Applied Computing and Informatics (2016) **12**, 1–15

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

REVIEW ARTICLE

The salient features of personal data protection laws with special reference to cloud technologies. A comparative study between European countries and Russia

Zharova Anna *

Department of Innovations and Business in IT, Faculty of Business Informatics, National Research University, Higher School of Economics, 33 Kirpichnaya Str., Moscow, Russia

Received 22 April 2015; revised 30 June 2015; accepted 27 July 2015
Available online 14 August 2015

KEYWORDS

Internet;
Relationships between entities;
The legal regulation;
Cloud computing;
Personal data;
ISP

Abstract This article describes the basic directions of state policy in the use and implementation of cloud computing. It answers the question about the applicability of foreign cloud services for the processing of personal data of citizens of Russia. It describes the systematization of cloud services in Russia and the EU. It defines some specific measures to ensure the protection of personal data using the standards of the EU and Russia.

* Tel.: +7 (495) 771 32 38.
E-mail address: ajarova@hse.ru.
URL: http://www.hse.ru/en/org/persons/index_best.html?ltr=Z.

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2015.07.001

Contents

1. Introduction

The term "cloud computing" is often used in various spheres of public life. It refers to technology created to optimize business processes and improve the service quality of different service providers and to increase people's informatization level. Questions on people's interpersonal relationships arise more acutely in the field of medicine, government, banking and the private sector. The application of cloud computing is a strategically important development for computer technologies and offers the opportunity to provide different services.

The active introduction of cloud computing posed questions for legislators about the specifics of regulating people's behavior online. These questions concern data security when it is stored in the cloud, and whether cloud computing is privately- or government-owned. Questions about the requirements for cloud Internet Service Provider's (ISP) effective functions, as well as an ISP's responsibility for its own actions and those of third parties, remain unanswered. Is it possible to be sure that technology which allows us access to cloud computing is reliable and safe? What if public information and IT systems are hosted abroad?

In this article we will not consider the questions of the processing of state secrets or publicly accessible data by cloud computing. Rather we will address the main issues with cloud computing as far as data protection is concerned. Kristina Irion has described this problem, saying "many governments have raised concerns about national data sovereignty when government information is moved to the cloud. How can confidentiality of public information assets residing in the cloud be ensured? What if public information and IT systems are hosted abroad?..." [[16], p. 41]

I will consider the difficulties that legislation encounters when trying to ensure the protection of limited-access data, such as personal details.

2. The concept of cloud computing in Europe and Russia

2.1. The legal concept of cloud computing in Europe and Russia

Although currently the active application of the term "cloud computing" in the Russian Federation, and implemented programs for public e-health and e-government are based on cloud computing, this term has no legislative definition. The State Program of the Russian Federation "Information Society (2011–2020)" considers the development of cloud computing to be one of the main priorities for 2015. The creation of a national platform of cloud computing is provided for in this government program. It is planned to connect all the public authorities of the Russian Federation in the period of 2011–2020 [30]. In fact, cloud computing was taught at technical universities in 1990s and the further development of this technology at public institutes was predicted.

Consequently, we use the definition of the Institute of Electrical and Electronics Engineers (IEEE). According to the IEEE's definition published in 2008, "Cloud data processing is a paradigm within which information is constantly stored on servers on the Internet and is temporarily cached with the client party, for example on personal computers, game consoles, laptops and smart-phones [15]." The IEEE, investigating the prospects for developing cloud computing, drew a parallel between this technology and the internet. In Russia, IEEE companies operate in Siberia, the Northwest (St. Petersburg) and Central Russia (Moscow) [32].

Unlike Russia, the European Union passed a law in 2012, in which it was specified that "Cloud computing in simplified terms can be understood as the storing, processing and using of data on remotely located computers accessed over the internet." This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can access their data from anywhere so long as they have an internet connection. Cloud computing has the potential to slash users' IT expenditure and to enable many new services to be developed [6]."

In Russia, the lack of a legal definition allows ambiguous interpretations of the area of legislative regulation.

2.2. The technical concept of cloud computing in Europe and Russia

Cloud computing is considered to be a platform for different services. However, it is only classified in the technical sphere. The site International Organization for Standardization (ISO) contains the following classification of cloud computing:

(1) SaaS (Software as a Service) – the user of cloud computing is granted the right to use and access the necessary software.

