202-1.

[29] The federal law from 06.07.2016 No 375-FZ "On Amendments to the Criminal Code of Russian Federation and the Criminal Procedure Code of Russian Federation with regard to establishing additional measures to counter terrorism and ensure public safety" "Rossiyskaya Gazeta", of No 150, 07.11.2016; The federal law from 06.07.2016 No 374-FZ "On Amendments to the Federal Law" On Combating Terrorism "and Certain Legislative Acts of Russian Federation to establish additional measures to counter terrorism and ensure public safety" "Rossiyskaya Gazeta", No 149, 08.07.2016.

[30] Government Decree of Russian Federation. (2005). "On Approval of Rules of interaction of operators with the authorised state bodies, engaged in the operational-search activities" of 27.08.2005, No. 538.

ratio of the RF Government Decree with the rules of the former European Directive 2006/24/EC (invalidated in 2014) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the "Data Retention Directive"). This directive obliges providers of internet and telephony services to keep detailed "traffic data" (or "metadata") regarding the identities and activities of their subscribers for between 6 and 24 months and provide access to police and security agencies for the purposes of investigating serious crime. It has been described as the "the most privacy-invasive instrument ever adopted by the EU".[31]

However, such long-term data storage increases the probability of information leakage and requires using reliable information systems ensuring data security. However, as we know, such a system cannot be created; there is no absolutely reliable technology. In this regard, we suppose that the EU decision[32] to reduce the storage time is a possible solution in such a situation.

Much of the logic of the proposed changes to Russian Federation legislation is similar to the logic of the EU 2006/24/EC Directive "On data storage" (which was declared invalid by European Court of Human Rights in 2014), which defines the duties of ISPs regarding the storage and transfer of Internet traffic to law enforcement agencies. However, civil legal relationships in this sphere are currently not covered under the rules for interaction of operators with authorised state bodies engaged in operational search activities. These rules are aimed at the implementation of actions related to pre-investigation and investigation of crimes.

Currently, Directive "On Privacy and Electronic Communications" No 2002/58/EC[33] with regard to the shelf life operates with concepts:

- the time period associated with the further need to send the message;
- the time period during which can be legally disputed bill for services;
- the time period necessary for such services or marketing.

The Russian databases must contain the following information on subscribers of operator:

- surname, first name, middle name, place of residence and details of the main identity document presented at a personal presentation of the subscriber of the document to a subscriber–citizen;
- the (corporate) name of the legal entity, its location, and a list of persons who use the equipment of the legal entity, including their names (first names and patronymic), place of residence and details of the main identity document of the subscriber;
- information on payments for services rendered, including connections, traffic and billing of subscribers;
- information about the subscriber's telephone number, which is stored at the conclusion of contracts for the provision of telecommunications services to other mobile telephone communications operators, and the names of these operators.[34]

But as A. Savelyev notes: "until recently, Russian legislation did not contain any special provisions governing data location . . . The first signs of data localization provisions appeared in the banking sphere . . . in 2013".[35]

In 2015, Roskomnadzor adopted measures to allow applications for the restriction of access to personal information processed in violation the Russian Federation legislation on personal data.[36]

2.3. *The status of personal information in the Russian Federation: conflicting concepts of privacy and personal data*

The European approach can be traced in the Russian personal data security system. Chronologically: In 1997, the term "personal data" was defined in the Russian Federation in Presidential Decree № 188 "On the approval of information of a confidential nature". At the level of federal legislation, the concept of "personal data" was enshrined in 2006 in Federal Law № 152-FZ "On Personal Data" (hereinafter Federal Law № 152). Federal Law № 152 defines personal data as *"any information that can directly or indirectly identify a person"*. According to this definition, any such data, including depersonalised data, can be considered personal data. The depersonalisation of personal data refers to actions that make it impossible to determine the identity of the person to whom the information pertains. Despite Federal Law №152 having been in existence for ten years, researchers are still discussing what information can be defined as personal data and what cannot.[37]

[31] Jones C and Hayes B, "D2.4 The EU Data Retention Directive: a Case Study in the Legitimacy and Effectiveness of EU Counter-Terrorism Policy" (Statewatch, SECILE 2013). http://www.statewatch.org/news/2013/nov/data-retention-directive-in-europe-a-case-study.pdf. [Accessed 3 November 2016].

[32] Jones C and Hayes B, "D2.4 The EU Data Retention Directive: a Case Study in the Legitimacy and Effectiveness of EU Counter-Terrorism Policy" (Statewatch, SECILE 2013). http://www.statewatch.org/news/2013/nov/data-retention-directive-in-europe-a-case-study.pdf. [Accessed 3 November 2016].

[33] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201 , 31/07/2002 P. 0037 - 0047. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[34] Government Decree of Russian Federation. (2005). "On Approval of Rules of interaction of operators with the authorised state bodies, engaged in the operational-search activities" of 27.08.2005, No. 538.

[35] Savelyev A, "Russia's new personal data localisation regulations: a step forward or a self-imposed sanction?" (2016) 32 Computer law and security review. doi: 10.1016/j.clsr.2015.12.003.

[36] Order Roskomnadzor from 22.07.2015 No 85 "On approval of the application form the subject of personal data on the adoption of measures to restrict access to information processed in violation of the Russian legislation in the field of personal data" (Registered in the Ministry of Justice of Russia 17.08.2015 No 38544).

[37] Dupan A et al. The new paradigm of protection and personal data management in the Russian Federation and foreign countries in terms of data processing systems on the Internet (The Publishing House of the Higher School of Economics 2016).

Russian and European approaches to the protection of personal data are similar in most respects. In 2005, Russia adopted the Federal Law "On Ratification of the Convention for the protection of individuals with regard to automatic processing of personal data" (ETS № 108).[38] However, the Russian legal tradition of ensuring privacy security has deeper roots. The right of citizens to the security and confidentiality of correspondence and dwellings was determined by the Constitution of the USSR in 1937. The Constitution of 1978 also identified citizens' rights to a private life, including to privacy of written correspondence, telephone conversations, telegraphs and other communications, as fundamental.

The new Russian Constitution of 1993 retained the concept of personal and family secrets and the confidentiality of correspondence, telephone conversations, postal, telegraph and other communications (Article 23). The provisions of the Constitution correspond to the norms of Article 12 of the Universal Declaration of Human Rights[39] that no one shall be subjected to arbitrary interference with his private and family life. These rights are protected by the rules of criminal and civil law. However, personal data protection is provided for only in administrative law.

There is, furthermore, a significant problem with inconsistencies in the legal status of information. The civil law of the Russian Federation of 1 January 2008 excluded information from the list of objects of civil law transactions.[40] However, the Federal Law "On Information, Information Technologies and Protection of Information" (hereinafter the Federal Law "On Information") determines that information may be the object of public, civil and other legal relationships. Information may be freely used by any person, and transmitted from one person to another if federal law does not restrict access to that information or have other requirements regarding its delivery or distribution (Article 5, Part 1). Under the provisions of the Federal Law "On Information", this category of information should be classified as information with limited access.

A decision by the Constitutional Court of the Russian Federation[41] indicated that:

> "In the provisions of Articles 23 (part 1) and 24 (part 1) of the Constitution, any information about the private life of a person is of a confidential nature, because it is information of restricted access. The right to privacy in personal and family life is acknowledged by the state, and the ability to control information about oneself and prevent the disclosure of information of a personal, intimate nature is guaranteed. The concept of a 'private life' includes any area of human activity that relates to an individual and concerns only him and is not subject to control by society or the state, [as long as the] actions of the person are legal. Accordingly, only the person has the right to determine what kind of information relates to his private life and must remain a secret. Therefore the collection, storage, use and dissemination of such information is not permitted without the consent of the person, as required by the Russian Federation Constitution."

Personal and family secrets and the confidentiality of correspondence, telephone conversations, postal, telegraph and other communications are protected by the rules of criminal and civil laws. For example: Art. 137 of the Russian Criminal Code provides for criminal liability for illegal collection or dissemination of an individual's private information that constitutes his/her personal or family secrets without his/her consent or dissemination of this information, and provides for a maximum penalty of 5 years of imprisonment.[42] Violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other messages of citizens (Art. 138 of the Russian Criminal Code) provides for a maximum penalty of up to 4 years of imprisonment. Disclosure of secrets of adoption (Art. 155 of the Russian Criminal Code) provides for corrective labour, etc. as a punishment.

