UDK 378.1

TRUST IN "CLOUDS": PROVIDER MODEL

Evgeniya A. Ostashova, Zhanna A. Rozhneva

National Research Tomsk State University, Tomsk, Russia
e-mail: evgeniya.ostashova@gmail.com; zhar@ido.tsu.ru

Abstract: *Today cloud technologies are widely used in both the public and corporate sectors and in the private sector. The focus of this article is placed on the use of "clouds" to solve personally oriented problems. The use of this technology implies the emergence of trust between the user and the provider. The authors believe that the user's and provider's trust models are not identical to each othe,r and at this stage of the study they attempt to identify the provider's trust model based on analysis of user agreements and privacy policies posted on the web sites of leading cloud storage providers.*

Keywords: *cloud technologies, public clouds, provider, user, trust.*

The market of cloud services in Russia in the last three years demonstrates a significant development, in terms of growth rates ahead of both other information technologies [1] and the global cloud market [2]. "Clouds" are used by state bodies and business to provide services, to provide various internal needs, as well as individuals to solve personally-oriented tasks. We believe that, as with any other transaction, when using "clouds" between the seller (provider) and the consumer, trust is formed. At this stage of the research, we set ourselves the goal to consider the use of cloud technologies and the trust model that is formed during this usage at individual level.

We will stipulate that the range of tasks solved at the personal level with the help of cloud technologies is very wide. These tasks can range from highly personal (storing photographs, video recordings, etc.) to organizing joint work on projects, "transporting" files necessary for work both in the office and at home. It seems to us that, despite the variety of goals, spheres and methods of using cloud services by individuals, the mechanisms for protecting their own data when using "clouds" that the state and business possess are much more powerful and diverse than those available to ordinary users, and the degree of dependence of the latter on provided by the provider of the conditions for presenting the service above. In many ways this is due to the fact, that most people choose public clouds and free services. Therefore, in case of personal use, a significant role in the relationship between the provider of cloud services and the user is played by trust.

We believe that we should distinguish between two non-identical trust models: the user's trust model and the cloud service provider's trust model. It is

obvious, that their formation is influenced by the legislative framework governing the provision and use of cloud computing by establishing a set of mandatory requirements for the openness and data security, the ways and means for their processing. Thus, we assume that the general model of trust in the clouds is formed at intersection of the models of trust between the user and the provider, while not offending against the law.

A lot of work in the field of studying the influence of the trust factor on the use of the Internet, including cloud services, as a medium for the existence and storage of a variety of documented information, is conducted within the framework of the international project InterPARES Trust [3], of which we are also participants. In Russian studies of cloud technologies, which began to appear not so long ago, the main focus is on studying the emerging practices of using "clouds" in the corporate and public sectors. In addition, there are a number of works in which "clouds" are regarded as an object of law. In them, in particular, there is a lack of a single interpretation of the notion of "cloud technologies" / "cloud services" / "cloud" and points out the need to develop a common terminology that would accurately describe the subject of regulation, since the currently existing regulatory Acts a lot of terms only complicates the development of the legislative framework [4]. Disputes among lawyers are also caused by which branch of law is called upon to regulate various aspects of the existence, provision and use of clouds [5, p. 377, 379; 6, p. 31, 33; 7]. Not being experts in the field of law, we did not set ourselves the task of studying in detail the problems, associated with the development of the legal status of cloud technologies.

Identifying models of trust between the user and the provider implies the need to conduct research in three ways. Firstly, it is necessary to study the legislation regulating the use of cloud services, in order to identify legislative requirements for clouds, as well as existing gaps in the legislative framework. Secondly, it is necessary to analyze user agreements, privacy policies and conditions for using the most popular services that provide the ability to store data in the clouds.

Unlike the models of trust formed by the law and the provider, which are of a "written" nature, the user's trust model manifests itself exclusively at the level of his actions, the internal logic of which is often not reflected by the user himself. It seems that the identification of this model and the permissible risks is possible within the framework of interviews that are still outside the scope of this study.

Our task at this stage was to identify a trust model designed by cloud service providers, by which we mean the online storage of user information resources and the organization of access to them.

