Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Russia's new personal data localization regulations: A step forward or a self-imposed sanction?

Alexander Savelyev *

Legal Department, IBM East ern Europe/Asia Ltd., Moscow, Russia

Keywords:
Personal data
Data localization
Cloud computing
Big data
Transborder data flows
Digital sovereignty

A B S T R A C T

The paper represents one of the first comprehensive analyses of Russian personal data localization regulations, which became effective at September 1, 2015. This work describes in detail the main components of the data localization mechanism: triggers of its application, scope, exemptions and enforcement. It also takes into account the official and non-official interpretations of the law by Russian regulators, some of which were developed with the participation of the author. Special consideration is given to the jurisdictional aspects of the Russian data protection legislation and the criteria of its application to foreign data controllers. The author also reveals the rationale behind the adoption of data localization provisions and analyzes their possible impact on foreign companies operating in Russia and implementation of innovative IT-technologies (Cloud computing, Big Data and Internet of Things). The paper concludes that most of the potential benefits of data localization provisions, i.e. in the area of public law, law enforcement activities and taxation. Nevertheless, data localization provisions may still have medium-term positive impact on privacy, since they force all stakeholders to revisit the basic concepts of existing personal data legislation (the notion of personal data, data controller, processing, etc.), thus serving as a driver for re-shaping existing outdated data privacy regulations and crafting something more suitable for the modern IT-environment.

1. Introduction

The Russian legislation in the sphere of information technologies is changing rapidly these days. Lots of newly adopted legal rules are reshaping the IT-market in Russia: software import substitution regulations in public procurement[1], special provisions governing blogger's activities, imposition of data retention obligations on Internet communication services, to name a few. But one of the most controversial and widely discussed is the recent "reinforcement" of Russian IT-law that relates to data localization provisions.

* IBM East ern Europe/Asia Ltd., Presnenskaya nab., 10, Moscow 123317, Russia.
E-mail address: garantus@rambler.ru.

[1] Federal Law No. 188-FZ of 19 June 2015, which established preferential treatment of "domestic" software during public procurement procedures. The criteria of domestic software are: 1) exclusive right to such software should belong to a Russian person, specified in a law (e.g. to Russian Federation or its region, Russian citizen, non-commercial entity controlled by the above persons, commercial entity, established by the above persons, etc.); 2) such software should be freely available for distribution on the territory of the Russian Federation, including Crimea; 3) licence fees to foreign persons should not exceed 30% of proceeds from sales of such software.

http://dx.doi.org/10.1016/j.clsr.2015.12.003
0267-3649/

Until recently, Russian legislation did not contain any special provisions governing data location: information could be stored and processed everywhere, subject to limitations associated with some traditional special regimes (e.g. information constituting state secret or conditions of transborder data flow to countries not providing adequate protection of personal data).

The first signs of data localization provisions appeared in the banking sphere. In accordance with amendments to Federal Law "On Banks and Banking Activities", adopted in 2013, financial institutions acting under a license from Central Bank of Russia were obliged to reflect all their financial transactions in electronic databases, allowing to store such data for a period not less than five years. Subsequent regulations of the Central Bank of Russia established that backup copies of such databases should be located in Russia[2]. However, location of primary databases with such data was not regulated: for the purposes of control and oversight activities, it is more than enough to have local backup databases not complicated by jurisdictional matters.

The second wave of data localization provisions happened in 2014. As a legislative response to the terrorist acts committed in Russian city Volgograd in the end of 2013, the so-called anti-terrorist "package" of laws was introduced, which apart from strengthening criminal liability for terrorist and related activities, introduced additional limitations on anonymous electronic money payments, obligations to identify users of Internet services in public access points and, what is more important, amendments to the main Russian statute regulating information technologies: Federal Law No. 149-FZ "On Information, Information Technologies and Protection of Information" (hereinafter – "Law on Information")[3].

These amendments may be divided into two parts: one relating to bloggers and another one to all other persons, which «organize dissemination of information in Internet». The first part, which was most widely discussed in blogosphere, pursues the goal of equalizing the legal status of popular bloggers (with more than 3000 views per day) with Mass Media and imposing obligations similar to those, which Mass Media has viz specifically, to be responsible for the accuracy of information published, to register with Russian supervisory authority in IT-sphere ("Roskomnadzor"[4]), to reveal true identity and provide contact details for sending communications relevant in law. Something similar was adopted in China as early as 2005, when all bloggers with independent web sites were required to register with the Government[5].

The second part directly relates to data localization requirements. A new legal status has been introduced, named as "*Organizer of dissemination of information in Internet*" (hereinafter – "Organizer"), which is defined as:

> *any person, facilitating functioning of information systems and/or computer programs, which may be used and/or are used for receipt, transfer, delivery and/or processing electronic messages of the users in Internet. (Article 10.1 of the Law on Information)*

Once it is established that a certain Internet-service falls within the definition of "Organizer", such person has to fulfil a number of obligations: to notify Roskomnadzor; to store user's traffic and other specified data for six months in Russia; and to cooperate with Russian law enforcement agencies (mostly Federal Security Service) by granting them access to the stored data upon request. Failure to comply with such obligations may lead to fines and blocking access to the web site of such Organizer.

As it may be seen, the definition of "Organizer" is formulated rather vaguely, allowing the inclusion in its scope of almost anyone associated with Internet service, even vendors of server hardware and software. Some further guidance is provided in subordinate regulations: Decree on Data Retention and Storage[6]. It contains a narrow approach, specifying that special data retention obligations associated with the status of Organizer apply only to providers of "communication Internet-services" understood as an:

> *information system and/or computer program that is used or may be used for receipt, transfer and/or processing of electronic messages between Internet users, including for sending messages to the general public.*

According to this definition, Organizer is understood to be a person providing the services that allow Internet users to communicate *with each other*. Such an approach narrows the practical application of the legal regime of "Organizer" to such ISPs as social networks, providers of public e-mail, providers of collaboration/storage cloud services, providers of forums and other discussion groups. This narrow approach is used in the day-to-day practice of the Russian supervisory authority ("Roskomnadzor") as well.

As of July 1, 2014, there were around 60 Organizers registered with Roskomnadzor, which represent major Russian Internet platforms, providing users with communication facilities, among which are: public e-mail services of Mail.ru, Yandex and Rambler; social networks VKontakte and Odnoklassniki; free hosting/web-site configurator service uCoz.ru; cloud storage service YandexDisk; some of the biggest news aggregators with user discussion functionality. There are no foreign Internet businesses, since none have a physical presence in Russia yet. However, Roskomnadzor is conducting extensive discussions with foreign communication Internet-service providers with the intent to facilitate their compliance with the law. Whether many foreign companies will comply with this law yet remains to be seen. For now, it is possible to conclude that addressees of the second wave of data localization are *Internet communication services operating in Russia*.

The list of the data subject to local storage requirements is provided in the Decree on Data Retention and Storage. It

[2] Section 3.6 of Regulation of Central Bank of Russia No. 397-II of 21 February 2013.

[3] In practice, these amendments are usually designated/referred to by the number of the amending law (Federal Law No. 97-FZ).

[4] The Federal Service for Supervision of Communication, Information Technologies, and Mass Media. URL: http://eng.rkn.gov.ru

[5] China orders bloggers to register with government // The Guardian, 7 June 2005 http://www.theguardian.com/media/2005/jun/07/chinathemedia.digitalmedia.

[6] Decree of the Government of the Russian Federation No. 759 of 31.07.2014.

includes several types of data: i) data about user; ii) data about electronic communications occurred and iii) information about electronic payment transactions. Actual content of the communications is exempted from data storage requirements.

Taking into account that, from a legal perspective, most of the information which has to be stored by Organizers falls within the definition of "personal data", this relates to individuals, which can be directly or indirectly identified by means of it[7]. So, it is possible to argue that Federal Law No. 97-FZ has established a *regime of partial local storage of personal data*, thus preparing the ground for subsequently adopting Federal Law No. 242-FZ on full local storage and processing of personal data of Russian citizens. (This will be reviewed later in this paper.)

However, it needs to be mentioned that Federal Law No. 97-FZ does not require that the data are stored exclusively on the territory of Russia. In other words, it does not prevent data from leaving Russia by prohibiting its processing abroad. The law only requires that the copy of it is stored locally. That seems to be logical taking into account the main purpose of this law: facilitating investigatory activities without jurisdictional complications. For such purpose, it is enough to facilitate availability of relevant data to local authorities: exclusive storage of data in Russia seems to be an excessive measure.