The Civil Code of the Russian Federation considers the name of a citizen, privacy, personal and family secrets to intangible benefits, along with life, health, dignity and personal inviolability (Art. 150 of the Civil Code).[43]

The collection, storage, dissemination and use of any information on the private life of a citizen shall not be allowed without his/her consent, in particular, this includes the information about his/her origin, the place of his/her residence or domicile, private and family life (Art. 152.2 of the Russian Civil Code).

It is especially determined that the publication and further use of the image of a citizen shall be allowed only with the consent of the citizen (Art. 152.1 of the Russian Civil Code).

Gloria Gonza'lez Fuster and Serge Gutwirth[44] believe that:

> "in the literature, the affirmation of the very existence of a European right to the protection of personal data is still relatively rare. When its existence is recognized, it is often discussed in conjunction with privacy – be it to assert the continuities or discontinuities between them. We think that the right to privacy consists of two components: the possibility of ensuring a person can be left alone, in terms of independence from the state and society; and the ability to control information about oneself and prevent the disclosure of personal information, in particular that of an intimate nature".

Thus, the Russian concept of "privacy, personal and family secrets" correlates with the American concept of "confidentiality" or "privacy", as described by Samuel D. Warren and Louis

[38] Federal Law № 160-FZ ." On ratification of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data", 19.12.2005. "Collection of the legislation of the Russian Federation ", 52 (1 hr.): 5573.

[39] Universal Declaration of Human Rights (US GPO 1949).

[40] The federal law No 231-FZ "On the introduction of Part Four of the Civil Code of the Russian Federation" of 18.12.2006 "Rossiyskaya Gazeta" No 289, 22.12.2006.

[41] *The decision of the* Constitutional Court of the Russian Federation (28 June 2012 No 1253-O it refused "To accept for consideration the complaint of the citizen Suprun Mikhail Nikolaevich about a violation of his constitutional rights in Article 137 of the Criminal Code of the Russian Federation").

[42] Criminal Code of Russian Federation. Available from https://web.archive.org/web/20150301191204/http://www.russian-criminal-code.com:80/. [Accessed 16 February 2017].

[43] Civil Code of Russian Federation // "Rossiyskaya Gazeta", No 238–239, 08.12.1994.

[44] Gonza'lez Fuster G, Gutwirth S, "Opening up personal data protection: A conceptual controversy" (2013) 29 Computer law and Security review 531.

D. Brandeis in The Right to Privacy.[45] Similarly, in Russia privacy is primarily understood as *"the right to be left alone, the right to secrecy, or the right to conceal any information from others"* including by means of stealth. The famous Russian lawyer Boris Topornin defines personal privacy as an *"individual's right to determine his behaviour in the community, to decide whom he can trust with how much information, and to demand from third parties these rights."*[46]

Government law enforcement agencies do have limited rights to access personal information, such as private communications, when doing so directly relates to protecting the security of the state and/or its citizens, for instance, to prevent crime or terrorist attacks. These rights are, nevertheless, limited: Article 13 of the Criminal Procedure Code of the Russian Federation stipulates that:

> "monitoring and recording of telephone and other conversations, obtain information about the connections between subscribers and (or) subscriber units can only be made on the basis of a court decision."[47]

The authors of this paper believe that a person's private information can be divided into that which he does not trust sharing with anyone and that which he is willing to share with a trusted group of people, defined by the person himself or the law.

As commentators have noted, in Russian law № 152:

> "a literal application of this provision to the concept of 'personal data' can refer to a wide range of information. In particular, there is no indication of the link between information and direct or indirect 'determinability' of a person. Accordingly, there is no clear understanding of the cases involving collecting information and processing information that will relate to privacy and public life".[48]

In 2015, Roskomnadzor published a report on the 2014 activities of the Authorized Body for the Protection of the Rights of Subjects of Personal Data. This report states that:

> "if the collection of data is necessary and [the data collected] sufficient for identification of the person, such data must be considered as personal data, even if it does not include data from identity documents. However, information cannot be considered as personal data if it does not allow identification of the individual without additional information. Such an approach should take into account the balance of interests of all participants in the relationships".[49]

The report also pointed out that the law has no clear position on the question of what kind of information is considered personal data and what is not. The authors of the report observe that this situation is related to the formal definition of personal data and identity, and conclude that a less broad definition of personal data is difficult to formulate.

For example, members of the National Institute of Standards and Technology, Big Data Public Working Group (NBD-PWG), Security and Privacy Subgroup, Information Technology Laboratory reported that "privacy-preserving mechanisms are needed for Big Data, such as for Personal Identifiable Information (PII). Because there may be disparate, potentially unanticipated processing steps between the data owner, provider, and data consumer, the privacy and integrity of data coming from end points should be protected at every stage. End-to-end information assurance practices for Big Data are not dissimilar from other systems, but must be designed on a larger scale".[50]

In summary, for the purposes of this paper, we define personal data as any information on the basis of which it is possible to determine the identity of the person, including information relating to his privacy.

2.4. *Principles behind the legal regulatory system protecting personal data in the Russian Federation*

2.4.1. *Personal data safety in Big Data technologies: the principle of legality or practice*

Is it possible for Russian companies to implement the principles of protection for personal data processed using Big Data technology? The essential principles of personal data are defined in the provisions of Article 5 of Federal Law № 152. This law does not refer to any particular form of technology but rather sets out certain principles in the collection and processing of all personal data. However, when it comes to Big Data, implementing of these principles is very difficult because combining sets of anonymised data can enable the user to identify individuals, a problem which applies in all countries using such databases. The European Data Protection Supervisor (EDPS) writes that *"in today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing"*.[51] Companies have repeatedly discussed this problem, as failure to meet regulatory requirements can result in administrative sanctions for non-compliancy.[52]

Article 13.11 of the Administrative Code defines the responsibility for a violation of the statutory order on the collection, storage, use or dissemination of citizens' personal data. There is no criminal liability for offenses in Russia.

Let us consider the specifics of how these principles are implemented by Russian companies that use Big Data.

[45] Warren S D and Brandeis LD, "The Right to Privacy" (1890) 4(5) Harvard Law Review 193–220.

[46] Commentary on the Constitution. ed. Topornin B (Lawyer 1997).

[47] Criminal Procedure Code of the Russian Federation \\ "Rossiyskaya Gazeta", No 249, 22.12.2001.

[48] Federal Law "On Personal Data" (2015) *"Rossiyskaya Gazeta*.

[49] Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor) "Report on the activities of the authorised body for protection of the rights of subjects of personal data in 2014" (Roskomnadzor 2014).

[50] NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. U.S. Department of Commerce. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-4.pdf. [Accessed 27 December 2016]. p. 6–7.

[51] "Opinion 4/2015. Towards a New Digital Ethics Data, Dignity and Technology" (EDPS 2015).

[52] Big data is not completely depersonalised. Available from: http://www.vedomosti.ru/technology/articles/2016/12/13/669300-bolshie-dannie-obezlichivayutsya. [Accessed 27 December 2016].

2.4.2. *The principle of the "rule of law and justice in processing personal data"*

Russian companies are currently facing the question of how to determine whether their processing of personal data is valid from a legal point of view. Jurisprudence has linked consent to the processing of personal data and determined that any processing should have a predefined, specific and legitimate purpose.[53] Mantelero and Vaciago[54] note that the complexity of data processing and the legal language in which the consent forms are written often forces users to give such consent based only on the basis of the reputation of the company.

In order to comply with the law, according to a statement by the Supreme Court of the Russian Federation, *"the storage of personal data should be . . . for no longer than required for the purpose of processing that personal data"*.[55]

The Bank of Russia uses the exact wording specified by the Supreme Court to ensure its compliance with Federal Law № 152.[56] The Russian company Yandex tackles the problem through a confidentiality agreement in which the procedure for processing personal data, including by means of Big Data technology, is described. It further assures customers that the issue of data confidentiality is subject to the jurisdiction of Russian legislation. Yandex uses depersonalisation when processing personal data.