To reconstruct this model of trust, it is of fundamental importance to determine those criteria on the basis of which, in the opinion of the provider, the user makes a choice in favor of trusting or not trusting the service. To this end, we analyzed user agreements, documents containing a privacy policy and terms of use, posted on the websites of leading companies that provide the ability to work in the "clouds" (document storage, modification, transfer, etc.) - Google Drive (Privacy

Policy [8] and Terms of Use [9]), Dropbox (Dropbox Service Terms [10], Dropbox Privacy Policy [11], Dropbox Acceptable Use Policy [12]), Yandex Disc (Privacy Policy [13], User Agreement (15), Microsoft's OneDrive (Microsoft Privacy Statement [16] and the Microsoft Services Agreement [17]), iCloud from Apple (iCloud Security and Privacy Overview) [18], Apple's Privacy Policy [19]).

The documents examined do not require a formal signing by the user (signing a paper copy, verifying with an electronic signature). The very fact of using the provided services (not only "clouds") assumes that the user is familiar with all the documents that determine the procedure for providing and using the service and agrees with them.

Explicitly, the basic principles, that help to earn users' trust are provided by Microsoft and include:

1. Management - providing "easy-to-use controls for confidentiality and clear choices";

2. Transparency - providing the user with information about the collection and use of data, so that the user can make an informed decision;

3. Security - the company guarantees the protection of data it trusts "with the help of a reliable security and encryption system";

4. Reliable legal protection - "respect" of local legislation on confidentiality and the struggle for its protection;

5. Lack of targeted advertising based on content – the refusal to use the user's personal data (content of letters, chats, etc.) to form advertising;

6. Expanding the user's capabilities - the use of data collected by the company about the user solely for its benefit and the expansion of its capabilities [20].

Google is committed to five principles of confidentiality, including: 1) "use of information to improve the quality of products and services"; 2) "development of products in accordance with strict standards of confidentiality" (including taking into account the requirements of legislation in the field of information protection); 3) "transparency of collection of personal information", i.e. informing the user about what data is collected and stored and for what they are used; 4) "the choice of means of protecting confidentiality", i.e. variability of work with personal information; 5) "responsible management of information received": protection of users and their information from malicious programs, fraud, technical failures, etc. [21].

In general, describing their services, companies emphasize the convenience and versatility of their use (the ability to access from anywhere, from any device, the speed of downloading files, extensive use, synchronization of files on various devices) and data protection from loss ("files they will not be lost anymore "[22]," You will not lose them [files], even if something happens with a computer or phone "[23]); flexibility of user settings and breadth of tools for managing their own content, including in the field of ensuring its confidentiality.

One of the key issues, discussed by all the above-listed providers of "cloud" services is the issue of processing user personal data. In the Russian Federation, the concept of "personal data", "subject" and "personal data operator", the rules for

processing and using this data are determined by the Federal Law "On Personal Data" [24].

The explicit reference to this Federal Law and its compliance with this law are present in the "Policy on the processing of personal data of Microsoft Rus" [25] ("Microsoft Rus" - the representative office of Microsoft in Russia) and in the "Privacy Policy" of Yandex [13]. Other services refer to international documents: The Convention for the Protection of Individuals with Automatic Processing of Personal Data [26], the APEC Cross-border Confidentiality Rules System [27] (iCloud), the US-EU Framework Agreement "Shield confidentiality "[28] (Google Drive, Dropbox, MS OneDrive), the Digital Millennium Copyright Act [29].

The documents, reflecting the confidentiality policy list the types of personal (personal) data collected (in this case the term is used without reference to Russian legislation and reflects what the cloud service provider understands for this kind of information), the methods of using them, are called the conditions transmission of these data by third parties and outlines the circle of third parties to which the personal information of the user can be transferred. It should be noted, that since the company's data not only provides access to the cloud, but also other services (mail, search engines, blogs and forums, purchases), the listed types of personal data are collected for all services provided by the company, and not exclusively for the "cloud".

Data collected about the name and surname are collected; physical and electronic address; phone number; credit card details; (iCloud, Dropbox, OneDrive, Google Drive), in addition, data about the use of other services, search queries, interests, contacts, frequently visited places (OneDrive, Google Drive), etc. can be collected.

