

Association for Information Systems

AIS Electronic Library (AISeL)

International Conference on Information
Systems 2019 Special Interest Group on Big
Data Proceedings

Special Interest Group on Big Data Proceedings

12-1-2019

Big Data issue and the personal data protection in the Russian Federation

Andrey Shcherbovich

Follow this and additional works at: <https://aisel.aisnet.org/sigbd2019>

Recommended Citation

Shcherbovich, Andrey, "Big Data issue and the personal data protection in the Russian Federation" (2019). *International Conference on Information Systems 2019 Special Interest Group on Big Data Proceedings*.

4.

<https://aisel.aisnet.org/sigbd2019/4>

This material is brought to you by the Special Interest Group on Big Data Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in International Conference on Information Systems 2019 Special Interest Group on Big Data Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Abstract

Dr. Andrey A. Shcherbovich

Big Data issue and the personal data protection in the Russian Federation

Keywords: big data; data protection; data localization; Russia; Internet Governance; human rights; digital aquarium.

Today the Big Data sciences turn its age out. Some years pass, and there will be no need of data scientists, because all process of the big data collection will be automated. And this makes a big challenge to the scope of issues related to human rights of the subjects of personal data. This is a complex issue related to ethical, legal, and technological problems of human rights in Internet Governance.

Big data, as we now refer to enormous collections of facts, figures and unstructured information like metadata and tweets has helped us better understand crime rates and predict outbreaks of communicable diseases, and it radically improves our online shopping experiences. But imagine the potential benefits when such data science innovations are applied to the world of human rights. Rather than a digital hazard, computer technology that can handle big data can draw from information about human sentiments and actions to predict potential atrocities reveal patterns of destructive human activities such as trafficking and help weigh prescriptive policies.

Due to the complex nature of the information law in Russia, there is no codified acts in information sphere. Russian information legislation consists of some generalized laws, led by the Constitution of Russian Federation. Among them there are legislative provisions governing information sphere in general, as well as specialized law on personal data

Constitutional provisions highlighting first contradiction between privacy rights and freedom of information. Information inviolability of private individuals ensured in the para.1 of Article 24, according to which the collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent. However, the term privacy, widely used in the foreign legislation and international rules, is not expressed directly in Russian Constitution or legislation acts.

Russian citizens do not consider their personal data extremely valuable. Evaluability of the personal data is more commercial than moral. There is no general habit for privacy protection in the country. In the last decade, personal data of Russian citizens could be found on sale on the black market.

In the era of the Internet and other technological innovations, we can see that the approach to security of the personal data has been changed. The Internet serves for transparency of societies but on the other hand, this transparency is now related to the ordinary users around the world. We can see the digital traces of people voluntarily leaving their personal data on the social network's websites, or other online services.

Personal data could be recognized as a digital currency. People are providing their personal information when registering and using different services, being free for them. Personal data is a good, which has commercial value. This personal data could be collected directly (by website registration) or indirectly (by using cookies or other instruments tracing users' behavior online). That data could help resource providers to individualize the use of services for particular users, providing context advertising, and for other similar purposes.

Although Russia is a member of the Council of Europe and a signatory of the Council of Europe Convention on the protection of individuals in the automated processing of personal data¹, the Russian personal data legislation has been criticized for not complying with the Convention². In the Convention, the ability to ensure adequate protection of personal data means the presence in the state of a specially authorized body and the independence of such a body. According to these criteria, Russia cannot be called a country that provides adequate protection of personal data, since the authorized body, the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications, better known as Roskomnadzor, is structurally dependent on the Ministry of Communications. One of the main causes of concern in this area has been the introduction of legislative provisions mandating the localization of the personal data of Russian citizens.

¹ Convention on the protection of individuals in the automated processing of personal data. Concluded in the city of Strasbourg on 28 January 1981. // ConsultantPlus Legal Reference System.

² Ivanov A.A. Storage of personal data abroad from the point of view of Russian law // The Law. 2015. No. 1. P. 134–143.

The Roskomnadzor, has the right, based on a judicial act that has entered into legal force, to restrict access to information processed in violation of the legislation of the Russian Federation in the field of personal data. The law defines the procedure for restricting access to information processed in violation of the legislation of the Russian Federation in the field of personal data. For this purpose, an automated information system entitled “Register of violators of the rights of personal data subjects” has been created.

Localization of personal data of all Russian citizens was indeed introduced by amendments to the Federal Law “On Personal Data”. The data localization law (hereinafter – Law No. 242-FZ) regulates the obligations of operators to ensure the recording, systematization, accumulation, storage, refinement (updating, modification) and retrieving of personal data of citizens of the Russian Federation who are in the databases located in the territory of the Russian Federation, as well as specifying the location data.

Starting from September 1, 2015, Internet service providers that deal with personal data of Russians have been required to process such information using databases located in Russia.³ The data localization provisions concerned, first of all, online stores, social networks, ticket booking services, hotels, and other services, where users must indicate their citizenship. Such provisions target both Russian companies that store data abroad and about foreign organisations that deal with customers from Russia.

The reason for adopting the Law is formulated by its authors as follows. Many citizens are registered on social networks, buy goods and receive services via the Internet. A significant part of such services is located abroad, mainly in the USA and Europe. As a result, credit card data, passport data, correspondence, including by email, are accumulated by service providers based in foreign jurisdictions.

As stated by Vadim Dengin, one of the proponents of the Law and First Deputy Chairman of the State Duma Committee of the Russian Federation on Information Policy, Information Technology, and Communications, the majority of Russians are opposed to the storage of their data abroad and wish it to remain in the territory of Russia. If not stored in

³ Federal Law of July 21, 2014 No. 242-FZ “On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for Processing Personal Data in Information and Telecommunication Networks” (as amended on 31.12.2014) // ConsultantPlus Legal Reference System.