In 2015, Article 10.3 was added to the Federal Law "On Information, Information Technologies and Protection of Information", a section that is informally referred to in the community as the "right to be forgotten". This addition specifies that any Internet search operator aiming advertising at consumers in the Russian Federation must, upon the request of a citizen, cease sharing any information they hold about that citizen, if this information is distributed in violation of the law or it is inaccurate.

Legislators have adopted this norm, but it in no way takes into account the technological features of the Internet, whose architecture means that nothing can be reliably and permanently removed. Thus, information can be recovered by Big Data technology and an exact description of the person who took certain actions can still be obtained via the Internet. Thus, this legislation does not work from either a technological or a legalistic point of view.

The new article includes legal proceedings under information legislation, giving users the right to contact the site administrator about the removal of inappropriate or inaccurate personal information from search engines, or refer the issue to Roskomnadzor. The law also allows complainants to initiate legal proceedings for a number of violations.

At the same time, well before the adoption of "the right to be forgotten" Roskomnadzor already had well-defined methods for personal data protection and the removal of personal information from the Internet. These methods were based on the rules governing industry self-regulation mechanisms, applying both judicial and non-judicial procedures. Roskomnadzor proposed a methodology of depersonalisation of personal data, including the methods and procedures of depersonalisation. These methods include: a method of introducing ID.[57]

This method replaces some personal data with ID and the creation of a reference table corresponding to the ID. The method divides the personal data array into several subsets and stores these subsets separately. The mixing method is a permutation of individual values or the groups of attributed values of personal data in the personal data array.

Roskomnadzor[58] has also determined violations by the operator of a registry of the rights of personal data subjects with the hosting provider in the following cases: notice to the hosting provider on the violation of personal data in the field of legislation; notice to the operator on deleting information from the registry, a domain name and (or) pages of sites in the Internet, or network address; obtaining from the ISP hosting information which is necessary for the organisation of cooperation between the operator and the hosting provider, in the framework of maintaining the register.

This method determines the form of the notification; the management of registry; the rights and obligations of the operator registry and hosting provider; the notification of processing procedure; the procedure for obtaining access to the information contained in the register.

Thus, it can be argued that the creation of a separate law enshrining the "right to be forgotten" in Russia is excessive, since this right can be regarded as a special case of the right to privacy and data protection, in which Russian domestic law already complies with the main international instruments.

This opinion is shared by A. Savelyev, who points out that during the discussion of the wording, the "right to be forgotten" lost its independent status, becoming an integral part of the more general right to personal data protection. In this context:

> "the invention of the legislators of some new rights or entitlements as part of the existing rights of subjects of personal data . . . may be considered rather as an indicator of the crisis legislation on personal data under the conditions of modern telecommunication and information technology, rather than as an indicator of its development."[59]

[53] Decree of the Federal Arbitration Court of the West Siberian District from 03.20.2013. Case No A27-13226/2012.

[54] Mantelero A and Vaciago G, "Data Protection in a Big Data Society. Ideas for a Future Regulation" (2015) 15 Digital Investigation 104.

[55] *The decision No APL14-583* (Board of Appeals of The Supreme Court of the Russian Federation).

[56] Russian Standard of Russian Bank STO BR IBBS-1.2-2014 "Information security organizations the Russian banking system. Methods of assessing the conformity of the information security organizations of the banking system of the Russian Federation, the requirements of STO BR IBBS-1.0-2014". Adopted and put into effect the order of the Bank of Russia of 17 May 2014 No. R-399.

[57] Guidelines of Roskomnadzor of 5 September 2013 No 996 on the application "Order of Roskomnadzor 'On Approval of the requirements and methods of depersonalisation of personal data' ", approved by Roskomnadzor December 13, 2013.

[58] Order of Roskomnadzor "On the violations of the operator of a registry of the rights of personal data subjects with a hosting provider", 22 July, 2015 No 84. Available from: http://www.pravo.gov.ru.18.08.2015. [Accessed 16 February 2017].

[59] Savelyev A, E-commerce in Russia and abroad: legal regulation (Statut 2014).

These changes to Russian legislation have led to legal uncertainty regarding the authority of Roskomnadzor to give binding instructions to operators or the subjects of personal data and to hold them accountable in the execution of Federal Law № 152, because search operators do not fall under the definition of a personal data operator.[60]

2.4.3. *The principle of the achievement of specific and lawful objectives*

The law (Parts 2 & 4 Art. 5 Federal law № 152) states that the processing of personal data should be limited to the achievement of predefined, specific, lawful objectives. Only personal data collected for the purposes of this processing may be used.

One problem with the application of this principle in banking is reflected in research by CNews Analytics, which notes that banks use Big Data technology:

> "for pre-scoring customers on the basis of data from social networks, search histories and the websites visited by customers. A number of banks focus on the development of a corporate data warehouse, improving the quality of information about customers and products. At the next stage, banks move from the effective use of available customer information to obtaining an all-encompassing vision of the client for personalizing services".[61]

One way to solve this problem for Russian companies is via a confidentiality agreement between the operator and the person (the subject of personal data). Such an agreement might explain that Big Data analysis will only be used on personal data supplied by clients, and that the bank will not process data obtained from third parties. However, we must understand that such an agreement does not solve the problem, because Big Data sets may contain any information, including information about individuals who are not customers of the bank. Therefore, it is impossible to analyse the information about the bank's clients, without analysing the information about third parties.

There are a number of aspects in the management and security of personal data by companies that process it using Big Data tools to be taken into account: (i) before processing begins, the operator is obliged to notify the personal data subject of the specific processing goals; (ii) there is no clear technical or regulatory definition on the basis of which the data handler can identify personal data among the processed information; and (iii) if there is personal information in the dataset then the person processing it is automatically defined as a personal data operator viz. (under Federal Law "On Personal Data", a personal data operator is defined not only as the public authority, municipal authority or legal entity but also any individual within that organisation who handles personal data).

The processing of personal data includes the collection of information. Term of the "collection of information" has become an obstacle in Russian practice, because in the law it is not disclosed. The Ministry of Communications and Mass Communications states that *"the collection of data includes the documented procedure of obtaining personal data by the operator from a person for further processing in accordance with the stated purposes of collection"*.[62]

However, as the US Department of Commerce observes: "Because of the broad collection and range of uses of big data, consent for collection is much less likely to be sufficient and should be augmented with technical and legal controls to provide auditability and accountability for use".[63] In other words, the fate of personal information destined for analysis by Big Data is difficult to define at the outset, making it impossible to obtain consent from the subject for all possible future uses. Instead, the individual should have the legal right to track what happens to their data.[64]

2.4.4. *The impossibility of complying on "content" and "scope" in the case of merged datasets*

By definition, Big Data processing involves the integration or merging of various datasets. The merging of databases presents a number of obstacles to compliance with the law. Provisions demanded by Federal law № 152 (specifically, Parts 3 and 5 of Art. 5) – namely that the purposes to which data will be put must be declared when it is collected and that the collection of excessive information in relation to the stated objectives is prohibited – are easily undermined when datasets are merged. Apart from the above-mentioned challenges in obtaining permission from data subjects for their data to be used in ways not imagined at the point of collection, the law is undermined by the ever-increasing volume of potentially personal data currently being accumulated from sources such as social media, Internet browsing history and other web-related activity. In this regard, the legal requirement to collect no more data than is required for a specific objective is rendered obsolete, or at least impossible to apply in practice, most particularly where large datasets are merged.

A further problem occurs when personal data protection has supposedly been ensured by the anonymisation of data subjects. As the EDPS has noted: *"Big data should be considered personal even where anonymization techniques have been applied: it is becoming ever easier to infer a person's identity by combining*

[60] Dupan A et al. The new paradigm of protection and personal data management in the Russian Federation and foreign countries in terms of data processing systems on the Internet (The Publishing House of the Higher School of Economics 2016).

[61] Kiryanova A, "Bolshiye dannyie ne stali meinstrimom v rossiyskikh bankakh [Big Data will not become mainstream in Russian banks]" (CNews.ru 2015). Available from: http://www.cnews.ru/news/top/bolshie_dannye_ne_stali_mejnstrimom. [Accessed 18 June 2016].

[62] Letter of Ministry of Communications and Mass Communications of the Russian Federation, March 10, 2016 No. P11-1-4201 "On clarifying the norms of the federal law".