In documents with varying degrees of detail, the purposes of using personal data are described. The main ones are:

1) provision of the company's own functions (improvement of existing and creation of new services, enhancement of personalization of provided services, relevance of search, internal analysis and audit). In this regard, the fundamental position of MS is the refusal to use phrases from letters, chat messages, as well as personal files of users for the formation of targeted advertising;

2) protection and identification of users (for example, based on data about devices from which the service is usually used, the company can warn the user in case his account has entered their unusual place or from a new device);

3) informing users. Apple also claims that it uses collected personal data if its customers participate in the lottery [19].

The collected data can be transferred to partners of provider companies, companies providing certain services (for example, processing information) to the provider itself, to government agencies (in accordance with the requirements of the law). Also, the provider provides public data about the user to other users (the user can determine what data will be considered public).

Thus, this information, presented in user agreements, documents that determine the policy of companies regarding personal data and confidentiality, should

form a user's perception of what (what data), who, how and for what collects, stores, transfers and processes.

The analyzed documents practically do not contain a description of the technologies used by companies. Corresponding references are given by MS company (only English-language document) [30]. Apparently, the brevity of technical information does not mean that providers do not view technology entirely as a factor of trust, but rather because they want to make user agreements as understandable to non-specialists.

Companies that offer cloud services claim to provide the user with ample opportunities to control their own content: posting, deleting and other actions on files and data; change Password; refusal from target distribution, granting another user access to their own materials or, conversely, limiting it, etc. In the context of maintaining control, it is interesting to consider the fate of the user's materials laid out in the cloud after they have been deleted by the user (deleting individual files or deleting the account as a whole). Obviously, such information will not be available to other users, but what are the further actions of the provider regarding these materials?

The considered user agreements provide that the provider will stop processing such data, but only Dropbox declares that after deleting the account by the user, all the information related to it will be deleted. At the same time, users are warned about possible delays in the removal of information related to the technical features of the process, as well as the possibility of preserving information, in cases where this is required by law, necessary to resolve litigation disputes or fulfill existing agreements [11].

The analysis of user agreements, terms of providing and using cloud services shows, that for a provider, a service, that can be trusted is, first of all, a service protected from unauthorized access by third parties not specified in the specified documents. At the same time, user agreements stipulate, that the content of the posted data is exclusively within the scope of the user's responsibility. At the same time, the provider can view the content and delete it in case of violation of the law or company policy, although it does not assume such an obligation and is not responsible for the materials posted by users.

In addition, the agreements stipulate some objective conditions under which the preservation of information or access to it becomes impossible (technical failures, cataclysms, etc.), emphasizing that the user uses the service "at his own risk" and the service is provided "as is "(this term is used by providers in the texts of user agreements and implies a waiver of responsibility for problems arising in the process of using the cloud service). Thus, the trust model, designed by the provider, is based, first of all, on those data security guarantees, that are provided by the legislation and which he himself considers necessary and sufficient to attract users to his own service. From the provider's point of view, the security of user data from unauthorized access is a factor of trust, since this provision is reproduced in all user agreements. However, it seems that these models are oriented, rather not at the user, but on the successful implementation of their own activities by provider company.

References

1. The growth of clouds is the result of technological, economic and legislative changes [Electronic resource]: an interview with S. Drugalev // CNews: analytics: an online edition about high technologies. – M., 2015. – URL: http://www.cnews.ru/articles/2015-12-01_stanislav_drugalev_rost_oblakov_rezultat_tehnologicheskih (access date: 07.06.2017).

2. Koptelov, A. How to combine the advantages of a public and private cloud? [Electronic resource] // CNews: analytics: an online edition about high technologies. – M., 2014. – http://www.cnews.ru/reviews/cloud_2014/articles/kak_sovmestit_preimushchestva_chastnogo_i_publichnogo_oblakov/ (access date: 07.06.2017).

3. InterPARES Trust [official site]. – Vancouver, BC, Canada, [2013-1018]. – URL: https://interparestrust.org/trust/contact (access date: 07.06.2017).

4. Kozhevnikova, Y.S. The essence of information and legal relations formed with the use of cloud technologies in the Russian Federation // Proceedings on Intellectual Property. – 2013. – № 2, volume XIII. – P. 211-284.

5. Kozhevnikova, Y.S. Problems of regulation of the activity of providers of cloud computing in the information legislation of Russia and the Federal Republic of Germany (comparative legal analysis) // European Social Science Journal. – 2012. – № 12. – P. 376-379.