Generally, Federal Law No. 97-FZ can be perceived as a legislative response to the convergence of Internet services and traditional telecommunication providers[8]. Historically, telecommunication operators were subject to multiple regulations, facilitating investigatory activities (e.g. as one of the conditions of their telecom license was that they have to implement special wiretapping infrastructure ("SORM") and provide relevant information upon request to authorized law enforcement agencies). However, in the modern era, where communications in the Internet environment become more and more common, limitation of those obligations to traditional fixed/mobile operators is no longer adequate. There are more and more voices in favour of the position that services of similar value and purpose need to have similar treatment, at least in critical matters. Of course, data retention obligations could be introduced without the localization requirements, but in such cases, Russian law enforcement authorities would lack enforcement teeth when such data are stored abroad. In such cases, special mutual legal assistance treaties should be followed, which provide lengthy procedures and discretion to the other party. So, absent other efficient enforcement mechanisms, localization of such data becomes an essential element of national sovereignty. But its limitation to traffic data and one type of actors (communication Internet-services) is not enough to make it efficient. Something more universal is needed; thus, the third wave of data localization has been introduced.

Such third wave is represented by the Federal Law No. 242-FZ, which supplemented Federal Law No. 152-FZ "On Personal Data" with a very controversial obligation. Data controllers, while collecting personal data of Russian citizens online, are obliged to store and process such data in databases located within the territory of the Russian Federation.

The Draft of Federal Law No. 242-FZ was prepared and adopted very quickly: it was submitted to the State Duma (lower house of Russian parliament) at June 24, 2014. On July 4, 2014, it was approved by State Duma, and on July 9, it was approved by the Federal Council (upper chamber of Russian parliament). On July 21, 2014, the President signed it. Explanatory materials accompanying the draft contain little information regarding the motives or justification of the proposed regulation. It simply states that the law is aimed at enhancement of the existing procedures of processing personal data and is "in line with the case law of European Court of Human Rights", referring to the decision of European Court of Justice of May 13, 2014[9]. Evident confusion of European Court of Justice with European Court of Human Rights illustrates the haste that accompanied the preparation of the draft and formal approach to its justifications. What can be said with absolute confidence, however, is that it will be adopted regardless of the presence or absence of persuasive arguments in its favour.

Regardless of all the circumstances surrounding the process of drafting and adoption of the Federal Law No. 242-FZ, the result is evident: Russia has introduced unprecedented regulation in the sphere of personal data protection.

2. Overview of Russian personal data localization law and its existing interpretations

The well-known truism that "the devil is in the detail" perfectly applies to the matters of practical implementation of data localization provisions and their alignment with the rest of the corpus of data protection laws. It is one thing to proclaim data localization provisions and quite another to make them work. Not surprisingly, initial feedback on the data localization concept was very sceptical because of the difficulties of its alignment with the possibility of transborder data transfer and jurisdictional issues, associated with potentially exorbitant scope of application of this law. Many other questions were raised, driven by the novelty of the data localization concept and interpretation of the "letter of law", which most experts consider to be poorly drafted. However, in the year between the adoption of the law and its effective date (September 1, 2015), as a result of hot discussions between regulators and business community, interpretations were developed, which make the data localization regulations even if not perfect, but at least feasible.

[7] In accordance with the position of ECJ, retention of data constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements. See: ECJ, Case C-293/12, Digital Rights Ireland and in Case C-594/12 Kärntner Landesregierung and Others. 8.04.2014.

[8] For more details, see Digital Convergence Policy and Regulatory Issues. Working Party on Communications Infrastructure and Services Policy. DSTI/ICCP/CISP(2015)2, 2 June 2015.

[9] C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (ECJ 13 May 2014). In this controversial decision, ECJ found that Google was a data controller and could be obliged to remove links to webpages published by a third party in order to protect an individual's so-called "right to be forgotten".

This section will be dedicated to the analysis of the details of application of data localization requirements within the scope of Russian personal data legislation, which is mostly based on Council of Europe Convention № 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 to which the Russian Federation is a party to.

According to the newly introduced section 18(5) of the Russian Law on Personal Data, "data controllers when collecting personal data of Russian citizens online or offline, are obliged to record, systematize, accumulate, store, update, change and retrieve such data in databases located within the territory of the Russian Federation, except as indicated in subsections 2,3, 4,8 of Section 6(1) of the present law"[10].

In order to understand the mechanism of application of data localization provisions, it is necessary to split it into the following components and provide their interpretation:

(1) *the "triggers" of its application*: i) "collection" of ii) "personal data" of iii) "Russian citizen", performed or arranged by the iv) data controller, which is subject to the jurisdiction of Russian Law on Personal Data;
(2) *the scope of obligation imposed*: types of processing, which have to be localized; correlation with transborder transfer provisions;
(3) *statutory exemptions;*
(4) *enforcement and liability.*

Let's consider these elements in more details.

2.1. *The "triggers" of data localization provisions*

One of the first question, asked by most companies and their associations, is when exactly do data localization requirements apply and which business-processes of the company fall within these requirements. The answer on this question depends on multiple factors.

2.1.1. *Information at hand should qualify as "personal data"*

Russian Law on Personal Data contains rather broad definition of personal data, according to which it is "any information, relating to directly or indirectly identified or identifiable individual (data subject)". As a result, much (if not all) data contains information that can be construed as personal data. Besides, in reality, there is no technical or legal way to separate personal data from non-personal mechanical information. Any transaction on the Internet made while logged in to an account may amount to personal data, and even the most harmless pieces of company data may contain information about the employee. Since such a broad approach to personal data makes enforcement of the law almost unmanageable, in its day-to-day practice, Roskomnadzor follows narrower approach to the definition of personal data. According to it, information is considered personal, if it meets two criteria: 1) it identifies *specific* individual, and 2) such precise identification is possible either from the data at hand itself or from this data and other information in the possession of the data controller[11]. Moreover, information constituting identifiers, assigned to a specific person by a state (passport number, social security number, taxpayer number, etc.), is assumed to be personal data in all cases, although may is difficult to identify a person based only on such number, without access to a database with information matching this number to the particular person. Thus, all information related to the individual, which allows to identification of her/him, is potentially within the scope of localization requirements, unless there is only one element of personal data at hand, for example, first and last name or e-mail address, or phone number, etc. But any combination of two or more such elements or the presence of the state-assigned identifiers brings all the data within the scope of localization obligations. Unfortunately, not all the information may be clearly qualified as personal or non-personal by using such an approach. The status of user-generated content, dynamic IP-addresses, nicknames in online games, and other types of information that potentially may be linked with a particular individual is in grey area [12].

2.1.2. *Personal data should be "collected"*

It means that such data should be received as a result of purposeful and direct interaction of operator (or its agent) with the data subject. Personal data received from third parties (e.g. from the employer of the data subject) is not subject to localization by its recipient, since it is assumed that such employer should have already localized it. As also clarified by Roskomnadzor and Russian Ministry of Communications, accidental receipt of personal data (e.g. in e-mail from data subject) does not amount to "collection". Similarly, a provider of IaaS cloud services does not perform collection with regard to personal data, put by its client in the cloud; therefore, such "data in the cloud" is not subject to localization by the cloud provider; however, the client of the cloud provider, being a data controller, may still be subject to data localization

[10] This section was introduced by the Federal Law No. 242-FZ, which is most common designation of the data localization provisions.

[11] This narrow approach is not formalized somehow, though. However, some traces of it can be found in the text of non-official commentary, prepared by the group of authors from Roskomnadzor. See: Commentary on the Federal Law No. 152-FZ "On Personal Data" [in Russian] /ed. by the deputy head of Roskomnadzor A.A. Priezzheva. "Russian gazette", Moscow, Vol. 11, 2015. P. 15–17. As it may be seen, described approach is rather close to the definition of personal data contained in the UK Data Protection Act of 1998. In accordance with section 1(1) of this act, "personal data" mean data which relate to a living individual who can be identified – (a) from those data or (b)from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

[12] European authorities experience similar difficulties in assessing the status of such information. For example, on October 28, 2014, the German Federal Court of Justice referred the question of whether a dynamic IP address constitutes personal data under the EU Data Protection Directive 95/46/EC to the European Court of Justice. The approaches of national courts to the status of dynamic IP addresses diverge. The Irish High Court decided that IP addresses do not amount to personal data under the terms of the Irish implementation of the Data Protection Directive (EMI & Ors v Eircom Ltd [2010] IEHC 108). The French Constitutional Court, when deciding the question on constitutionality of Hadopi law, held that IP addresses constitute personal data (Décision No. 2009-580 DC du 10 juin 2009).

requirements[13]. Linkage of data localization requirements to some kind of purposeful and clearly defined action of a data controller is aimed to provide a degree of predictability to the overall mechanism and avoid its potentially overreaching scope of application.

2.1.3. *Collected personal data should be linked with Russian citizen*

The practical application of this requirement is rather complicated and tricky. It is generally quite unusual to limit the scope of application of personal data laws by the nationality principle. European data protection legislation, which treats protection of personal data as a fundamental human right, is nationality-neutral. As Working Party 29 clarified:

> *. . .Nor would it be acceptable to reduce the scope of protection to persons residing in the EU, since the fundamental right to protection of personal data is enjoyed regardless of nationality or residence*[14].