[63] NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. U.S. Department of Commerce. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-4.pdf. [Accessed 27 December 2016]. p.7.

[64] Details of how the EU revised the rules and definitions used in the organisation of relations in the electronic environment to protect privacy in the face of the challenges presented by Big Data can be seen here: Article 29 Working Party (European Parliament and of the Council 1995). Available from: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. [Accessed 1 June 2016].

allegedly 'anonymous' data with other datasets including publicly available information, for example, on social media".[65]

A final consideration is that consolidating information in one place presents increased risks in terms of data security. Nir Kshetri observes that a *"higher volume and concentration of data makes a more appealing target for hackers. Moreover, a higher data volume increases the probability that the data files and documents may contain inherently valuable and sensitive information".*[66]

2.4.5. *The principle of ensuring the accuracy, adequacy and relevance of personal data*

Part 6 of Art. 5 of Federal Law № 152 states that the accuracy, sufficiency and relevance of personal data must be ensured. The operator must make the necessary arrangements to ensure accuracy and to remove or specify incomplete or inaccurate data.

The management and security of personal data is also regulated in Governmental Decree № 1119,[67] which states that:

> "under threats, personal data should be understood as a set of conditions and factors that create an actual risk of unauthorized, including accidental, access to personal data when they are processed in an information system. The result of threats may be the destruction, modification, blocking, copying, provision or distribution of personal data as well as other illegal actions."

The Decree requires the maintenance of four levels of security for personal data that depend on various combinations of the following parameters:

- The categories of personal data being processed (special,[68] biometric,[69] popular,[70] other).
- The nature of the relationship between the operator and the subject of personal data (e.g. whether the operator is an employee). At the same time, an individual directly or indirectly defined or identified based on the information provided should be referred to as a personal data subject. Thus, at the beginning of the personal data processing a legal relationship arises, where the data owner is defined as a "subject" and the other side becomes an "operator".
- The number of subjects whose data are processed (less or more than 100,000);
- The nature of potential threats to the security of the system on which data is processed, such as undeclared (undocumented) possibilities in the system software used for handling personal data, or in its application.

The Ministry of Communications and Mass Communications specifies personal data should be stored in a form that does not allow individual subjects to be identified, and that it should be held for no longer than required to fulfil the processing objectives. Processed personal data should be destroyed after the objectives of processing have been achieved or if the processing is no longer required, and if not otherwise stipulated by federal law.[71]

To meet this requirement, both the Pension Fund and the Ministry of Taxes and Fees use the personal insurance number created by the compulsory state pension insurance system (SNILS), binding it to the subject's name, patronymic and surname. They then limit employees' levels of access to information through a controlled data access system. Binding SNILS to personal data is an example of the transformation of information from personalised to depersonalised.

Under certain circumstances, such as the transfer of information via the Internet, the protection of personal data can only be ensured with encryption. Cryptographic protocols are used by SberBank, one of the largest banks of the Russian Federation, as well as the tax authorities and the Pension Fund, when sending personal information via the Internet.

The personal data operator, having received personal information through Big Data analysis, should process the data using only FSTEC-certificated technology and methods of protection. FSTEC is the supervisory and monitoring body and it can impose sanctions if it finds violations of the Federal Law "On Personal Data".[72] Failure to comply can lead to the company being blocked from registering as a Big Data operator. In connection with difficulties in the legal regulation of personal data that falls into the category of Big Data, and in the absence of a common approach to the protection of personal data, the head of Roskomnadzor, Alexander Zharov has said that in future a law should be adopted on "Big Data". He also noted that we must think about the national operator of "Big Data", which will work under the terms of a public–private partnership. In particular, it is necessary to determine the risks that are arising in connection with the transfer of large information, information that can be collected by operator, and conditions of transfer information, including abroad.[73]

3. Discussion

Single datasets holding personal data tend to include a number of safeguards that ensure the protection of data subjects' iden-

[65] Towards a new digital ethics. Data, dignity and technology (EDPS 2015).

[66] Savelyev A, E-commerce in Russia and abroad: legal regulation (Statut 2014).

[67] Government Decree of Russian Federation No 1119 "On approval of requirements for the protection of personal data at their processing in information systems of personal data" "Rossiyskaya Gazeta", No 256, 07.11.2012.

[68] Includes information on race, ethnic origin, political opinions, religious or philosophical beliefs, health, sexual life.

[69] Includes the information specifying the physiological and biological characteristics of a person.

[70] Reference and address books. The public sources of personal data with the written consent of a personal data subject can include his/her name, surname, patronymic, date and place of birth, address, subscriber number, information on the profession and other personal data reported by the personal data subject.

[71] Letter from the Ministry of Communications and Mass Communications of the Russian Federation, March 10, 2016 No. P11-1-4201 "On clarifying the norms of the federal law".

[72] Government Decree of Russian Federation 01.11.2012 No 1119 "On approval of requirements for the protection of personal data at their processing in information systems of personal data" "Rossiyskaya Gazeta" No 256, 07.11.2012.

[73] Roskomnadzor wants to create a national operator of Big Data. Available from: http://www.media-pravo.info/news/175. [Accessed 16 February 2017].

tities, but their combination creates an ambiguous situation in the realm of legal regulation. In this regard, it is difficult to say whether current regulations governing the management of personal data in the Russian Federation are sufficient when Big Data technologies are applied.

The Russian model for protecting personal data in Big Data processing is based on depersonalisation of subjects. However, in practice this is insufficient because it is possible to apply tools that can identify an individual by comparing data from various sources. Today, it is impossible to anonymise data completely, because of the proliferation tools enabling re-identification. MIT Research found that *"just four fairly vague pieces of information – the dates and locations of four purchases – are enough to identify 90% of the people in a data set recording three months of credit card transactions by 1.1 million users"*.[74]

R. Ameline[75] observes that the requirements laid out for the integration of government information systems and government databases in the "Strategy for Information Society Development in the Russian Federation"[76] *"may eventually lead to an invasion of privacy because such mergers will give rise to Big Data"*.

This substantiates the view that ". . .the ongoing expansion of state control through the creation of a universal electronic identification card for Russian citizens may lead to the violation of this principle, as the universal electronic cards include various pieces of personal information, such as identification data, information about compulsory health insurance and pension data, and furthermore have the potential to carry other information. . .".[77]

The importance of this principle is considered to be so great that a prohibition against combining a variety of personal information was reflected in the Governmental Decree *"On the Approval of personal data processing features, carried out without the use of automated equipment"*, which states that *"when securing personal data on physical media, personal data not required for processing purposes may not be stored on a single tangible medium."*

Russian companies still do not have any best practice guidelines on the practical implementation of this principle. The concern is not just that Big Data increases the risk of data breaches; it increases the range of possible risks. Data theft remains as much a risk with Big Data as with other forms of personal data storage due to the impossibility of creating a 100% safe and reliable security system, but the sheer scale of Big Data sets makes them a more attractive target to hackers. This aside, Big Data also poses new challenges which current legislation and protections are ill equipped to deal with. The three core legislative strategies for ensuring privacy – individual "notice and consent", the possibility of non-participation and the anonymisation of data – have lost much of their effectiveness. We have already discussed the difficulty in obtaining informed consent from data subjects for as-yet unimagined uses of their information. Withdrawal of consent is difficult to apply if an individual's data cannot easily be separated from a large volume of anonymised data. Meanwhile, as discussed above, individual data subjects can be identified through the combination and analysis of multiple databases. And finally, existing legislation is difficult to implement, despite there being well-organised law enforcement and regulatory body structures in place, either because it is too weak, or because it is not applicable to the realities of Big Data. Changing this situation requires new solutions.

The Committee of Ministers of the Council of Europe CM/Rec (2010) 13[78] sums up some of the key issues pertaining to data privacy and consent which arise with the processing of Big Data sets for the purposes of profiling users, noting that *"data . . . are processed by calculation, comparison and statistical correlation software, with the aim of producing profiles that could be used in many ways for different purposes and uses by matching the data of several individuals"*. The report goes on to note that *"profiles, when they are attributed to a data subject, make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which she or he can reasonably presume to be known to the controller"*.