(2) IaaS (Infrastructure as a Service) – the user of cloud computing is granted the right to use a provider's hardware–software complex for work and data storage.
(3) PaaS (Platform as a Service) – the user of cloud computing is granted the right to use a hardware–software complex for the development, testing, expansion and support of web applications [13].

In 2013, the Russian Federation's service for technical export control set out the State projected standard which defined cloud services such as follows:

– Hardware as a Service (HaaS);
– Security as a Service (SecaaS);
– Business process as a Service (BPaaS);
– Data as a Service (DaaS);
– Trust as a Service (TaaS);
– Infrastructure as a Service (IaaS);
– Cloud Development Environment as a Service (CDEaaS);
– Communication as a Service (CaaS);
– Platform as a Service (PaaS);
– Connection as a Service (CnaaS);
– Transparency as a Service (TraaS);
– Workplace as a Service (WaaS).

This classification complements the ISO classification. However, it seems it is redundant. Probably for this reason it is not accepted in Russia as a legal standard.

3. The policy of the States about the regulation of cloud computing

Legal questions about the regulation of the use of cloud computing are a concern for the majority of the European countries. In 2012, the EC developed a proposal for the regulation of the European parliament and for the Council on the protection of individuals' personal data processing and on the free movement of data (General Data Protection Regulation) [21].

The Cloud Security Alliance (CSA) discussed the importance of this problem of data protection, particularly personal data, in cloud computing. ''Data privacy considerations are often overlooked in the development phase of the cloud, Internet of Things and Big Data solutions, and instead are viewed through a maze of complicated regulations and guidance [4].'' Angela Adrian remarks also that ''unfortunately the legal infrastructure is inadequate to secure privacy.'' [[1], p. 49]

This problem is very important for Russia. In 2010 the Deputy Minister of the Ministry of Communications and Mass Communications, Ilya Massukh, said that ''these kinds of proprietary technologies in Russia are practically non-existent, therefore this sector is actively engaging with foreign companies such as

Google [20].” But, in 2014, a Russian Advisory Council from the Ministry of Communications and Mass Media Communications was created to improve the development of, and implement a state policy for, standards and legal regulation of cloud computing. The Advisory Council aimed to develop suggestions for improving the legislation for cloud computing to ensure the regular interaction of the Ministry of Communications and Mass Media with the expert community on cloud technologies [29].

EU Member States are also attempting to solve the problems which have arisen for users and developers of cloud computing. On 11 September 2013, the European Commission (EC) adopted a legislative package called “Connected Continent: Building a Telecoms Single Market.” The website claimed that “the package could boost the cloud computing market in Europe, as, among others, it aims at improving the quality of service that new services (such as cloud computing, video-conferencing, 3D printing) can offer [7].”

In Russia, according to the Order of the Government of the Russian Federation of 22.02.2012 No. 238-p Rostelecom[1] was appointed the sole executor for the further creation and development of complex information technology and telecommunications infrastructure including cloud computing and e-government for 2012–2014.

Rostelecom must execute the list of activities of the Russian state program “Information Society (2011–2020 years).” This program includes the development of a portal for public services, the development of a common space of trust in electronic signatures, the development of interagency electronic interaction and a single identification system. It is planned that Rostelecom will engage in the development of mechanisms which enable the use of mobile devices for access to e-government services and to the state-mail address which is used for the interaction between citizens and government agencies.

Rostelecom must create common directories and qualifiers for state information systems and it must develop systems such as the “Electronic Registry Office,” “E-Regions” and “E-democracy.” The basis for the implementation of these systems is a cloud computing platform. These systems offer infrastructure and software as a service (IaaS and SaaS). [The Official website of the Ministry of Communications and Mass Communications of the Russian Federation]

The Strategy “of the development of information technologies in the Russian Federation for 2014–2020 and planning until 2025” directs the creation of a Russian national platform for cloud computing [31]. For the realization of this strategy, the Russian government operates as the sole customer for everything needed for the Russian market for information technologies. Rostelecom developed and launched a cloud platform in August 2011. This helps Rostelecom sell their computing resources and software to third parties. In the future, this platform could be integrated into the national platform of cloud computing.

[1] The largest national telecommunications company in Russia.

Currently, the Russian Federation plans to create seven powerful data centers, on the basis of which cloud services for government agencies and academia will be provided. They include the public services platform, "Gospriklad," which was developed for the provision of public services [27].