Russia, such information may fall into the hands of malicious actors, including fraudsters and foreign intelligence services.⁴

As was to be expected, the Law provoked a rather skeptical reaction among the experts of the Internet industry. The terms of the document are generally accused of being unattainable, and, in practice, they will in no way ensure the safety of the Russians, but rather complicate their lives and delay the development of the Internet in Russia. Academic Director of the Higher School of Economics Faculty of Law, Anton Ivanov, believes that Law No. 242-FZ is referring to the prohibition of the cross-border transfer of personal data to databases hosted on tangible media located abroad. However, the Convention on the Protection of Individuals in the Automatic Processing of Personal Data and the Law on Personal Data generally allow the cross-border transfer of personal data.

According to the European Center for International Political Economy (ECIPE), the entry into force of the Law on the Localization of Personal Data will lead to a decrease in Russia's GDP, which is equivalent to a loss of 286 billion rubles⁵.

Also, according to a European diplomatic source, the Russian Law on the localization of personal data can create problems when issuing Schengen visas. The source explained that the servers that store data on European visas for Russian citizens are located in Europe⁶.

Notably, the list of resources that may be blocked by Roskomnadzor due to inconsistency with the law on the localization of personal data does not mention such specific technical elements as foreign domain names, DNS addresses, and static IPs, essential for the transmission of personal data. On the one hand, the application of Law No. 242-FZ to the databases containing these objects could paralyze the entire Russian segment of the Internet because the basic mechanisms enabling the smooth functioning of the Internet are located outside the Russian Federation. On the other hand, it is important to stress that such large-scale restrictions as the ones foreseen by

⁴ Filimonov A. "It is necessary to share!" Or Protection of personal data of Russians from foreign special services // GARANT.RU information legal portal. <<http://www.garant.ru/article/559071/>> accessed October 12, 2019.

⁵ Personal unprofitable. How much will Russia lose due to personal data law. RBC News Agency <<https://www.rbc.ru/newspaper/2015/06/16/56bcc9349a7947299f72bef0>> accessed October 12, 2019.

⁶ The EU warned about problems with issuing visas due to the law on personal data. Interfax News Agency. <<http://www.interfax.ru/russia/402035>> accessed October 12, 2019.

the law are hardly possible to implement from a technical perspective because the authors of the law did not take into account the transnational nature of the Internet and its technical features. The law concerns social networks, airline reservation services, hotels and other services of foreign origin and transnational scope and such services may prove hard to block on a national basis.

The case of the ban and blocking of the social network LinkedIn in the Russian Federation is particularly noteworthy. Roskomnadzor filed a lawsuit against the LinkedIn Corporation on the recognition of the activities of its Internet resources for the collection, use, and storage of personal data of Russian citizens, indicating the claim was justified by the fact that Roskomnadzor, in accordance with its Internet monitoring attributions, identified a violation of the rights and legitimate interests of citizens of the Russian Federation as personal data subjects. According to Roskomnadzor, LinkedIn violated the requirements of the legislation of the Russian Federation in the field of personal data, specifically of law No. 152-FZ on personal data, by collecting information about LinkedIn users, as well as citizens of the Russian Federation who are not LinkedIn users, and by processing and transmitting such information without proper consent.

The Tagansky District Court of Moscow established that the administrator of the domain name of the website (LinkedIn.com) is a company, LinkedIn Corporation, located outside the Russian Federation and recognized LinkedIn's collection, use and storage of personal data of citizens of the Russian Federation as violating the requirements of the Law on Personal Data and citizens' rights to privacy, personal and family secrets. Accordingly, the Court ordered Roskomnadzor to take measures to restrict access to information on the Internet that has been processed in violation of the legislation of the Russian Federation in the field of personal data⁷.

As many Russian companies, LinkedIn stores data on servers located out of Russia, as this is a cheaper and more convenient option. Besides, utilizing servers in non-Russian countries facilitates access to these resources for all individuals who are not in Russia.

Even though technically such localization is possible, many questions arise regarding the implementation of the constitutional rights and freedoms of citizens. Indeed, may be argued that Law No. 242-FZ could be deemed as

⁷ The decision of the Tagansky District Court of Moscow dated 04.08.2016 in case No. 2-3491/2016 // ConsultantPlus Legal Reference System.

unconstitutional. By restricting the right of a citizen to the cross-border transfer of personal data, even if an individual has given his consent to such a transfer, the Law conflicts with Art. 23 (privacy of correspondence) and Art. 29 p. (freedom of information). of the Constitution of the Russian Federation⁸.

Internet goes much forward against efforts of legislators to regulate it. Legislator imposes old approaches to the national sovereignty and recognition of the state borders, but it is absolutely have no sense regarding the Internet.

National network infrastructure in Russia is not so developed as transnational one, so people have to use transnational services even in case they are not know other languages and never traveled outside Russia. When people are using mobile phones they addressing to the transnational services. Both Android and iPhone online application stores, which are required for regular technical maintenance and updating, store their data outside of Russia and could be blocked for incompliance with data localization requirements.

The concept of digital aquarium. If the personal data could be recognized as digital currency, people are paying for using of the free services by their personal data. In the digital world, the concept of privacy and the personal data could be different. There is a need to ensure balance between personal data protection and openness, interoperability and transparency of the Internet.

⁸ Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, with the amendments made by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of 30.12.2008 No. 6-FKZ, of 30.12.2008 No. 7-FKZ, of 02.05.2014 N 2-FKZ, of 21.07.2014 N 11-FKZ)