The Committee's recommendations aim to protect the rights of data subjects in situations where mass quantities of data are processed, and to avoid situations where profiling gives rise to negative decisions, stigmatisation or discrimination. The recommendations include ensuring data subjects are informed that their data will be used for profiling, the purposes of that profiling, what categories of personal data will be used, how long it will be kept for, and the existence of appropriate safeguards, including the right to withdraw consent. The committee also recommends that even in cases where personal data are not collected directly from subjects, the controller should nevertheless inform subjects of the above details.

Russian law stipulates that: In the case of the achievement of the objective of the processing of personal data, the operator is obliged to stop processing personal data or to provide its termination and to destroy personal data, no later than 30 days from the date of the achievement of the objective of the processing." In cases where it is impossible to destroy the personal data during the specified timeframe, the operator must block access to it and ensure its destruction no more than 6 months later (Part 4 Art. 23 Federal Law № 152 "On Personal Data").

According to Part 5 of Art. 18 of Federal Law №152 "the operator collecting personal data of Russian Federation citizens is obliged to provide recording, systematization, accumulation, storage, clarifications (updates, modifications) and extraction of the personal data from databases located on the territory of the Russian Federation, except as specified in paragraphs 2, 3, 4 and 8, Part 1 of Art. 6 of Federal law №152."

[74] Hardesty L | MIT News Office, "Privacy Challenges" (MIT News 29 January 2015). Available from: http://news.mit.edu/2015/identify-from-credit-card-metadata-0129. [Accessed 11 June 2016].

[75] Ameline RV, "On the legal principles of the development of the state AIS that process personal data" [2009] Information Law 26.

[76] Strategy for Information Society Development in the Russian Federation, "On the integration of information systems of state and government databases to ensure effective inter-agency and inter-regional exchange of information and interaction between civil society and business with public authorities". 7. 2008 No. Pr-212.

[77] Government Resolution of Russian Federation. (2011). "On the technical requirements for the universal electronic card and electronic applications to the federal", 24 March 2011, No. 208.

[78] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Available from: https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf. [Accessed 21 December 2016].

One complexity in implementing this requirement arises from the question of how the citizenship of data subjects is defined. This issue is not regulated in any existing laws, although the Ministry of Communications and Mass Communications states that current legislation provides *"an opportunity for the operator of personal data to decide this question based on the specifics of its activities. If the operator does not resolve this issue, then Part 5 Art. 18 will be applied to all personal data collected on the territory of the Russian Federation."*[79]

The situation regarding the management and security of personal data used in Big Data analysis is ambiguous. In Russia, legal management and security systems for personal data consist of federal laws, subordinate legislation and a significant number of regulations made by executive authorities that are methodological – they all define a mandatory set of operator actions to protect personal data.

In the Russian legal system, perpetrators of illegal actions regarding family secrets, the confidentiality of correspondence, telephone conversations, postal, telegraph or other messages face criminal liability. However, only administrative liability is stipulated for the violation of laws on the collection, storage, use or dissemination of personal data. The vagueness of the concept of "personal data" leads to an operator of personal data being defined as everyone who has access to and/or works with personal data.

In the face of these ambiguities, companies are left to form their own practices of compliance with the legislative requirements for personal data protection when handling Big Data. Thus, actions that should be defined based on a system of legal regulation are in practice being applied ad hoc by individual companies, based on their interpretation of a law that is at best vague.

Of course, there is a significant difference between the processing of information in order to ensure the safety of the state or the public, and processing for commercial purposes. However, if the risk of violating the principle of legality is significant, then these types of threats and possible methods of dealing with them should be clearly defined.

FSTEC defines basic types of security threats to personal data according to:

- the type of protected information;
- the source of potential threats;
- the type of information systems used for processing;
- the process by which threats are realised;
- the type of unauthorised acts that are carried out with personal data;
- the nature of the vulnerability;
- the type of impact on the object.[80]

Despite the existing risks, Russia still has no normative document in which methods of risk prevention have been described.

However, we can say that Russia's approach provides extensive opportunities to prevent offences relating to misuse of personal data, either via Roskomnadzor blocking or demanding removal of infringements on websites by the disseminating organisation/individual, or by the Attorney General. The latter can order redress within the framework of civil liability and administrative liability (Art. 15.5 of the Federal Law "On Information" and Art. 13.31 of the Administrative Code).

Nevertheless, the sharing of data protection roles between state authorities has pros and cons. Practice shows that the creation of a single authority overseeing personal data protection – as is the case, for example, in Singapore[81] – allows the state to achieve success swiftly and efficiently compared to situations where oversight of various aspects of data protection is divided between several organisations.

One major problem is that violations in the handling of personal data are difficult to prove. Another is that determining the level of injury (e.g. damage to property or the amount of non-pecuniary damage) is always at the discretion of the court. There is a strong need to introduce special civil liability for personal data violations that would allow the complainant to claim compensation. A civil liability framework, which compensates the victim for violations, will enable citizens to understand the value of their personal data and the importance of monitoring how it is being processed. A policy, which encourages citizens to be active in relation to managing and guarding their personal data, would also increase companies' focus on compliance with data protection legislation.

To solve this problem, it is necessary to update the Civil Code to include the possibility of compensation for violations of personal data handling (by analogy with Article 1301 of the Civil Code. This establishes that in cases of infringement of the exclusive right of an author or of other rights holders, applicants are entitled to demand from the infringer compensation for losses from 10,000 to 5,000,000 rubles). Since the possible range of compensation for personal data infringements that can be collected would be set in advance (for example, from 10,000 to 1,000,000 rubles per violation), this would simplify the foreclosure procedure.

In view of the above, it seems appropriate to complement Chapter 4 of the Federal Law №152-FZ with a new article that establishes the obligation of the operator to a) notify the authorised body about all incidents of personal data infringement by defining the incident (any unauthorised provision – including access – or dissemination of personal data) and b) in certain cases, notify the personal data subject.

The following table summarises the above discussion, laying out the specific current challenges in data protection, showing how existing legislation covers the problem, and suggesting what further legislation is required, if any, to solve the problem

[79] The official website of Ministry of Communications of Russia. Processing and storage of personal data in the Russian Federation which were changed on 1 September 2015. Available from: http://minsvyaz.ru/ru/personaldata/#1438174940445. [Accessed 25 December 2016].

[80] Federal Service for Customs and Export Control (2008). The basic model of threats of personal data security at their processing within the information systems of personal data is approved. FSTEC RF 15.02.

[81] Warren B, The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform (2013) 29 Computer Law & Security Review. doi: 10.1016/j.clsr.2013.07.010.

The essence of the problem	The basis of the problem	Existing legal methods of solving problems in the Russian Federation	Suggested legal methods of solving problems
Cross-border transfer of personal data.	Data centres may be located outside the territory of a state and therefore outside its jurisdiction	Before any transboundary transfer of personal data, the operator must be sure that the foreign state, on territory of which the personal data will transfer, provides adequate protection of the rights of subjects of personal data. Personal data must be stored on servers located in Russia, according to Federal Law № 152 "On Personal Data".	
Ambiguity over whether anonymised data is personal data or not.	Through the use of Big Data technology, it is often possible to identify anonymised data subjects through the combination of multiple databases, thus effectively changing the status of the dataset to 'personal data'.		It is necessary to legally determine the status of the Big Data operator, and define the responsibilities of any legal entity involved in processing Big Data.
Big Data processing can make it impossible to comply with the legal requirement to tell the data subject how their data will be used at the point of collection, as future uses cannot be anticipated.	The combination of datasets for Big Data analysis can mean that personal data subjects lose control of how, by whom, and for what purposes their data will be used.		Any legal entity using Big Data should be required to implement procedures to ensure all data relating to citizens is given the same protections as personal data, even if it is anonymised, and to ensure that any anonymous data they handle remains anonymous.
Ensuring privacy and security of identity on the Internet, when the provided Internet service includes applying to Big Data technology.	Lack of unified security solutions (e.g. authorisation, authentication, and access control) in the field of Big Data.	Procedures for identification and authentication of access subjects and objects shall ensure the assignment of a unique ID access code (identifier) to the subjects and objects, a comparison between IDs which have been brought by the subject (object) and a plurality of assigned identifiers; as well as checking the belonging of an access ID (authenticity conformity) to the access subject (object).[a]	The Federal Law "On information" must be supplemented with a set of rules aimed at forming a space of trust on the Internet. The space of trust includes the creation of Trust Services, which allow ensuring the reliability of services provided in the Internet. It is necessary to develop standards for the provision of services in the Internet, in strict accordance with the following: 1) requirements for the activities of persons providing such services; 2) standards; 3) requirements of the current legislation; 4) the current level of technology development (including cryptographic algorithms).
The lack of legal status for electronic agreements as contracts for services with the use of Big Data.	On-line service agreements have no proper legal force because there is no corresponding legislation defining permissible use of electronic documents in civil law. Russian law defines the status of an "electronic document", but only recognises its validity in relation the corresponding paper document.	According to Law № 63-FZ "On electronic signatures",[b] information in electronic form may be recognised as equivalent to paper documents bearing a handwritten signature only if signed using an electronic signature.	The Law "On the electronic document" must be updated to recognise the status of an electronic document and the details held therein as formal document submitted in electronic form.