Attempts of some European countries to introduce a narrower, country-specific approach were not successful. According to Kuner, Greece once tried to follow a nationality-based approach in application of its data protection legislation, by requiring data controllers operating outside Greece, who processed data of Greek residents to appoint a representative in Greece, who would be liable for such processing. These provisions were later changed following the objections by the European Commission[15].

But even apart from the fundamental rights considerations, it is very difficult to link the application of data protection legislation to the nationality of the data subject. Most data operators, especially those collecting and processing personal data via the Internet, do not have information relating to the nationality of data subjects. Such information is irrelevant for the provision of most Internet services. But even if some kind of additional field in the registration form is introduced, reflecting the nationality of the user, there is no guarantee that the information provided is correct, unless a burdensome procedure of verification of user passports is introduced which is not feasible in most cases. Roskomnadzor understood the magnitude of the problem and decided to entrust its solution to data controllers themselves.

According to the interpretations provided, it is up to data controllers to define how they will identify the citizenship of the data subject. However, in case of doubt, it is possible to localize all the personal data collected on the territory of Russia and remain compliant[16]. So, Roskomnadzor basically substituted a nationality criterion with the residence one as more convenient both in practical application and enforcement. It is also more coherent with the general Russian approach granting "national treatment" to foreign persons[17]. Besides, this approach also means that data localization requirements do not apply to personal data of Russian citizens collected outside Russia (e.g. from Russian citizens who are living outside Russia). What leads to a more adequate jurisdictional reach of the Russian data protection law will be discussed in more detail later. Generally, as Russian experience shows, it is not feasible to structure personal data localization requirements based on citizenship criteria, although it may have some populist advantages for politicians lobbying for such laws.

2.1.4. *Collection of personal data of Russian citizen is performed or arranged by a data controller*

In accordance with Russian Law on Personal Data, the data controller ("operator" in terminology of Russian law) is the natural or legal person, state or municipal authority, processing personal data solely or jointly with other persons and determining the purposes of such processing, scope of personal data and means of processing. So, data processors, acting in the interest of data controller and in accordance with existing agreements, are not subject to data localization obligations themselves. The data controller is liable for their activities. Therefore, if a transnational company, acting as a data controller, has a global IT-outsourcing agreement with a foreign company, and is a provider of these services, as a part of its obligations, then collects and processes personal data of Russian clients of transnational company, such company is liable for non-compliance with Russian law on Data Protection, not the service-provider.

Data localization obligations apply to all data operators without industry-based exemptions. Although initially there were discussions to limit localization requirements only to Internet-businesses as the source of most risks, associated with misuse of personal data in the digital economy, such an approach was considered unsatisfactory as discriminating and difficult in application.

Finally, it is necessary to emphasize that not any person formally falling within the definition of "data controller" is subject to data localization requirements of Russian law, but only the person falling under the jurisdiction of Russian laws. Jurisdictional aspects of Russian Law on Data Protection will be considered later on in detail.

2.2. *The scope of data localization obligations*

Once it is established that data localization provisions are triggered, the data operator has to ensure that such types of processing as "recording, systematization, accumulation, storage, updating, changing and retrieving" of such data are performed in databases located within the territory of the Russian Federation. Such types of processing as usage,

[13] While supporting the result of the clarifications, I think that it would be more appropriate to say that IaaS cloud service provider is not a data controller, rather than just saying that it does not perform "collection" as one of the methods of processing. But anyway, any approach recognizing the specifics of cloud services is a big step to recognizing the sui generis status of IaaS cloud providers, advocated by Christopher Millard and others. See: Cloud Computing Law / ed. by Christopher Millard. Oxford University Press. 2013. P. 193–220.

[14] Article 29 Data Protection Working Party. Opinion 8/2010 On Applicable Law. 16 December 2010. P. 24.

[15] *Christopher Kuner*, Data Protection Law and International Jurisdiction on the Internet (Part 1) // International Journal of Law and Information Technology. Vol. 18 No. 2, 2010. P. 189.

[16] § 5 of Letter of Roskomnadzor No. 08АП-3572 of 19 January 2015.

[17] Article 2(1) of Civil Code of the Russian Federation.

dissemination, depersonalization, blocking, erasure, destruction are not on the list of types of processing, which are subject to localization. Therefore, they can be performed elsewhere. Provision of remote access to local database is not prohibited either.

The data controller is also obliged to notify Roskomnadzor about the location of its primary databases, unless such controller falls within one of the notification exceptions, as indicated in Section 22 of Russian Law on Personal Data (e.g. it processes only personal data of its employees or clients under the contract without further transfer of such personal data to third parties; processes personal data necessary for facilitating one-time access to the controller's premises, etc.). The presence of such notification obligation is essential for performance of compliance audits by Roskomadzor.

But one of the most critical questions relating to the scope of data localization obligations is whether transborder transfer of personal data of Russian citizens is allowed, and if yes, how to align it with data localization requirements.

From the very beginning, it was not clear how the wording of the law may co-exist with the remaining opportunity to transfer personal data abroad. If storage of personal data should be arranged on Russian territory, then transborder transfer is not possible since, from technical point of view, the transferred data will inevitably be stored at least for some period of time on a server located somewhere abroad. Besides, transborder transfer is usually accompanied with such types of processing on the side of recipient as "systematization and retrieval"; otherwise, it will be impossible to work with the received data.

The question was further complicated by the statements of the Russian officials, according to which data localization regulations are intended to prevent misuse of personal data of Russian citizens by foreign data controllers and to protect Russian citizens from the surveillance of foreign states[18]. Assuming that it is so, the right to transfer personal data abroad, especially in countries not providing adequate protection, seems to be at odds with the stated purposes. How can personal data localization requirements protect from all those risks, if after all personal data can be still transferred and processed abroad, without any control by the Russian authorities?

However, the Russian data protection authority (Roskomnadzor) managed to find a solution enabling co-existence of data localization and transborder transfer of personal data. The essence of the solution is to divide all the databases that may contain personal data into two groups: *primary databases* and *secondary databases*. The database where the personal data should be *initially* recorded into, as well as stored and updated at a later stage, must be located in Russia (the "primary database"). After that, information from such "primary databases" can be transferred to databases located outside of Russia ("secondary databases"), subject to provisions of the Law on Personal Data related to transborder transfer.

In other words, a master copy of personal data of Russian citizens, collected in Russia, should be located in Russia, as well as subsequent updates and additions to that personal data. Technical solutions where the primary database is located abroad, and only a Russian copy ("replica" or "mirror") of such foreign database is created, are not in line with the law. What it means for companies and what are the potential reasons for such an approach from the perspective of Russian government will be discussed in subsequent sections of the paper.

Provisions on transborder transfer of personal data in Russian Law on Personal Data are generally similar to those in Directive 95/46/EC. The conditions of transfer of personal data to a foreign jurisdiction depend on the level of protection of personal data, which such jurisdiction has. If it can be considered as "safe harbour" jurisdiction, providing "adequate" protection (countries, which are the parties to the Council of Europe Convention 108, and those states, which are considered as providing an adequate level of data protection by the decision of Roskomnadzor[19]), transfer of personal data to such "safe harbour" states does not require additional consent in a written form and is generally permitted, subject to the general provisions of Russian Law on Data Protection (e.g. the presence of specific and informed consent for processing personal data).

Transfer of personal data to the country, which does not provide for an adequate protection of data subjects' rights, may take place with the prior written consent of the data subject or in limited cases without such specific consent, for instance, in the context of the performance of an agreement with the data subject.

2.3. *Statutory exceptions*

Section 18 (5) of the Russian Law on Personal Data containing data localization obligations includes four exceptions. All of them are structured by means of reference to some grounds of processing of personal data without consent of a data subject, listed in Section 6, specifically, to its subsections 2, 3, 4 and 8:

(1) processing is required for meeting the goals of international agreement or statute, or for the purposes of compliance with obligation imposed on data controller by the Russian legislation (subsection 2);
(2) processing of personal data is performed for the purposes of law enforcement (subsection 3);
(3) processing of personal data is performed by government agencies authorized in a course of provisions of public services (subsection 4);

[18] Savelyev A. Data localization laws and their potential impact on E-commerce in Russia [in Russian] // Zakon. Vol. 9, 2014. P. 51–68.