The Decree of the Government of the Russian Federation of July 20, 2011 N 1275-p approved the concept of the creation and development of an integrated information system for the state management of public finances, the so-called "Electronic budget." This concept was recommended to the executive authorities of the Russian Federation and local authorities for the development of systems of public (municipal) finance. The subsystems of "Electronic budget" system will be available as a service for citizens of the Russian Federation, the municipalities or government sector organizations on a *pro bono* basis. These subsystems will be submitted as a model of "Software as a Service" (SaaS).

The portal of the Russian "Electronic budget" will consist of closed and of open parts.

The open part of this portal is being provided as a public information resource, providing free access to the regulatory, statistical and analytical information for the management of public finances. Storage and processing are being carried out in a centralized service of the "Electronic budget" system.

The closed part of this portal consists of "private offices" which can be available to users with the appropriate authorization and electronic signature keys. The closed part is the common point for user access to all services of the "Electronic budget," which will include a unified system of management of user access levels, depending on their powers. These services will be available to users of the cloud platform in areas such as medicine, housing, energy, and transport.

An example of the application of cloud computing for providing public services is the UK. In 2010 the UK started a project called G-Cloud ("Government cloud"). This optimizes the activities of government data centers and reduces government spending. Features of the G-Cloud include flexible scaling, open access to resources, an adequate level of security, a high degree of standardization and extensive information sharing. Such features make G-Cloud an attractive and economical solution to the complex architecture of internet-based administration. It is planned that through the G-Cloud the British authorities will have been able to reduce IT costs by over 20% in 2014 [25].

In the UK, a government gateway (Government Gateway) was introduced which provided the centralized online access to the government cloud. The Government Gateway has helped to bring together the disparate public internet resources of Great Britain, and also has closed a thousand duplicate administration sites out of a previous total of four thousand. This government gateway allows the exchange of information between portals. In addition, it stores all information in case of the failure of one of the subordinate portals. All citizens and legal entities are required to register in the Government Gateway for work and

to use this technology. The residents and the organizations in Britain are able to use three main British online services:

1. DirectGov: the portal of the Ministry of Work and Pensions for individuals;
2. NHS Choices: the portal of the Ministry of Health for individuals;
3. BusinessLink: the portal of the Ministry of tax and customs revenues for businesses.

The applicable technological system provides the transaction authentication and security. According to experts, the savings will be not less than £8 each time a citizen accesses these services [25].

Unfortunately, in the Russian Federation there are not so many examples of the use of models of public services based on cloud computing, although, from 2013 the idea of cloud computing in government was being actively implemented [26].

4. Legal regulation on use of personal data in Russia

Of course, answers to the above questions are linked to the category of information (limited access or open information) and also to subjects of the relationships such as the ISP, the user or the government. Cloud technology can belong to foreign or Russian ISPs. Information can be public or have limited access (ch. 2 Art. 5 of Federal law ''Information, Informational Technologies and Protection of Information'') [9]. Limited access information can be personal data; ''know-how''; and secret data imported from companies, and is regulated only by Federal legislation.

Cloud computing depends on its owner, which can be public or private. Public clouds belong to the state authorities or the local council. Furthermore, public cloud data may be better protected than the private cloud computing.

As Angela Adrian remarks, ''how should legal rules change to accommodate the new communication technology? If cloud computing does not alter our fundamental values, how should legal rules adapt and change in order to maintain our current values? What should the substance of our rules be in light of the changing environment for the actors in the cloud? [Angela Adrian, p. 49]

According to Art. 7 of the Russian Federal law ''On personal data,'' ''the users of personal data and other persons who have access to personal data are obliged not to disclose this information to third parties and not to impart personal data without consent of the subject of personal data. The other cases must be provided by the law [10].''

What ought to be done if information is stored in a foreign cloud?

According to item 11. Art. 3 of the Federal law ''On personal data,'' the cross-border transfer of personal data is the transfer of personal data to the territory of a foreign state, to the authority of the foreign state, to a foreign national person or a foreign legal entity.

Therefore, the cross-border transfer of personal data is the transmission of personal data on any person from the Russian Federation to a foreign person, abroad as, for example, when a person is filling in a form online to purchase goods from a foreign seller.