(*continued on next page*)

The essence of the problem	The basis of the problem	Existing legal methods of solving problems in the Russian Federation	Suggested legal methods of solving problems
Combined databases that contain personal data may be used for analyses that are incompatible with the original stated purposes of data collection.	When the owner of a database containing personal information forms an agreement for that dataset to be combined with other datasets for Big Data analysis, there is a risk that their original agreement with individual data subjects over how their information will be used not taken into account by the Big Data operator and will be lost in the database restructuring process.		Big Data operators must be required to guarantee the security of personal data under the same conditions agreed between the personal data subject and the original data operator.
Data subject may lose the ability to monitor what is happening to their data and how it is being used.	When databases are combined for Big Data analysis, data subjects may lose the ability to monitor whether the operator is complying with the conditions set out for processing personal data.		It is necessary to establish the requirement that if personal data must be transmitted in a combined database, it must be anonymised first. There is also a need to develop a basis for a pre-judicial form of dispute resolution in such cases. New legislation is required to ensure subjects retain the right to withdraw permission for participation, even when subjects' data have been passed on in the anonymised form for use in a Big Data set.
Big Data makes a bigger target for data theft.	The security of databases can be compromised by flaws in the IT system, through hacking, or removal on physical medium by somebody with access to the data. Depersonalisation is not always an effective protection, as it can be potentially be reversed by analysing various pieces of information about the same individual.	Order №21 FSTEC sets out regulations determining the appropriate security requirements for data operators' software environment, specifying that only FSS or FSTEC-approved software can be used and that no other types of software should be installed in systems handling personal data.	As mentioned above, there is a need for legislation defining the responsibilities and authority of Big Data operators, which will make it possible to determine the circle of decision-makers involved in the security of information processed. At present time, in addition, operators of Big Data should be obliged to locate their data centres in Russia. When collecting personal data, a personal data operator shall be obliged to ensure recording, systematisation, accumulation, storage, clarification (updating, modification), extraction of the Russian Federation citizens' personal data with the use of databases located in the territory of the Russian Federation. However, there are no such requirements for Big Data operators. This requirement may result in the development of requirements for the certification of a Big Data technology.

(*continued on next page*)

The essence of the problem	The basis of the problem	Existing legal methods of solving problems in the Russian Federation	Suggested legal methods of solving problems
The problem of technological obsolescence of the mechanisms for personal data security with the development of collection, storage and processing technologies.	There is a problem of determining specific criteria, upon the presence or absence of which we can conclude on personal data security. At the same time, the simple use of processes and technologies is not enough. The simple use of a technology is not enough for ensuring information security, because security policy should define specific security criteria, but should not regulate the use of technological procedures.		The policy and management should not introduce specific technological solutions, but they should formulate a set of planned results. For example, the prevention of risks and the definition of responsibilities of the parties could be resolved upon the use of ISO international standards by personal data operators and other private companies
The gap between technological and legal approaches to the protection of personal data	The absence of a common approach to regulation between lawyers and technology professionals. Backlog of technological developments demanding new legal approaches		New research into the organisational, technical and social protection methods for personal data security must be carried out from a legal point of view. There is a need to develop and to implement the Russian Federation Law "On the security of the Russian Federation's critical information infrastructure."

[a] Order № 21 of the Federal Service for Customs and Export Control (2013a). On approval of the composition and content of organizational and technical measures to ensure the security of personal data being processed in information systems. FSTEC RF 18.02.
[b] Federal Law 06.04.2011 No 63-FZ "On Electronic Signature" (2011) *"Rossiyskaya Gazeta"*.

4. Conclusions

The changes to data handling and usage presented by Big Data demand new legislation, such that the principles behind existing data privacy laws can be upheld in the context of potential new threats to privacy and potential for abuse posed by Big Data technology. To be effective, these changes must include clearer liability and more stringent sanctions in the case of infringements.

It is necessary to develop a law on "Big Data", in which we must identify and define a risks and threats, and we must the desired level of protection required in the processing of information may be requested technology Big data.

In this law we should define the algorithms of separation a data types, in process their handling by Big Data and the procedures of processing such information.

In this law, we should define the term "national operator of 'Big Data' ", which has to work on the type of public–private partnership. Despite the existence of Russian legislation on protection of personal data, a number of amendments are required to protect data subjects in the face of Big Data technology.

Roskomnadzor's powers as control and oversight body, as established by Art. 23 of Federal Law № 152, relate only to the interaction between personal data operators and their compliance with regulatory powers; they are insufficient to implement the protection of the rights of personal data subjects, and do not match the scope of powers held by public authorities in other countries (e.g. within the EU). Thus, persons who do not fall under the definition of personal data operators – for example, operators of search engines, or those analysing Big Data sets which do not include personal data, or include anonymised data – are not subject to audits or enforcement by Roskomnadzor. In light of this, it is necessary to modify the concept of "personal data" so that the laws governing the handling of personal data also apply to operators processing, for example, anonymised Big Data sets that can potentially be used retrospectively to identify the individuals involved. There is also a pressing need to update Roscomnadzor's powers to enforce these new rules among entities not currently covered under existing personal data protection laws (operators of search engines, operators of Glonas and GPS navigation, etc.).

The basic principles of regulation regarding operators processing information that is not currently defined as personal data, but which can nevertheless be used to retrospectively identify and create profiles of individual subjects, can be formulated on the basis of the aforementioned provisions of the Recommendation of the Committee of Ministers of the Council of Europe "The protection of individuals with regard to automatic processing of personal data in the context of profiling".[82]

[82] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00. [Accessed 11 June 2016].

These involve establishing special rules for operators engaged in profiling based on information gleaned about individual users from the Internet. In the case of the Russian Federation, these rules should form an additional article to the Federal Law "On Information, Information Technologies and Protection of Information".

To implement the recommendations, it would be necessary to:

1) Add the concept of profiling.
2) Determine if the operator of the information system, service provider or hosting provider collects data on its users for the purposes of profiling. If so, then data subjects must be provided with the following information before the data is collected:
   – That the data will be used for profiling
   – The purposes of profiling
   – Categories of personal data that can be obtained as a result of profiling
   – Information on the operator of the information system, service provider or hosting provider and (or) his representative
   – Guarantees of data security
   – The categories of persons, authorities and other entities that will be able to obtain the personal data because of profiling
   – The duration of storage
   – The expected consequences of profiling the data subject
   – The possibility or impossibility of abandoning the collection and processing of data for profiling without sacrificing the quality of the relevant service
3) Establish that the operator of the information system, service provider or hosting provider does not have the right to restrict access or degrade the quality of service provided to the user, should they refuse to allow their data to be used for profiling (with the exception of cases where such collection, processing or storage of data is necessary for the provision of the service and has been performed in accordance with law).

It is also necessary to supplement Federal Law № 152-FZ with a new article establishing the duty of the data controller to notify Roskomnadzor of all incidents involving violations of personal data and to help the relevant authorities inform individuals whose data has been misused about the nature of the violation. Due to the lack of clarity in existing law, it is necessary to define an "incident" as any unauthorised granting of access to or dissemination of personal data.