[19] In accordance with the Order of Roskomnadzor No. 274 of 15 March 2013 (as amended by the Order No. 152 of 29 October 2014), among such countries are: Australia, Israel, Canada, Morocco, Malaysia, Mexico, Mongolia, New Zealand, Angola, Benin, Cape Verde, South Korea, Peru, Senegal, Tunisia, Chile. Accordingly, such countries as USA, China, Japan and other are not considered as providing "adequate" level of protection of personal data. The criteria which Roskomnadzor uses for assessment are not formalized, but from personal sources the author knows, that there are three of them: 1) the presence of legislation, based on the same principles as reflected in CE Convention No.108; 2) the presence of special government agency, responsible for supervision in this sphere, which cooperates with Roskomnadzor, and 3) the presence of liability for breach of personal data legislation.

(4) processing is performed by Mass Media or journalists in the course of performance of their professional activities, or in the course of scientific or other creative activities, if rights and legitimate interests of data subject are not harmed (subsection 8).

The list of exemptions from the requirement of local personal data storage is a closed one and is covering situations, relating to the public sphere. There are no exemptions specifically addressing the private sphere, e.g. the list does not include such vital e-commerce exceptions as processing personal data for the purposes of performance of a contract to which the data subject is party. Nor does such a list contain an exception for personal data that were made publicly available by the data subject himself, an exception relevant for social networks and blogging platforms. Finally, the situations where processing is performed based on legitimate interests of the data controller are also not covered by the exemptions to local storage obligations. Therefore, most of the operations of Internet businesses are not exempted from the data localization requirements.

The most valuable exemption on the list relates to situations where processing is required for meeting the goals of international agreement or statute, or for the purposes of compliance with obligations imposed on data controllers by the Russian legislation (subsection 2). The most evident example is processing by financial institutions of personal data of their clients, in accordance with the provisions of Federal Law No. 115-FZ of 7 August of 2001 "On combating money laundering and terrorist financing activities". Another example relates to the sphere of civil aviation, which is governed by the Russian Air Code and a number of international conventions to which the Russian Federation is a party to[20]. According to the clarifications of the Ministry of Communications of Russia, since air carriers have to process personal data of the passengers for the purposes of performance of their obligations and ensuring security of flights and passengers, such processing can be performed abroad. This exception is also applicable to the agents of air carriers, e.g. to reservation systems. However, if air carriers and their agents are involved in other types of activities, having a complementary nature (e.g. such as provision of hotel booking services), they are subject to the data localization requirements on a general basis. However, since this exception applies mostly to those of a public nature rather than private relations, it does not apply to processing driven by the existing contractual relations in its core, e.g. to situations where a seller processes personal data of a consumer as a part of its statutory warranties or where an employer processes personal data as a part of existing labour obligations.

As the analysis of the scope of exemptions from data localization requirements shows, application of this mechanism is not dependent somehow on the will of the data subject, in contrast to, e.g., the Malaysian Personal Data Protection Act of 2010, which established localization requirements but still permits transfer of personal data abroad if the data subject has given their consent for transfer abroad[21]. Even if he is fully aware about the potential risks of processing his personal data abroad and is ready to accept them, it is not possible, since data localization provisions are mandatory and override all the possible private agreements between data subject and data controller. It may look like excessive paternalism and intrusion in the private sphere of an individual, but in the era of universal use of privacy, policies suggested a "take-it-or-leave-it" basis; this other approach would effectively negate data localization obligations, since it would be very easy to bypass them by updating privacy policies with relevant provisions. In reality, there is no feasible alternative to the mandatory nature of data localization requirements (subject to a narrow list of public policy driven exemptions), if government wants to ensure that they work in practice *and there are no economic or other incentives that could ensure compliance with them on voluntary basis*.

2.4. *Enforcement and liability*

Enforcement authority is vested with Roskomnadzor, whose powers were substantially expanded by Federal Law No. 242-FZ. Roskomnadzor performs its supervisory activities in several forms, including the old ones, such as audits of data controllers, and a new one: systematic monitoring of the Internet. Audits can be either documentary, where only documents relating personal data processing are requested and analyzed, or onsite, where apart from documents, IT-infrastructure can be checked as well as other aspects of personal data processing. Audits can also be scheduled, when the audited company is included on the special list available on the Roskomnadzor's website and valid for the relevant year[22], or unscheduled, when an audit is initiated with 24-hour prior notice of the data controller (usually based upon a data subject's complaint)[23]. In the latter case, relevant violations can be revealed by the Roskomnadzor's official himself, without prior interactions with a data controller. Among the possible grounds for performance of audits is information about possible violations, which is circulating in Mass Media, and complaints of data subjects. Roskomandzor also received a right to engage experts for performance of onsite audits, since analysis of IT-infrastructure and information flows require deep expertise, which ordinary officials usually lack. If any non-compliance is found, Roskomnadzor is obliged to issue a prescription to fix it with an indication of specific measures which need to be taken. Thus, the degree of certainty is increased since the data controller will be able to work out an action plan to

[20] e.g. Convention on International Civil Aviation 1944 (Chicago Convention), Convention for the Unification of certain rules relating to international carriage by air 1929 (Warsaw Convention) and others.

[21] Article 129 (3)(a) of Personal Data Protection Act 2010, No. 709. URL: http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.

[22] The most likely candidates for inclusion on the list of scheduled audits are those companies, which fell "on the radar" of Roskomanzor as a result of submission of notification to it on performance of personal data processing operations, which do not fall within the list of exemptions indicated in Section 22 of Russian Law on Personal Data.

[23] Draft of Regulations on the procedure of State control and supervision for the compliance with personal data protection requirements of the legislation of the Russian Federation approved by the Decree of the Government of the Russian Federation. It is expected to be adopted in the beginning of 2016.

implement them, without guessing what exactly was the reason for dissatisfaction of the DPA. Roskomnadzor is also entitled to issue a binding order to suspend or terminate processing.

Failure to comply with data localization obligations may lead to a number of consequences. One of them is an administrative fine, which may be imposed on legal entities for violation of the general rules of collection, storage, use or distribution of personal data that amounts to RUB 10,000[24] (approx. $175). Of course, such fines can hardly be regarded as an efficient deterrent of unwanted behaviour, especially comparing to the costs of localization of personal data processing processes. Currently, the amount of fine and wording of specific types of violation of data protection legislation is under reconsideration in the Russian parliament and may be increased. No criminal liability is established for violation of data localization provisions and personal data legislation provisions in general.

However, the main risk of non-compliance with new data localization provisions is represented by the new provisions on blocking access to web sites. Federal Law No. 242-FZ also empowered Roskomnadzor to block access to web sites, containing information which is being processed in breach of Russian data protection legislation. Network addresses (IP addresses and/or domain names) of such Internet services are included in a special Register maintained by Roskomnadzor, while the data controller is included in a special black-list of companies, violating data protection legislation.

This provision is, perhaps the strongest incentive for companies, valuing their reputation, to comply with the new law. As Uta Kohl aptly puts it, "The fact is that being perceived as a law-breaker is not good for business"[25]. As Kuner further explains, "soft" penalties such as adverse publicity are an important incentive to comply with data protection law, since damage to a company's reputation can ultimately cause it more harm in the marketplace than can a fine[26]. So, associated reputational risks of being blacklisted and "tagged" as a violator of data protection legislation with subsequent negative publicity force many foreign companies, especially public ones, to consider compliance with new data localization provisions seriously.

Taking into account that most of the Internet companies are out of the jurisdictional reach of the Russian government authorities, blocking access to their web sites by means of local intermediaries seems to be the most effective way of enforcing exterritorial application of the law. As Goldsmith and Wu note: "With few exceptions governments can use their coercive powers only within their borders and control offshore Internet communications only by controlling local intermediaries, local assets, and local persons"[27].

2.5. *Jurisdictional scope of Russian law on data protection*

Whether or not Russian Law on Personal Data and particularly its new data localization requirements apply to foreign data operators, if that is so, then on which conditions? These questions were among the top ones for almost a year between the adoption of Federal Law No. 242-FZ and its effective date during discussions within the business community. Ironically, prior to Federal Law No. 242-FZ, jurisdictional aspects of personal data legislation were not of much concern for international market players and regulators. The former perceived Russian personal data legislation to be something on the periphery, not worthy of serious attention, especially in light of the amounts of fines for its violation. The latter was trying to enforce its provisions at least with regard to domestic data controllers; there were no resources, desire or directions from the above to apply it to companies acting outside Russia. Data localization provisions changed the attitude of the business community to personal data legislation in general and provoked massive interest and desire to ensure compliance with it.

But from the very beginning, lots of criticisms were directed at the data localization provisions on the ground that these are overreaching and make the entire world non-compliant with it. It was argued that small hotels say, somewhere in Austria, processing personal data of Russian tourists or Oxford university processing personal data of Russian students will hardly involve servers in Russia for those purposes. These arguments were further heated by the concerns expressed in blogosphere, that Roskomnadzor would start massive blocking of access to foreign web sites because of their non-compliance with data localization provisions. It is evident that the key question here is not whether data localization requirements are applicable as such from the jurisdictional perspective, but what is the territorial scope of the application of Russian Law on Personal Data, including those data localization obligations. The answer to this question will define whether such 'absurd-looking' situations fall within the ambit of the law, or not.