Art. 19 of the Law "On personal data" states that the Russian operator of personal data has to establish in the agreement with the foreign handler of the information, the duty to comply with the confidentiality of personal data, to ensure to the safety of personal data, and also to comply with other requirements to protect personal information. According to item 3. Art. 12 of the Law "On personal data" the operator of personal data must be convinced that the foreign country to which the data are transferred provides adequate protection for people's rights to their personal data. The Federal law "On personal data" specifies that states can be considered in two groups of countries:

(1) Member countries of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981); (This Convention came into force in the Russian Federation on September 1, 2013) [24].
(2) Countries which are not the party to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981), but which are listed as foreign states which provide adequate protection of the people's rights to their personal data.[2]

The Russian Ministry of Communications and Mass Media, in unofficial letter on May 13, 2009, explained that "the adequacy of protection means that the foreign state provides a level of security of people's rights to their personal data, not less than the standards provided for in Russia. One of the assessment criteria of the state in this respect is the ratification of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981) [17]."

However, if a cross-border transfer of personal data is being carried out in foreign states which do not provide adequate protection for people's rights to their personal data, then the user of the personal data must receive, in written form, that person's consent for their personal data to be transferred. These relationships between foreign ISP (operator of personal data) and the owner of personal data are regulated by the two Russian laws. They are the Federal law "On personal data" and the Federal law "On electronic signatures" [11].

[2] Australian alliance; The Argentine Republic; The State of Israel; Canada; Kingdom of Morocco; Malaysia; United Mexican States; Mongolia; New Zealand; The Republic of Angola; The Republic of Benin; The Republic of Cape Verde; The Republic of Korea; The Republic of Peru; The Republic of Senegal; Republic of Tunisia; Republic of Chile; Hong Kong Special Administrative Region of the People's Republic of China; The Swiss Confederation//The Order of the Federal Service for Supervision of Communications, Information Technology and Communications of March 15, 2013 No. 274 "On approval of the list of foreign countries that are not parties to the Convention of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, and provide adequate protection of human subjects personal data"// http://www.garant.ru/products/ipo/prime/doc/70268490/#ixzz3E8YwESIQ.

In accordance with part 4 Art. 9 of the Federal law "On personal data," the participants in the relationship have the right to use an electronic signature to create a written form of their agreement. Art. 4 of the Federal law "On electronic signatures" defined the rights of parties in the electronic interaction been using any information technology and (or) the technical means to apply an electronic signature. However, the Federal law "On electronic signatures" requires that participants (the provider of personal data and owners of personal data) must approve of these actions. This approval can be placed on the main web page of the cloud ISP which handles personal data. The owner of the personal data must agree with these conditions.

However, there is another view. Vladimir Kanashevsky writes that sending an e-mail message from a Russian user to a foreign cloud ISP of personal data cannot be signed with an electronic signature. "The foreign ISP potentially can be brought to civil liability in accordance with Russian law. In connection with this action, the claim for the damages and compensation for moral damages can be brought to the foreign operator [14]."

I do not accept the opinion of Vladimir Kanashevsky. Firstly, this author did not consider the provisions of the Russian Federal law "On electronic signatures." This law points directly to the recognition of foreign electronic signatures. Article 7 of this law indicates that "if an electronic signature is created in accordance with the law of a foreign state and the international standards then it is recognized in the Russian Federation as an electronic signature that corresponds to the Federal law "On electronic signatures." Also, according to part 2 of Art. 7 of this law "On electronic signatures," an electronic document signed by an electronic signature cannot be regarded as illegal only on the basis that the electronic signature verification key certificate is issued in accordance with the rules of the foreign law. [Federal law "On electronic signatures," 2011]

Secondly, part 2 of Art. 9 of the Federal law "On personal data" determines that the consent of the subject of personal data can be given in any form. For example, this form can be an e-mail message. Thus, the Federal law "On personal data" and the Federal law "On electronic signatures" define the legal conditions of consent recognition.

However, be aware that the Federal law "On personal data" allows the ISP of personal data not to obtain the consent of the subject of personal data if the cross-border transfer of personal data is carried out "for the execution of a contract. And party to this contract is the subject of personal data." (part 4 Art. 12 of the Federal law "On personal data"). Thus, this Federal law indicates the presence of the preliminary agreement on cooperation.

There is another exception under which the telecom operator[3] does not have to obtain the consent of the personal data individual. In 2013, the Russian Federal law "On communications" was changed [12]. Art. 53 of this law added the right

[3] The telecom operator in accordance with Russian law is a legal entity or individual employer which provides communication services based on a relevant license.

of the telecom operator to entrust the processing of personal data of clients to third parties even if a telecom operator has not received the consent of this person. This is the case only if the telecom operator processes the personal data in accordance with the contract for the provision of telecommunications services, and/or the telecom operator acts for the implementation of the rights and legitimate interests of the service provider or the client. However, the Federal law "On communications" did not disclose whether the operator had to warn of the fact that personal data was processed by a third party.