In some foreign countries (such as the USA and the UK), exacting measures of responsibility have already been established for violations of confidentiality of personal data. The Russian Federation does stipulate administrative punishment for violations in the handling of personal data, such as the illegal collection, storage, use or dissemination of information about citizens (Article 13.11). These actions entail issuing a warning or imposing an administrative fine: from 300 to 500 rubles for individual citizens; from 500 to 1000 rubles for officials; and from 5000 to 10,000 rubles for legal entities. However, criminal liability for such violations has not been established (with the exception of the illegal use of personal data for entering information into the Unified State Register of Legal Entities).

Moreover, the existing fines do not create incentives for companies to take all possible measures to protect personal data, especially in the use of Big Data to create personalised advertising, as the risks are outweighed by potential profits.

To resolve these inconsistencies, we recommend the following:

1) Update existing laws to take into account new possibilities for data breaches presented by Big Data technology.
2) Clarify legal definitions of 'personal data' to include anonymised records that may, in future, be used in combination to identify individual data subjects.
3) Provide clear 'best practice' guidelines to help companies handling Big Data sets comply with their legal duties.
4) Increase the level of administrative responsibility for violations in the field of personal data.
5) Establish criminal liability for violations of personal data protection legislation, with sanctions occurring immediately after the violation and not linked to the size of the damage caused.
6) Improve the model of civil liability for violations in the field of personal data.
7) Introduce legislation that requires the operator to inform the relevant bodies about leaks of personal data.

For example, the prevention of risks and the definition of responsibilities of the parties could be resolved by use of the ISO international standards for personal data operators and other private companies, which could have a number of positive effects. Firstly, the widely used standards involve a wide range of stakeholders, which contribute to the strengthening of confidence in the adequacy, equity and viability of such rules. Needless to say, the topic of trust and fair treatment is now a matter of paramount importance. Secondly, when most governments around the world use the standards, as is the case with many ISO standards, then the result is strengthened consistency, predictability and legal certainty. Although the standards themselves are not regulatory documents, after turning in a contract these requirements become binding. In any case, they set the standard of reasonable precautions used in private litigation.

The principles upon which existing data protection laws are built remain sound: the law aims to protect citizens' rights to a private life and ensure their personal details remain confidential. However, the rapid accumulation of massive datasets containing information on private citizens and the ever-increasing power of Big Data tools to identify specific individuals from combined anonymised records have left the law unable to cope with these new threats to privacy. Companies are confused about compliance, about what does and does not count as personal data, and with whom responsibility over data protection lies when dealing with data obtained from third parties. Without urgent amendment to existing legislation, the potential for personal data to be exploited for commercial gain or other purposes remains a serious threat to Russian citizens' constitutional right to a private life.

Acknowledgement

We thank the Russian Humanitarian Science Foundation for their assistance in the project "Comparative legal research methods of information security in the Russian Federation and EU Members (№ 16-03-00679)".

Support from the Research Program of the Faculty of Business and Management at National Research University Higher School of Economics is gratefully acknowledged.

REFERENCES

Agapov V, Pratusevich V, Yakovlev S. Obzor i otsenka perspektiv razvitiya mirovogo i rossiyskogo rynkov informatsionnykh tekhnologiy [Review and assessment of the prospects of development of world and Russian markets of information technology]. International Data Corporation; 2014.

Ameline RV. On the legal principles of the development of the state AIS that process personal data. Information Law 2009;26.

D'Acquisto G, Domingo-Ferrer J, Kikiras P, Torra V, de Montjoye Y, Bourka A. Privacy by design in big data. European Union Agency For Network and Information Security Privacy; 2015 doi:10.2824/641480.

Decree of Russian Federation Government. On approval of requirements for the protection of personal data that is processed in information systems. Collection of the legislation of the Russian Federation, 45:6257; 2012.

Dupan A. In: Titov S, Zhulin A, Zharova A, Elin V, Bikbulatov T, Bikbulatova Y, et al., editors. The new paradigm of protection and personal data management in the Russian Federation and foreign countries in terms of data processing systems on the Internet. The Publishing House of the Higher School of Economics; 2016.

Federal Law of 06.04.2011 No 63-FZ "On Electronic Signature", "Rossiyskaya Gazeta"; 2011.

Federal Security Service. Model rules of within the authority of measures for control (supervision) over compliance with the requirements established by the Russian Government to ensure the security of personal data while it processing in information systems. Approved by Federal Security Service of Russia 08.08. No. 149/7/2/6–1173; 2009.

Federal Service for Customs and Export Control. The basic model of threats of personal data security at their processing within the information systems of personal data is approved. FSTEC RF 15.02; 2008.

Federal Service for Customs and Export Control. On approval of the composition and content of organizational and technical measures to ensure the security of personal data at their processing in information systems of personal data. FSTEC RF 18.02; 2013a.

Federal Service for Customs and Export Control. On Approval of the Requirements for the Protection of the information, not the state secret contained in the state information systems. FSTEC RF 02.11; 2013b.

Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor). Report on the activities of the authorized body for protection of the rights of subjects of personal data in 2014. Roskomnadzor; 2014.

Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor). Public report 2015, Roskomnadzor 2015.

Gonza'lez Fuster G, Gutwirth S. Opening up personal data protection: a conceptual controversy. Comput Law Secur Rev 2013;29:531.

Government Decree of Russian Federation. On approval of rules of interaction of operators with the authorized state bodies, engaged in the operational-search activities, of 27.08.2005, No. 538; 2005.

Government Decree of Russian Federation. On approval of the personal data processing features, carried out without the use of automation equipment, of 15.09.2008 No. 687; 2008.

Government Decree of Russian Federation. On the Federal Service for Communications, Information Technology and Mass Communications Supervision, of 16.03.2009, No. 228; 2009.

Government Decree of Russian Federation. On approval of requirements for the protection of personal data at their processing in information systems of personal data, of 05.11.2012, No. 45; 2012.

Government Resolution of Russian Federation. On the technical requirements for the universal electronic card and electronic applications to the federal, March 24, 2011 No. 208; 2011.

Hardesty L, MIT News Office. Privacy challenges. MIT News; 2015 Available from: http://news.mit.edu/2014/mit-white-house-co-sponsor-workshop-on-big-data-privacy-0304. [Accessed 11 June 2016].

Interview with CNews, Yukhno O. Yandex: Big Data technology has helped us to increase market share; January 15, 2014. Available from: http://www.cnews.ru/articles/yandeks_tehnologii_big_data_uzhe_pomogli. [Accessed 5 June 2016].

Jones C, Hayes B. D2.4 The EU data retention directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy. Statewatch, SECILE; 2013 Available from: http://www.statewatch.org/news/2013/nov/data-retention-directive-in-europe-a-case-study.pdf. [Accessed 3 November 2016].

Kiryanova A. Bolshiye dannyie ne stali meinstrimom v rossiyskikh bankakh [Big Data will not become mainstream in Russian banks], CNews.ru; 2015. Available from: http://www.cnews.ru/news/top/bolshie_dannye_ne_stali_mejnstrimom. [Accessed 18 June 2016].

Kshetri N. Big Data's impact on privacy, security and consumer welfare. Telecomm Policy 2014;38:1134–45.

Mantelero A, Vaciago G. Data protection in a Big Data society. Ideas for a future regulation. Dig Invest 2015;15:104–9.

Ministry of Telecom and Mass Communications of the Russian Federation Report mistakes. Processing and storage of personal data in the Russian Federation will be changed from September 1. 2015; n.d. Available from: http://minsvyaz.ru/ru/personaldata/#1438174940445. [Accessed 18 June 2016].

Nadkarni A, Vesset D. Worldwide Big Data technology and services forecast; 2015. Available from: http://www.idc.com/getdoc.jsp?containerId=259532. [Accessed 1 September 2016].

Naidich A. Bolshiye dannyie: naskolko oni bolshiye? [Big Data: how big they are]. Kompyuter Press; 2012. p. 12 Available from: http://compress.ru/article.aspx?id=23469. [Accessed 1 June 2016].

National Institute of Standards and Technology and NIST, Special Publication (NIST SP) – 1500-4; 2015. Available from: https://dx.doi.org/10.6028/NIST.SP.1500-4. [Accessed 27 December 2016].

Naydenov R, Liveri D, Dupre L, Chalvatzi E, Skouloudi C. Big Data security. European Union Agency for Network and Information Security; 2015 doi:10.2824/13094.