Russian Law on Data Protection does not contain any specific provisions governing its territorial scope and potential application to foreign persons. Its section 1, dedicated to the scope of the law, the provision just says that it governs automatic and non-automatic personal data processing, performed by federal, regional and municipal authorities, natural or legal entities and lists some activities, exempted from the scope (processing for personal use such as processing of information constituting a state secret, or processing of information subject to regulations on archives). Foreign persons are not specifically mentioned in the text, unlike what is done, e.g., in the Singapore Data Protection Act of 2012[28]. However, since personal data legislation contains both public law provisions (e.g., relating to the authority of DPA and enforcement

[24] Article 13.11 of the Code of Administrative Offences of the Russian Federation.

[25] Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity*. Cambridge University Press. 2007. P. 208.

[26] Christopher Kuner, *The "Internal Morality" of European Data Protection Law,* (November 24, 2008), P. 9 *available at* http://ssrn.com/abstract=1443797.

[27] Jack Goldsmith & Tim Wu, *Who Controls the Internet?* Oxford University Press, 2008. P. 159.

[28] The definition of «organization», provided in this law includes «any individual, company, association or body of persons, corporate or unincorporated, whether or not — (a) formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore» (Section 2(1)).

procedures) and civil law ones (e.g., relating to consent requirements, agreements between data controllers and processors, etc.)[29], it is possible to refer to the provisions of the Russian Civil Code, according to which foreign persons enjoy national treatment, unless otherwise is provided in the law (Article 2(1)). So, even in the absence of explicit reference to foreign companies in the Russian Law on Personal Data, there are no reasons to limit it only to national data controllers. This is exactly what the Russian Ministry of Communications did in one of its early responses on private requests for clarifications. It maintained a position that since Russian law applies only on the territory of the Russian Federation, it does not apply to foreign companies and nationals, and applies only to Russian individuals, companies and public authorities, including those, which process personal data abroad.

However, not everyone shared that approach, as it creates a basis for law evasion and shifts the burden of compliance mostly on Russian-based data controllers, since they are cut off from access to cheap hosting services and have to incur extra costs for reconfiguring their infrastructure, what inevitably will be reflected in their competitive position.

Thus, there was a need for balanced criteria which, on the one hand, would provide a sufficient degree of certainty and predictability, allowing market players to foresee the possibility of application of personal data legislation, while, on the other, would provide a necessary degree of application flexibility, thus minimizing the temptations for law evasion. Such criteria should take into account the specifics of Internet architecture: it is a global network based on protocols without regard to national borders, where information is routed across the network based on automatic decisions driven by efficiency.

To develop such criteria, a special working group within the Advisory Board of Roskomnadzor was created. The group consisted of the representatives from the leading Russian universities, legal consulting companies, business community, and was headed by the author[30]. The results of this work were reflected in a report[31] and official interpretations of Federal Law 242-FZ, provided by the Ministry of Communications of Russia[32], the summary of which is provided below.

The working group based on the performed analysis of various approaches to definition of the territorial scope of data protection legislation (accessibility, country of origin, equipment-based, targeting) came to the following conclusions.

While having some value in criminal jurisdiction by allowing policing of serious crimes committed via Internet from abroad, accessibility of web sites on the territory of a particular country is quite unsatisfactory as a factor for defining the jurisdictional reach of data protection legislation, since it leads to exorbitant jurisdiction. Associated enforceability problems leading to mass-scale non-compliance, undermining the law's and regulator's credibility, are also evident.

It was also concluded that a country of origin approach, as initially proposed by the Ministry of Communications, and which assumes that a data controller has to comply with data protection legislation of the country of its establishment (incorporation), works well only when data protection legislation of countries for which it is applied is highly harmonized and there is an established effective cooperation between their data protection authorities. Otherwise, the country of origin approach may lead to "forum shopping" and choosing the most favourable jurisdiction for data controller. Since personal data localization requirements are unique for Russia and do not have analogies in other countries[33], and compliance with them is associated with certain costs, the country of origin approach for Russia would mean a massive exodus of data controllers from Russia to foreign countries. So, the effect of the data localization law could be the exact opposite to what was intended, just because of the outdated approach to handling of jurisdictional matters concerning the Internet.

The equipment-based approach similar to the one provided for in Article 4 (1)(c) of Directive 95/46/EC, establishing the application of data protection laws of the country where data controller uses equipment for the purposes of processing personal data, was also considered unsatisfactory. Although, at least at the first glance, such an approach may seem to be a good compromise between traditional territory-based jurisdictional criteria and new technological realities, it was considered to be too complex in application. It took into account that as European practice shows, it is difficult to provide a clear definition of "equipment" (e.g. whether user's equipment with cookies installed may amount to "equipment" used by data controller). It is also difficult to trace the exact location of equipment used in cloud environment. Besides, an equipment-based approach may lead to undesired and unexpected results of application of the country's personal data law to processing which has no real connection with such country (e.g. EU law may be applicable in situations, where a Singaporean

[29] For details see: Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)* // 18 Int'l J.L. & Info. Tech. 2010. P. 181–183.

[30] The following members of the working group, who provided valuable contributions need to be especially mentioned: Vadim Plekhanov (Ph.D., associate professor of the faculty of law of Moscow State University), Elena Voinikanis (Ph.D., associate professor of the faculty of philosophy of Moscow State University, GR executive of Rostelecom company), Vadim Perevalov (associate of Baker & McKenzie, Moscow), Ludmila Terentieva (Ph.D, associate professor of Moscow State Law Academy), Vladislav Arkhipov (Ph.D., associate professor of the faculty of law of Saint-Petersburg State University, counsel at Dentons, Saint-Petersburg).

[31] Currently, this report is for Roskomnadzor internal use only. However, there are plans to publish it on the official web-site of the Roskomnadzor.

[32] The text of interpretations (in Russian) is available on official website of the Ministry of Communications of Russian Federation via the link: http://www.minsvyaz.ru/ru/personaldata/.

[33] Data localization requirements are presented in legislation of some other countries, e.g. in Australia, India, Malaysia, Vietnam (see generally: A. Chander, U. P. Le, Breaking the Web: Data Localization vs. the Global Internet, Working Paper 2014-1, California International Law Center, 12.03.2014. P. 28–30. http://ssrn.com/abstract = 2407858). However, neither of them are as general and comprehensive as in Russia and backed up with specific enforcement mechanism, such as DPA's audits with the possibility of outside experts involvement and website blocking provisions.

company processes personal data of Singaporean residents, using cloud services of a provider with the data centre located in the Netherlands)[34]. In Russian realities, the equipment-based approach to jurisdiction of personal data legislation also creates a basis for evasion of such laws, by moving processing activities offshore.

As a result, the working group came to the conclusion that a targeting approach for definition of the scope of jurisdiction is the most appropriate one with regard to the objectives set. When a data controller purposefully directs its activities on the territory of the Russian Federation and extracts benefits from such activities, such benefits should be accompanied with corresponding obligations of compliance with the laws of the Russian Federation. Therefore, a fine-tuned targeting approach may provide a degree of certainty and predictability, allowing market players to foresee the possibility of the application of Russian personal data legislation to their activities, while on the other hand providing a substantial degree of flexibility, allowing it to address new trends in the IT-sphere while minimizing the temptations for the legal evasion. Besides, the targeting approach is presented already in the Russian law. Initially, it has been reflected in the Russian Civil Code, which establishes special rules applicable to the choice of law in consumer contracts, pretty similar to those expressed in Section 6 (1) of Rome I Regulation[35]. Recently, targeting approach found its expression in the sphere of information law. The new law the "right to be forgotten", which will be described in more detail later, is applicable to search engines, which direct their ads on consumers located in the Russian Federation[36]. So the "targeting approach" is not something alien to the Russian legal system, and it was not very difficult for the Ministry of Communications of the Russian Federation to put it as a main jurisdictional criterion for the personal data protection legislation.

However, the most challenging objective is to define factors which may serve as evidence of targeting of online activities on the territory of the Russian Federation. After extensive discussions and analysis of foreign experience, the following list of factors has been prepared.

[34] Article 29 Data Protection Working Party. Opinion 8/2010 On Applicable Law. 16 December 2010. P. 29.

[35] Article 1212 of the Russian Civil Code states: «The choice of law applicable to a contract concluded with an individual, using, acquiring or ordering, or having an intent to use, acquire or order tangible good (works, services) for personal, family, home and other needs, not associated with performance of commercial activity, cannot deprive such individual (consumer) of protection of his rights, provided by the laws of the country of the habitual residence of such consumer, if the counterparty of the consumer (the entrepreneur) pursues his commercial activities in such country or by any means **directs such activities** to that country or to several countries including that country, and the contract falls within the scope of such activities».