In addition, in 2014 the Federal Law "On Personal Data" was included the obligation of the operator of personal data to provide entry the storage, clarification, update, change and the extraction of personal data of citizens of the Russian Federation with the use of databases that were in the territory of the Russian Federation.

Thus, Kanashevsky's opinion about the complexities of personal data processing by a foreign cloud ISP of personal data does not apply in most cases.

In 2013–2014, the overall transmission model of personal data to external operators was changed in Russia. The list of cases expanded in which consent is not required from the subject of personal data on processing their data by third parties. So in terms of legal regulation in Russia, the implementation of any cloud service through the use of foreign cloud has become easier.

5. Ensuring the technological security of the transmission and processing of personal data in Russia and Europe

Of course, the cross-border transfer of data is associated with problems of transmission security and the processing of personal data. Experts in the technical sphere claim that it is impossible to ensure the absolute safety of these technologies [2]. Noriswadi Ismail has also written about these problems [18].

Providers of cloud services must address the questions of data security. The technological complexity of security in the cloud means that a virus-infected file from one client can infect other connected and inactive clients. In connection with this, there is the danger of compromised data being stored in the cloud. The responsibility for protection lies with the provider. Users of cloud services need to be sure that the provider uses security tools. The provider of cloud services should allow the user to check the level of protection and should record the actions of all clients who have access to the cloud.

Also it is difficult to select a required standard from all the existing standards. A European Commission communication described this problem: "A jungle of standards generates confusion by, on one hand, a proliferation of standards and on the other hand a lack of certainty as to which standards provide adequate levels of interoperability of data formats to permit portability; the extent to which safeguards are in place for the protection of personal data; or the problem of the data breaches and the protection against cyber-attacks... [6]". The authors propose to

solve the problem of responsibility for the actions of third parties through a choice of jurisdiction which is determined by the agreement.

But here it is necessary to bear in mind that there is no legal obligation to choose standards in the European Union or the Russian Federation. The choice of technology depends only on the parties to the relationship. Usually, the responsibility lies with the cloud ISP of personal data for the choice of the standard. Taiwan chose this approach. Fa-Chang Cheng and Wen-Hsing Lai write that "The Information Industry in Taiwan is now trying to realize the accountability concept through building up the certificate system in protecting the personal information privacy, especially for the purpose of protection within Cyberspace [8]."

In Russia, the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) for reducing the requirements for the protection system described in the "Recommendations on the choice of methods for the depersonalisation of data [19]" made recommendations and proposed various methods to anonymize personal data. When personal data depersonalize the complexity of the selection standards is lowered.

Noriswadi Ismail writes about solution adopted by Microsoft. "Microsoft proposes the amendment of CFAA's civil action provision that the cloud service providers possess a private right of action against those who illegally access their datacenters or secure unauthorized access to their customers' accounts. This proposed cause of action shall allow cloud service providers to combat digital criminals on behalf of their customers." [[18], p. 252]

If there are no special requirements of the law, then a Russia provider of cloud computing can voluntarily be audited and certified by the ISO/IEC 27001: 2005 and (or) SAS 70 Type II and Type I. Voluntary certification will allow the provider to prove that he sought by his actions to ensure data security.

The European Network and Information Security Agency (ENISA) proposed using ISO27001. Moreover ENISA noted that all suppliers must demonstrate compliance. They are NOT required to be accredited but compliance is verified through yearly submission of their information security management system and associated policy documents.

Additional certifications and accreditations assist European Health organisations in choosing appropriate providers, e.g., ISO20000 (Service Management), ISO9001 (Quality), but these are not required.