6. Kozhevnikova, Y.S. Problems of the regulation of relations formed with the use of information cloud technologies: a combination of regulation and self-regulation // Jurist. – 2014. – № 13. – P. 30-35.

7. Saveliev, A.S. The legal nature of "cloud" services: freedom of contract, copyright and high technology / / Herald of civil law. – 2015. – № 5. – P. 62-99.

8. Google Privacy Policy [Electronic resource]. – Mountain View, CA USA, 2017. – URL: https://www.google.com/intl/ru/policies/privacy/ (access date: 07.06.2017).

9. Google Terms of Service [Electronic Resource]. – Mountain View, CA USA, 2014. – URL: https://www.google.com/intl/ru/policies/terms/ (access date: 07.06.2017).

10. Terms of Service Dropbox [Electronic resource]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#terms (access date: 07.06.2017).

11. Privacy Policy Dropbox [Electronic resource]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#terms (access date: 07.06.2017).

12. The policy of acceptable use of Dropbox [Electronic resource]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#acceptable_use (access date: 07.06.2017).

13. Privacy Policy [Electronic resource]. – M., 2016. – URL: https://yandex.ru/legal/confidential/index.html (access date: 07.06.2017).

14. User agreement of Yandex services [Electronic resource]. – M., 2016. – URL: https://yandex.ru/legal/rules/index.html (access date: 07.06.2017).

15. Terms of use of the Yandex.Disk service [Electronic resource]. – M., 2016. – URL: https://yandex.ru/legal/disk_termsofuse/ (access date: 07.06.2017).

16. Microsoft Privacy Statement [Electronic resource]. – [Б.м.], 2017. – URL: https://privacy.microsoft.com/ru-ru/privacystatement (access date: 07.06.2017).

17. Agreement on the use of Microsoft services [Electronic resource]. – [Б.м.], 2016. – URL: https://www.microsoft.com/ru-ru/servicesagreement/ (access date: 07.06.2017).

18. Overview of security and privacy iCloud [Electronic resource]. – [Б.м.], 2017. – URL: https://support.apple.com/ru-ru/HT202303 (access date: 07.06.2017).

19. Apple Privacy Policy [Electronic resource]. – [Б.м.], 2016. – URL: https://www.apple.com/ru/legal/privacy/ru/ (access date: 07.06.2017).

20. Six principles of Microsoft privacy [Electronic resource]. – [Б.м.], [2017]. – URL: https://privacy.microsoft.com/ru-RU/ (access date: 07.06.2017).

21. Google Privacy Policy and Terms of Use: Technology and Principles [Electronic resource]. – Mountain View, CA USA, 2017. – URL: https://www.google.com/intl/ru/policies/technologies/ (access date: 07.06.2017).

22. Official site of the Dropbox service [Electronic resource]. – [Б.м.]. URL: dropbox.com (access date: 07.06.2017).

23. Official site of Yandex.Disk service [Electronic resource]. – M., [2012-2017]. – URL: https://disk.yandex.ru/ (access date: 07.06.2017).

24. On the personal data [Electronic resource]: federal law of Russ. Federation of July 27, 2007 No. 152-FZ // ConsultantPlus: reference legal system. – M., [1997-2017]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (access date: 07.06.2017).

25. Policy regarding the processing of personal data by Microsoft Rus [Electronic resource] - [LM], [2017]. – URL: https://www.microsoft.com/ru-ru/about/piidatapolicy/privacy.aspx.

26. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Electronic resource]. – Strasbourg, 1981. – European Treaty Series, № 108. – URL: https://rm.coe.int/1680078b37 (access date: 07.06.2017).

27. APEC Cross-Border Privacy Rules System [Electronic resource]. – [Б.м.], 2016. – URL: http://www.cbprs.org/ (access date: 07.06.2017).

28. Privacy Shield Framework [Electronic resource]. – Washington, D.C., [2017]. – URL: https://www.privacyshield.gov/EU-US-Framework (access date:07.06.2017).

29. The Digital Millennium Copyright Act of 1998 [Electronic resource]. – [Б.м.], 1998. – URL: https://www.copyright.gov/legislation/dmca.pdf (access date: 07.06.2017).

30. Microsoft Enterprise Cloud Red Teaming [Electronic resource] – [Б.м.], 2014. – URL: https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf (access date: 07.06.2017).