[36] Federal Law No. 264-FZ of 13 July 2015, 'On amendments to the Federal Law No. 149-FZ "On Information, Information Technologies and Protection of Information" and Articles 29 and 402 of the Code Civil Procedure of the Russian Federation'. The law becomes effective January 1, 2016.

2.5.1. *Primary factors*

2.5.1.1. Usage of geographic domain name, associated with Russian Federation or its regions (.ru, .su, .рф, .moscow, etc.). This approach is already being used by Russian Federal Antimonopoly Service (FAS) for definition of the scope of application of Russian law on advertising[37]. It seems to be justified, since registration and factual use of such geographic domain names can be interpreted as a will of the company to perform its activities "having Russia in mind", due to a strong linkage of such domain names with the territory of Russian Federation. However, if such domain name is registered for protective purposes only (e.g. for prevention of its takeover by a competitors or cybersquatters), and is not accompanied with its factual use, it should not be generally regarded as a "targeted" activity within the Russian Federation.

2.5.1.2. Usage of Russian language. The presence of a localized Russian version of web sites can be regarded as a strong indicator of a targeting of Russian users, regardless which domain name is used (i.e. this criteria is applicable also to web sites registered under functional domain names such as .com, .org, etc.). However, such a presumption can be valid only if translation has been purposefully performed by the owner of a web site himself or by other person, acting under a contract with the owner. Use of automated translation functionality, allowing translation into multiple languages chosen by the user, cannot be a basis for a conclusion that a web site targets the Russian Federation: rather it is possible to argue that it targets an *international audience in general*, without its nationality differentiation. Moreover, if automated translation functionality is implemented by the user himself (e.g. by using special web-browser plugins), subjecting web-site owner to Russian data protection laws (absent other factors, evidencing about the targeting of its activities on Russian Federation) would mean that a legal duty of a person depends not only on the circumstances beyond control of such person, but also on the circumstances, which such person is not reasonably aware of. Such an approach is incompatible with the principles of legal certainty.

Taking into account that the Russian language is widely used in countries other than Russia, and can even be recognized as the official language in some of them (e.g., in Belarus, Kazakhstan, Kirgizstan, Tajikistan), there is a need for secondary, fine-tuning factors. Therefore, in addition to the presence of localized Russian version of a web site, there should be at least one of the following secondary factors in place:

2.5.2. *Secondary factors*

(1) Pricing in rubles;
(2) Availability of Russian phone numbers or Russian toll-free numbers (8–800. . .);
(3) Russia-oriented marketing activities of the web site owner, including usage of keyword advertising or banners in Russian language with a link to a relevant web site;

[37] Letter of FAS No. АК/24981 of 3 August 2012 "On advertising of alcoholic drinks on Internet and print media".

(4) Possibility of conclusion of the contract with a Russian resident and possibility of delivery of goods/digital content in Russia;
(5) Place of services provision. If the service is provided outside Russia (e.g. hotel or education services), it is possible to argue that the customer himself "came" in a foreign jurisdiction by choosing a foreign service provider; thus, there is no reason for the conclusion that the service provider purposefully "came" into Russia, making it a part of its business strategy, unless targeting activities of relevant web-sites follow from other factors evaluated;
(6) Presence of a branch or other local establishment of the company, operating a web site, provided that the activities of such local establishment are directly linked with the activities performed via the web site.

The above list of factors was reflected in official clarifications of the Ministry of Communications of Russia. It is expected that it should provide more certainty both for the business community and for regulators, than just reference to a targeting approach, leaving to define its application for each case on an *ad hoc* basis. How it will be applied in particular cases yet remains to be seen.

3. The reasons behind the adoption of personal data localization requirements in Russia

One of the key questions lying on the surface, while analyzing new personal data localization obligations, concerns the purposes of their adoption. What were the goals the legislator tried to achieve and have they been achieved? Depending on the answers, some predictions about future enforcement can be made, as well locating the key for interpretation of its uncertain provisions.

3.1. *Protection of data subjects*

According to the commentaries made by Russian officials, the main purpose of the law is to provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments[38]. While sounding pompous, such an explanation may seem plausible only for those who disinclined to dig into details. After a closer look, it does not stand up to criticism.

The first problem with such an interpretation is that it rests on an untested assumption that data localization somehow facilitates extra protection of the rights of data subjects. On the one hand, it is possible to argue that data localization facilitates better enforcement and protection of data subjects. Some basis for this kind of argument can be found in ECJ case law. In one of the cases, ECJ stated,

> . . .that directive[39] *does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured.* (Emphasis added – A.S.)

"Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data. . ."[40] It should be noted, however, that this passage from the ECJ decision seems peripheral; thus, it is not clear how much emphasis should be put on this paragraph and whether it is really central to the judgment.

But even if it is true, and data localization indeed facilitates better enforcement, it does not solve the problem of unconscionable practices during personal data processing itself. Nothing prevents transnational companies misusing their rights to process client's personal data from pursuing their questionable activities even if data is localized: it is still under the control of such companies which, as data controllers, define the purposes, means and other elements of the processing mechanism. Especially, it is true if data localization does not prevent transborder transfer of personal data, as is the case with Russian regulation. Even being fully compliant with Russian data localization requirements, data controllers may perform their "dark deeds" with the data after it is transferred into a foreign database of its choice.

It is also doubtful that data localization may prevent or at least make it harder to perform foreign surveillance over Russian citizens. According to one source, it was recognized that data localization is ineffective against foreign surveillance[41]. US NSA and its counterparts in other countries already concentrate much of its surveillance efforts abroad. Moreover, the use of malware eliminates the need to have operations on the ground of the countries where the data are located. Besides, due to data localization, foreign intelligence agencies may concentrate on spying citizens of a particular country more easily, since information gathered together in one place offers a tempting "honeypot"[42]. The only realistic way to remove the risk of foreign surveillance in the Internet is not to connect anything to it. Thus, data localization requirements are hardly a remedy against US surveillance. However, whether it minimizes the risks in this sphere or not is still subject to a deeper research. It is argued that a more appropriate solution to the privacy/security issues would be to encourage the creation and use of de-centralized and end-to-end encrypted services that

[38] See: Interview with the head of Roskomnadzor, Alexander Zharov [in Russian]. 12 November 2014. URL: http://82.rkn.gov.ru/news/news70654.htm.

[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC // OJ L 105/54, 13 April 2006.

[40] ECJ Joined Cases C-293/12 and C-594/12.

[41] A. Chander, U. P. Le, Op. Cit.P. 28–30.

[42] Idem

do not store data in one place[43]. If it is true, then the technical solution, such as sharding[44] used in Cloud Computing, would be less costly and more effective than a legal solution such as data localization regulations.

The second problem with the explanation at hand lies with the role of the data subject's will in defining the legal destiny of its personal data. As was noted earlier, Russian personal data localization provisions have a mandatory nature and cannot be changed by the decision of the data subject, e.g. expressed in their consent. Although such an approach has valid reasons, it is still questionable from a human rights perspective. Assuming that blocking the access to web sites non-compliant with data localization requirements is the main mechanism of protection of Russian citizens, it looks like data localization regulations are "protecting" the privacy of Russian citizens at the cost of minimizing their freedom of choice. Basically, a person is stripped of the ability to control its personal data and define how it should be used (at least assuming that in the age of pre-formulated privacy policies, something still depends on the will of the data subject). At the same time, Russian government officials did not ask citizens whether they approved of such acting in their "best interests". No association representing the rights of the data subjects and no research or survey of Russian citizens' opinions has been conducted. It is possible to argue that mandatory data localization requirements violate constitutional rights of Russian citizens to privacy[45] (the right to control the flow of personal information) and the right to freedom of information[46] (the right to take decisions regarding the dissemination of certain information)[47]. However, the perspectives of recognizing data localization provisions as unconstitutional, on the basis of the above arguments, are rather murky in the present political environment.

For the sake of objectivity, it is necessary to mention that apart from the data localization requirement, some other provisions from the Federal Law No. 242-FZ may enhance the protection of the data subjects. When the data subject is entitled to ask the court to block the web site from processing his personal data in violation of personal data legislation, it both creates extra incentives for compliance for those companies which have something to lose, and creates more or less an efficient remedy against those companies which have nothing to lose.

And such blocking may be justified with reference to international law. In accordance with Article 3 of the International Covenant on Civil and Political Rights, each State Party to it undertakes:

(a) *To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;*
(b) *To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;*
(c) *To ensure that the competent authorities shall enforce such remedies when granted* (Emphasizes added – A.S.).

Thus, implementation of web site blocking provisions as a remedy against violation of privacy rights ensured by data protection legislation may be viewed as an "effective" remedy[48]. In this case, Federal Law No. 242-FZ indeed has some extra protection mechanisms for data subjects. It is another matter that web site blocking provisions are not inevitably linked with data localization requirements, and the privacy enhancing nature of the latter remains questionable.