In terms of audit and compliance with regulations or the nominated standards of the service provider, cloud computing service providers must ensure that they are able and willing to allow the right to audit their policies, processes, systems and services." [Cloud Computing. Benefits, risks, 2009]

There are other mechanisms to ensure information security of processed and stored data. The report made by ENISA suggests possible solutions to existing problems. All data collected by European Health must satisfy the following requirements:

Data (including sensitive personal data) must be encrypted in transit and at rest where potentially at risk (e.g., on mobile devices);

Data processing must satisfy European data protection law (e.g., definition of "data processor" for all operations);

National law applies certain restrictions on the processing of the data (e.g., data should not leave the original country of collection at any time);

Clinical safety has to be paramount with certain applications, meaning that integrity and availability have to be guaranteed in some instances;

Sensitive data should be destroyed at a specified time in its lifecycle (e.g., by destruction of hard disks at the 'end of life' of equipment);

Physical security controls in data-centers where data is stored must be adequately assured (some of this is covered currently via ISO27001 submissions from suppliers);

Senior staff are given special responsibility for the confidentiality of "patient and service-user information [3]."

The Federal law, "About Technical Regulation [12]" in Art. 12 permits the voluntary application of standards in the field of a hardware–software. At the same time, the Russian Federation is actively cooperating with such organizations as the Technical Committee (TK) in the field of standardization. This has given Russian experts the opportunity of working in the international field of IT standardization. The international organization is the joint technical committee IS0/IEC JTC1, "Information technologies," with its subcommittees and working groups. The Russian experts working in this organization have had the opportunity to vote when standards have been discussed and new rules proposed.

Thus, the question of the technological security of personal data between Europe and Russia can be solved if countries agree on a specific standard as any international standard is developed by ISO is legal in the territory of Russia.

Every participant in a well-regulated market knows that, without implementation of the requirements of the existing standards which are have been developed with the direct voluntary participation of the product suppliers and service providers, not only successful activity but the existence of the market itself, would be impossible.

6. Conclusion

Cloud computing has drawbacks which carry new risks. These are topical both in Russia and Europe.

The European Network and Information Security Agency (ENISA) has identified network and information security risks which small and medium size enterprises (SMEs) should take into account when adopting cloud computing. [5]

1: Software security vulnerabilities
2: Network attacks
3: Social engineering attacks
4: Management GUI and API compromise

5: Device theft/loss
6: Physical hazards
7: Overloads
8: Unexpected costs
9: Vendor lock-in
10: Administrative or legal outages
11: Foreign jurisdiction issues

The Cloud Security Guide for SMEs detailed the causes of such risks for platforms such as IaaS, PaaS, and SaaS.

Russia has not produced an official, systematized description of the risks associated with cloud computing. However, there is a systematized list of requirements for the protection of the information contained in information systems. Thus, in 2013, the Federal Service for Technical and Export Control promulgated an Order "On approval of requirements on data protection that do not constitute state secrets and that are included in state information system [28]." In this Order, cloud computing is mentioned only in claim 24 as "the measures of information protection that is being selected and is being implemented in information system...can apply to the environment of virtualization and cloud computing."

In 2014, the Ministry of Communications prepared a bill "On Amendments to Certain Legislative Acts of the Russian Federation regarding the use of cloud computing [23]." This proposed amendments to the Federal Law "On Information, Information Technologies and Protection of Information." It included the concept of "cloud computing" and the qualification requirements for providers of cloud computing services; requirements for financial stability of the respective suppliers; data protection which is processed by such providers; rules for tariff regulation of prices for cloud computing services; conditions for the use of cloud computing and rules for the provision of cloud services; and responsibilities of the parties. Simultaneously, the bill proposes to amend the Federal Law "On personal data" to establish protection for personal data subject to cross-border transmission.

The adoption of this bill should enable a definition of the scope of legal relations, rules and regulations applicable to the parties involved in such relationships. However, it has not yet been introduced into the State Duma for consideration. This is a serious impediment to the further development of relationships in connection with cloud computing in the Russian Federation.

References

[1] Angela Adrian, How much privacy do clouds provide? An Australian perspective, Comput. Law Secur. Rev. 29 (2013).
[2] A.P. Baranov, Can we protect in the "cloud" of confidential information?, High Avail Syst. 8 (2) (2012).
[3] Cloud Computing, Benefits, risks and recommendations for information security, November 2009, <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> (accessed 12.12.14).