Order of Roskomnadzor "On interaction an operator of registry a violators of the rights of personal data subjects (further operator registry) with hosting provider", 22 July, 2015 No 84. Available from: http://www.pravo.gov.ru,18.08.2015. [Accessed 16 February 2017]

Presidential Decree. Issues of the Federal Service for technical and export control. Collection of the legislation of the Russian Federation, No. 1085, 34:3541; 2004.
Savelyev A. E-commerce in Russia and abroad: legal regulation, Statut; 2014.
Savelyev A. Russia's new personal data localization regulations: a step forward or a self-imposed sanction? Comput Law Secur Rev 2016;32:doi:10.1016/j.clsr.2015.12.003.
Security Service of Russia. Methodical recommendations for personal data security by using cryptographic in processing in the information systems. Approved by Federal Security Service of Russia. 21.02.2008 No. 149/54–144; 2008.
Strategy for Information Society Development in the Russian Federation. On the integration of information systems of state and government databases to ensure effective inter-agency and inter-regional exchange of information and interaction between civil society and business with public authorities. 7. 2008 No. Pr-212.
Tadviser. 100 profiles of top Russian companies about the strategy in Big Data [Report]; 2015. Available from: http://www.tadviser.ru/index.php. [Accessed 3 June 2016].
Topornin B, editor. Commentary of the constitution. Lawyer; 1997.
Towards a new digital ethics. Data, dignity and technology, EDPS; 2015.
Warren B. The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. Comput Law Secur Rev 2013;29:doi:10.1016/j.clsr.2013.07.010.
Warren SD, Brandeis LD. The right to privacy. Harv Law Rev 1890;4(5):193–220.
Zharova A, Elin V, Dem'yanets M. Entrepreneurial activity on the Internet, Yurcompany; 2014.
Ziora ACL. The role of Big Data solutions in the management of organizations. review of selected practical examples. Procedia Comput Sci 2015;65:1006. doi:10.1016/j.procs.2015.09.059.
Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. Available from: http://www.gartner.com/newsroom/id/3114217. [Accessed 1 June 2016].
Decree of the Federal Arbitration Court of the West Siberian District from 03.20.2013. Case No. A27-13226/2012.
The decision No APL14-583, Board of Appeals of The Supreme Court of the Russian Federation.
Russian Standard of Russian Bank STO BR IBBS-1.2-2014 "Information security organizations the Russian banking system. Methods of assessing the conformity of the information security organizations of the banking system of the Russian Federation, the requirements of STO BR IBBS-1.0-2014". Adopted and put into effect the order of the Bank of Russia of 17 May 2014 No. R-399.
Roskomnadzor wants to create a national operator of Big Data. Available from: http://www.media-pravo.info/news/175. [Accessed 16 February 2017].
Appellate Decision N 33–30344, Moscow City Court.
The official website of the Ministry of Communications of Russia. Processing and storage of personal data in the Russian Federation which were changed as of September 1, 2015. Available from: http://minsvyaz.ru/ru/personaldata/#1438174940445. [Accessed 25 December 2016].
Basic directions of the state policy in the security of automated control systems of production processes critical infrastructure of the Russian Federation approved of Russian President of February 3, 2012 № 803.
RRI Opportunities in Horizon 2020 Science with and for society relevant topics in the Horizon 2020 Work Programme 2016-17. Project funded by the European Commission. Available from: https://www.hse.ru/data/2015/12/11/1133574498/RRI_opportunities_in_%20Horizon%202020_151208.pdf. [Accessed 1 September 2016].
Order Roskomnadzor from 12.08.2013 N 912 "On the order of the information system of interaction", Registered in the Ministry of Justice of Russia 26.11.2013 N 30454.
Order Roskomnadzor from 22.07.2015 N 85 "On approval of the application form the subject of personal data on the adoption of measures to restrict access to information processed in violation of the Russian legislation in the field of personal data", Registered in the Ministry of Justice of Russia 17.08.2015 N 38544.
The Federal Law "On Prosecutor's Office of the Russian Federation" of 17.01.1992 № 2202-1.
Federal Law 02.12.1990 No 395-1 "On banks and banking activity", "Rossiyskaya Gazeta", No 27, 10.2.1996.
The Federal law N 208-FZ "On Amendments to the Federal Law" On Information, Information Technologies and Protection of Information "and 'the Russian Federation Code of Administrative Offences' ", 23.06.2016. "Collection of the legislation of the Russian Federation".
Presidential Decree "On approval of the list confidential information" No. 188 from 06.03.1997 with the latest amendments from 2015.
The Federal law N 160-FZ "On ratification of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data", 19.12.2005. "Collection of the legislation of the Russian Federation", 52 (1 hr.): 5573.
National Standard of the Russian Federation GOST R ISO/IEC 27002-2012 "Information technology. Security techniques. Code of practice for information security management date of introduction". Approved by order of the Federal Agency for Technical Regulation and Metrology of the September 24, 2012 No. 423-st.
Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00. [Accessed 11 June 2016].
Letter of Ministry of Communications and Mass Communications of the Russian Federation, March 10, 2016 No. P11-1-4201 "On clarifying the norms of the federal law".
Standards governing the organization and requirements for protection of information systems of personal data in non-state pension fund Official website of the non-state pension fund. Available from: http://napf.ru/14154. [Accessed 1 September 2016].
Federal Law of 21.07.2014 No 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation to clarify the processing of personal data in the order of information and telecommunications networks". "Rossiyskaya gazeta", No 163, 07.23.2014.
Criminal Procedure Code of the Russian Federation. "Rossiyskaya Gazeta", No 249, 22.12.2001.
Civil Code of Russian Federation, "Rossiyskaya Gazeta", No 238–239, 08.12.1994.
Directive No. 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive On Privacy And Electronic Communications), Brussels, 12.VII.2002. Available from: http://eur-lex.europa.eu/. [Accessed 16 February 2016].
Privacy challenges. Analysis: It's surprisingly easy to identify individuals from credit-card metadata. Available from: http://news.mit.edu/2015/identify-from-credit-card-metadata-0129. [Accessed 17 February 2017].
Guidelines of Roskomnadzor of 5 September 2013 No 996 on the application "Order of Roskomnadzor 'On Approval of the

requirements and methods of depersonalization of personal data' ", approved by Roskomnadzor December 13 2013.
Federal Law № 152-FZ "On Personal Data", " Rossiyskaya gazeta", No 165, 29.07.2006.
The Tax Code of the Russian Federation, "Rossiyskaya Gazeta", No 148–149, 06.08.1998.
The Family Code of the Russian Federation, "Rossiyskaya Gazeta" No 17, 27.01.1996.
The Federal Law from 06.07.2016 No 375-FZ "On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation with regard to establishing additional measures to counter terrorism and ensure public safety", "Rossiyskaya Gazeta", No 150, 07.11.2016.
The Federal Law from 06.07.2016 No 374-FZ "On Amendments to the Federal Law" On Combating Terrorism "and Certain Legislative Acts of the Russian Federation to establish additional measures to counter terrorism and ensure public safety", "Rossiyskaya Gazeta", No 149, 08.07.2016.
The Federal Law from 18.12.2006 No 231-FZ "On the introduction of Part Four of the Civil Code of Russian Federation", "Rossiyskaya Gazeta", No 289, 22.12.2006.
The decision of the Constitutional Court of the Russian Federation (28 June 2012 No 1253-O it refused "To accept for consideration the complaint of the citizen Suprun Mikhail Nikolaevich about a violation of his constitutional rights in Article 137 of the Criminal Code of Russian Federation").
Government Decree of Russian Federation 01.11.2012 No 1119 "On approval of requirements for the protection of personal data at their processing in information systems of personal data", "Rossiyskaya Gazeta", No 256, 07.11.2012.
Universal Declaration of Human Rights, US GPO; 1949.
Constitution of the Russian Federation; 1993. Available from: http://www.constitution.ru/en/10003000-03.htm. [Accessed 10 June 2016].
Working Party, European Parliament and of the Council; 1995. Available from: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. [Accessed 1 June 2016].
Federal Law 06.04.2011 No 63-FZ "On Electronic Signature", "Rossiyskaya Gazeta"; 2011.
Federal Law "On Personal Data". "Rossiyskaya Gazeta"; 2015.