3.2. *Retaliation for US/EU sanctions*

This opinion was very popular when the Federal Law No 242-FZ was just adopted and there was confusion in the market[49]. The main arguments in favour of this opinion relate to the timing of the adoption of the law, which corresponded to the period of escalation of the Ukrainian crisis and associated tensions between Russia, the USA and its allies. Besides frequent mentioning by Roskomnadzor officials of Facebook, Twitter and other big transnational Internet services in the context of the potential application of this law, mention was also made to the "offshore" orientation of the law. As ECIPE argues, data localization requirements are effectively disruptive bans on data processing and hence the foreign provision of that service into the domestic territory[50].

After almost a year of discussions about the implementation of the law, which were conducted by Roskomnadzor with the business community, including representatives from US-based companies, this explanation cannot be treated now as the dominating one. However, it is impossible to deny completely the effect which the Federal Law No. 242-FZ law produced on foreign IT-companies operating in Russia: they started to express more willingness to engage in the dialogue with the Russian regulator and to ensure compliance with Russian legislation.

[43] Rohin Dharmakumar, India's Internet Privacy Woes, Forbes India (Aug. 23, 2013). URL: http://forbesindia.com/article/checkin/indias-internet-privacywoes/35971/1#ixzz2r0zriZTF.

[44] Sharding is a process of dispersing of a data set in fragments among the servers or other storage equipment, to be reunited and delivered to a user logging in with the correct credentials.

[45] Article 23 of the Constitution of the Russian Federation.

[46] Article 29 (4) of the Constitution of the Russian Federation.

[47] Such an opinion was expressed by Anton Ivanov, the former Chief Justice of the Supreme Commercial Court of Russian Federation (merged with Supreme Court of Russian Federation in 2014). See: Anton Ivanov. *Cross-Border Personal Data Storage by the Russian Law* [In Russian] // Zakon, 2015. No. 1. P. 141–143.

[48] However, the author should acknowledge, that the question of correlation between web site blocking provisions and international law deserves much deeper research.

[49] The author of this paper also shared this opinion to a certain extent. See: Savelyev A. Data localization laws and their potential impact on E-commerce in Russia [in Russian] // Zakon. Vol. 9, 2014. P. 67.

[50] The Costs of Data Localisation: Friendly Fire on Economic Recovery // Occasional Paper. European Centre for International Political Economy (ECIPE). 2014. № 3. URL: http:// ecipe.org/publications/dataloc.

3.3. *A measure to support of local data-centre market*

Introducing mandatory comprehensive data localization regulations increases the demand for local hosting and data centre services, at least from those companies which are willing to comply with such regulations. Not surprisingly, some Russian companies link new opportunities with data localization regulations, and one of these is the Russian telecommunications behemoth, Rostelecom[51], which is a frequent participant in various government-held meetings on implementation of Federal Law No. 242-FZ. Apart from Rostelecom, many local data centres have already announced their readiness to accommodate foreign companies. Other local IT-companies may also benefit from these regulations, e.g., providing integration and software development services.

However, it is very unlikely that Federal Law No. 242-FZ had economic objectives, at least as primary ones. No analysis of the potential economic impact of data localization provisions on the IT-market and Russian economy in general was performed. Besides, strong opposition and critics of the law, which accompanied its discussions for almost a year since its introduction, could have changed the position of the Russian government given, it seemed, that the lobbying efforts of some companies were the sole drivers of the law at that time. But the reluctance of the Russian parliament and other government agencies to change something in the law evidences the fact that something bigger than purely economic interests was at stake here.

3.4. *Implementation of the new "digital sovereignty" agenda of the Russian government*

Data localization regulations can be regarded as a part of the new approach of the Russian government to regulation of the IT-sphere and Internet in particular. This new approach can be designated as "digital sovereignty", although this phrase is not stated in Russian legislation and other official acts, but is still frequently used in speeches of officials and Mass Media. In general terms, digital sovereignty, being a derivative from state sovereignty[52], can be defined as a right of a national government to exercise control over information processes within the country without external interference. Implementation of a "digital sovereignty" agenda may be considered as a natural and predictable reaction of national government to the situation of the political, social and economic instability surrounding it. Revolutions in Egypt and other Arabic countries (Arab spring), where according to the prevailing opinion social networking played a prominent role;[53] US National Security Agency's global surveillance program, revealed by Edward Snowden in 2013; several terrorist acts, committed in Russia in December 2013; the Ukrainian crisis and heightened USA-Russia political tensions; international sanctions imposed on Russian government officials and Russian companies, examples of unilateral refusal without notice to perform its obligations demonstrated by Visa and MasterCard, were only a fraction of the political events which can be regarded as a threat to a stability of the Russian government. Taking into account the role of the Internet in the modern society, it would be too imprudent from the national government's perspective to stay away from it. After all, "information is the foundation of all governing"[54]. As one Russian official in informal conversation argued: "If you don't control the Internet, someone else controls it".

Data localizations requirements can facilitate strengthening the control of the Russian government over Internet activities in the following ways.

3.4.1. *Prevention of mass-scale loss of personal data if Russian segment of Internet becomes isolated*

Due to the current geopolitical situation, this has moved from the hypothetical to the actual. Lots of possible scenarios were discussed within the Russian government including the most extreme reaction such as cutting Russia off from the global Internet. In this case, if most of the data resides on foreign servers, such cut off would mean that the Russian segment of the Internet becomes almost useless, since it would be stripped of valuable data, most of which constitutes personal data. To some extent, this risk is indeed mitigated by the concepts of "primary" and "secondary" databases, which form the element of Russian data localization mechanisms. If personal data should be first recorded and further updated in the primary database located in Russia, it will be still available even if the Russian segment of the Internet becomes isolated, thus making it more independent and operational. If data localization provisions only required making a copy of personal data in Russia, thus allowing primary databases to be located outside Russia, access to personal data could be still be cut off, since "mirrors" of primary databases technically depend on the replication processes and may not function without having access to the primary database.

3.4.2. *Additional opportunities for Russian law enforcement agencies*

The presence of relevant information on the territory of the Russian Federation triggers the territorial basis for jurisdiction, thus giving additional powers to police and other law enforcement agencies. Relevant data can be requested more easily and without following burdensome provisions of mutual legal assistance treaties, which are unlikely to work effectively during intense political environments.

---

[51] According to various sources, Rostelecom plans to invest more than 40 billion rubles in new data centres. http://www.interfax.ru/russia/416473.

[52] State sovereignty is defined as «supreme, absolute, and uncontrollable power by which an independent state is governed and from which all specific political powers are derived; the intentional independence of a state, combined with the right and power of regulating its internal affairs without foreign interference». West's Encyclopedia of American Law, edition 2. 2008. The Gale Group, Inc. http://legal-dictionary.thefreedictionary.com/State+sovereignty.

[53] Catherine O'Donnell. *New Study Quantifies Use of Socia Media in Arab Spring* // University of Washington. 12 September 2011. http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/.

[54] Governance and Information Technology, eds. Victor Mayer-Schönberger and David Lazer, Cambridge, MA: MIT Press, 2007, P. 1.

3.4.3. *Additional instrument of control over distribution of unwanted content*

Since lots of user-generated content distributed on web sites can be qualified as personal data, relevant takedown and web site blocking mechanisms may apply. Thus, personal data legislation, accompanied with the blocking "functionality", may be used to put pressure on foreign Internet resources distributing undesired content. Recently introduced into Russian law, the "right to be forgotten", inspired by ECJ decision of *Google v. Spain*[55], further expands this opportunity. This new Russian law requires search engines distributing ads targeted at Russian audience to remove links to content distributed "in violation of the law", or deemed "untrustworthy", or that is "no longer relevant due to subsequent events or actions"[56]. Since there are no exceptions relating to the public persons, there are reasons to believe that such law may be used for limitation of access to information compromising public officials and perform some kind of censorship in favour of government policy.

As it can be seen, the benefits of data localization provisions for national security purposes are rather evident, at least from a theoretical perspective. National security reasons may explain the speed of the adoption of the law and massive ignorance of the industry feedback on it: arguments appealing to national security are immune from almost all the possible criticisms in the time of crises[57]. Appeals to national security matters were frequently used by Russian officials in comments relating to Federal Law No. 242-FZ[58]. Data protection legislation thus plays a role of a "shelter" for reaching important national security goals, just like protection of minors or control over distribution of child pornography is often used as a reason for control over online content. Personal data regulations are more and more becoming "dual use" in nature and pursue two different purposes. One purpose is the official one: the need to protect the interests of data subjects. Another hidden purpose is implementation of an existing political agenda for increasing control over the Internet. And Russia is not a new player in the field of using personal data legislation for such purposes. According to Kuner, national regulation of data protection (transborder personal data flow in particular) frequently may be one of the ways to protect national interests and national sovereignty. Although examples provided by him relate to the 1970–80s period of the last century, these seem hardly outdated even today[59].