[4] Cloud Security Alliance, Published 2014, 23, September/2014 CSA Research News/New Cloud Security Alliance Survey Reveals Emerging International Data Privacy Challenges, <https://cloudsecurityalliance.org/media/news/csa-survey-reveals-emerging-international-data-privacy-challenges/> (accessed 10.12.14).
[5] Cloud Security Guide for SMEs, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes>.
[6] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions unleashing the potential of cloud computing in Europe, Brussels, 27.9.2012, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF> (accessed 12.12.14).
[7] Digital Agenda for Europe, A Europe 2020 Initiative, European Cloud Computing Strategy, 2012, <https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy> (accessed 10.12.14).
[8] Fa-Chang Cheng, Lai Wen-Hsing, The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy, Procedia Eng 29 (2012) 241–251.
[9] Federal law of the Russian Federation on 27 July 2006, in N 149-FZ "On Information, Informational Technologies and Protection of Information", The system GARANT Legislation with comments.
[10] Federal law of the Russian Federation on 27 July 2006, in N 152-FZ "On Personal Data", The system GARANT Legislation with comments.
[11] Federal law of the Russian Federation on 6 April 2011, N 63-FZ "On Electronic Signature", The system GARANT Legislation with comments.
[12] Federal law of the Russian Federation on 27 December 2002, N 184-FZ "About Technical Regulation", The system GARANT Legislation with comments.
[13] ISO/IEC TR 20000-9:2015 Information technology – Service management – Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services, <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65671>.
[14] V.A. Kanashevsky, Legal regime of cross-border transfer of Personal Data, Legislation, N 12, December, 2012.
[15] Klaus, How High Clouds Go, 2011, <http://blog.stimulsoft.com/articles/how-high-clouds-go> (accessed 12.12.14).
[16] Kristina Irion, Government cloud computing and national data sovereignty, Policy Internet 4 (3–4) (2012).
[17] Letter of the Ministry of Communications and Mass Communications of the Russian Federation of 13 May 2009 N CP-P11-2502 "On the implementation of the cross-border transfer of personal data", The system GARANT Legislation with comments.
[18] Noriswadi Ismail, Cursing the cloud (or) controlling the cloud?, Comput Law Secur. Rev. (2011) 27
[19] Official website of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), <http://rkn.gov.ru/news/rsoc/news23181.htm> (accessed 12.12.14).
[20] Official website of the Ministry of Communications and Mass Communications of the Russian Federation, <http://minsvyaz.ru/ru/monitoring/index.php?id_4=43034> (accessed 12.12.14).
[21] Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (accessed 11.05.15).
[23] The bill of the Russia Federation "On Amendments to Certain Legislative Acts of the Russian Federation regarding the use of cloud computing", <http://www.consultant.ru/law/hotdocs/33631.html?utm_campaign=hotdocs_day8&utm_source=ya.direct&utm_medium=cpc&utm_content=412295200>.
[24] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I., 1981, <http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm> (accessed 12.12.14).
[25] The experience of the e-government in the United Kingdom, <http://www.microsoft.com/rus/government/electronic/> (accessed 12.12.14).
[26] Internet interview with the head of the department of information technologies, communication and information security of the Ministry of Internal Affairs of the Russian Federation, Lieut-Gen of internal service Tyurkin M.L. Development and introduction of modern information technologies in system of the Ministry of Internal Affairs of Russia, The system GARANT Legislation with comments.
[27] The Ministry of Telecom and Mass Communications will create a resource it is Gospriklad.ru in, 2011, <http://minsvyaz.ru/ru/monitoring/index.php?id_4=41944> (accessed 12.12.14).
[28] The Order of the Federal Service for Technical and Export Control "On approval of requirements on data protection that do not constitute state secrets and that are included in state information system.", <http://

fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?highlight> (accessed 12.12.14).

[29] The Order of the Ministry of Communications and Mass Communications of the Russian Federation N 178 of June 30, 2014 "On the Council of Experts on the use of cloud computing in the Ministry of Communications and Mass Communications of the Russian Federation", The system GARANT Legislation with comments.

[30] The State Program of the Russian Federation "Information Society (2011–2020)" endorsed by Order of the Government of the Russian Federation on 20 October 2010, N 1815-r, The system GARANT Legislation with comments.

[31] The Strategy of development of branch of information technologies in the Russian Federation for 2014–2020 and on prospect till 2025 endorsed by Order of the Government of the Russian Federation on 1 November 2013, The system GARANT Legislation with comments.

[32] The Tomsk group and student's office of Institute of engineers on electrical equipment and radio electronics, <http://ieee.tusur.ru/index.htm> (accessed 11.12.14).

Further reading

[22] Security Issues in Cross-border e-Authentication, <http://www.enisa.europa.eu/media/news-items/security-issues-in-cross-border-e-authentication> (accessed 12.12.14).