Summing up the above, it is possible to draw the conclusion that adoption of personal data localization provisions in Russia is mostly driven by national security concerns, covered in "protection-of-data-subjects" wrap. All other reasons, even if indeed they were considered by the ideologists of the law, are only of a supplementary nature. Understanding of the reasons behind the law helps to understand its possible interpretation. National security driven laws usually have a broad nature, enabling maximum discretion during its enforcement. It explains the long-lasting reluctance of the Russian Ministry of Communications and Roskomnadzor to provide any written official interpretations of the law. It also indicates the risk that the law may lead to selective enforcement, depending on the political needs.

4. Potential impact on the market and technologies

After all the buzz personal data localization regulations created on the Russian market, they will hardly remain only on paper. However, compliance with them has economic as well as technological consequences, which are substantially intertwined. This section will provide a brief analysis of the potential impact of data localization on the Russian market in general and the IT-market in particular.

4.1. *Extra costs for companies*

Compliance with data localization requirements requires time and money. The first steps for a company typically include identification of all the existing databases and analysis of the information contained in them. Then for those databases, which process information qualifying as personal data, it is necessary to understand how the information flows: where and from whom it is received (whether it is "collected" in the meaning of the law) and where it goes thereafter. If the relevant database is used mostly by the local entity, it is possible to ensure its localization without substantial difficulties. Complications appear when there is a need to localize centralized databases of large multinational companies, since it requires reconfiguration and restructuring of its IT-infrastructure. Typical solutions for global databases (e.g. HR databases) are to create a customized local application with the database and integrate them within the global ("Core") database. When personal data, collected in Russia, is entered and saved in a local database, it will be automatically transferred into the Core database. Such a solution requires changes in the core

[55] Google Spain SL v. Agencia Espahola de Proteccion de Datos, Case C- 131/12, 13 May 2014.

[56] Federal Law No. 264-FZ of 13 July 2015, 'On amendments to the Federal Law No. 149-FZ "On Information, Information Technologies and Protection of Information" and Articles 29 and 402 of the Code Civil Procedure of the Russian Federation'. The law becomes effective January 1, 2016.

[57] The history of the adoption of US PATRIOT act after terrorist acts of 9/11 is a vivid example of it. Another one is the history of adoption of EU Data retention directive. Several EU Member States adopted regulations, which imposed obligations on service providers with regard to data retention putting the aim of combating terrorism and serious crimes upfront as a result of the terrorist attacks of 11 September 2001 in New York (United States), 11 March 2004 in Madrid (Spain) and 7 July 2005 in London (United Kingdom). See generally: Peter J Milford. *The Data Retention Directive too fast, too furious a response? Implementing and Transposing European Directive 2006/24/EC*. LLM Dissertation. Southampton Business School. http://www.petermilford.com/downloads/Data_Retention_PMilford.pdf.

[58] See e.g.: Interview with the head of State Duma's committee on information policy Leonid Levin, where he explicitly stated that Russian will resist the attempts to destabilize Russian Internet from the outside. He also pointed out that data localization is meant to increase stability of Russian Internet by implementing "backup" infrastructure. Tass.ru, 6 October 2014. URL: http://tass.ru/politika/1489008.

[59] Christopher Kuner, *Transborder Data Flows and Data Privacy Law*. Oxford University Press. 2013. P. 30 ff.

application of the user interface and bi-directional synchronization between them. Writing the new code followed by integration and testing may require months of work and millions of dollars, depending on the complexity of the Core database.

Of course, such expenses do not bother Roskomnadzor or the Russian Ministry of Communications, since they are perceived to be a "cost of doing business" in Russia. Such an approach is generally typical for all government authorities responsible for supervision. A similar approach can be seen among European regulators as well[60]. It is possible to expect that extra costs incurred by foreign companies, which decide to comply with the data localization provisions, can be shifted on to consumers, thus increasing the price of goods and services for them. The same may be true for Russian companies which will have less flexibility for optimization of its costs. Since average prices for hosting of comparable quality in Russia are higher than, say, in Germany, such a limitation may lead to extra costs imposed on foreign companies, which have to choose less efficient local suppliers to handle their personal data processing operations.

4.2. *Losses for the Russian economy*

It is also necessary to mention that ECIPE[61] has conducted research into the impact of data localization provisions on the Russian economy with a name which already reflects the biased nature of the research[62]. The overall conclusion of the research is rather pessimistic. According to the executive summary, "the losses are equivalent to –0.27% of gross domestic product (GDP), equivalent to a loss of 286 billion roubles (USD 5.7 billion). Applied with 2015 IMF forecasts, the Russian economy would contract by –4.1% this year. Investments in the Russian economy would drop by –1.41% or 213 billion roubles, with considerable effects on employment".

The main problem with this research is that no detailed methodology of calculation was provided, which could enable independent verification of the results. ECIPE only stated that

> *The analysis uses a computable general equilibrium model (CGE) based on the GTAP8 database, which is a well-acknowledged methodology that is frequently used for trade and economic impact analyses by academia and policymakers worldwide. Based on these computations, we calculate the impact of data privacy and data localisation requirements on key variables – real GDP, sectorial output, domestic income, exports, and investment*[63].

But the GTAP8 database does not have data older than 2009, what is more than six years old already[64]. Besides, no official Russian statistics were used (Federal State Statistics Service or Russian Ministry of Economic Development), only data from the International Monetary Fund (IMF) and World Bank, which may lack objectivity in the present political situation. It is also not clear how "any possible positive effects, e.g. from Russian data processing firms replacing foreign ones", as claimed by ECIPE, have been taken into account: nowhere else in the document are these "positive effects" disclosed. At the same time, it would be very interesting to see such an analysis, taking into account that the idea of localization of Internet services is rather popular in some European countries under the mottos of development of the local IT-market. For example, in Germany, the leading Telco provider, Deutsche Telekom, launched "E-mail made in Germany", a service that seeks to store and route data exclusively through German servers[65]. France also has plans for building "Made in France" a set of Internet services, such as cloud computing, big data and Internet of things as a part of national innovation plan, which also implies efforts to keep data processing in France[66]. So, there is nothing principally extraordinary in the possible protectionism of local IT-companies by Russian government by adoption of data localization provisions. Whether such protectionist measures will indeed help to strengthen local market players remains to be seen, but one thing is clear: the outcome will strongly depend on the results of the import substitution policy, initiated by the Russian government in parallel. Otherwise, localization of data centres might lead to an increase in the import of US/EU hardware and software, a result which is at odds with digital sovereignty objectives.

It is not surprising that the overall reaction towards the ECIPE research has been very sceptical, both from the government authorities' perspective as well as the blogosphere. Nevertheless, the Administration of the President of Russia expressed interest in conducting a thorough research on the economic impact of personal data localization[67]. It is expected to gather relevant data by the end of 2015 year for subsequent analysis. If such research is done, it could provide a unique source of information for decision-makers in other jurisdictions considering the option of adoption of similar legislation.

4.3. *Possible discrimination of Russian users*

Some technical solutions, e.g., collaboration solutions, provided in Software-as-a-service mode, such as instant messaging, videoconferencing, etc., have architecture which cannot be

[60] «Situations where the same database can be subject to different applicable laws do increasingly happen in practice. This is often the case in the field of human resources where subsidiaries /establishments in different countries centralize employee data in a single database. While this traditionally happens for reasons of economies of scale, it should not have an impact on the responsibilities of each establishment under local law. This is the case not only from a data protection perspective, but also in the context of labour law and public order provisions». Article 29 Data Protection Working Party. Opinion 8/2010 On Applicable Law. 16 December 2010. P. 15.

[61] The European Centre for International Political Economy (ECIPE) is an independent and non-profit policy research think tank dedicated to trade policy and other international economic policy issues of importance to Europe. http://www.ecipe.org/about-us/.

[62] Data Localisation in Russia: A Self-imposed Sanction by Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, June 2015. URL: http://www.ecipe.org/publications/data-localisation-russia-self-imposed-sanction/.

[63] Idem

[64] https://www.gtap.agecon.purdue.edu/databases/v8/.

[65] Deutsche Telekom, WEB.DE and GMX launch "E-mail made in Germany" initiative. 9 August 2013. URL: https://www.telekom.com/media/company/192834.

[66] A. Chander, U. P. Le, Op. Cit. P. 12.

[67] Results of the Meeting at the Administration of the President of the Russian Federation of 16 July 2015 (not publicly available).

"federated", meaning that the Russian data are stored in Russia, Spanish data are stored in Spain, US data are stored in US, etc. The most evident solution for such situations is to restrict provision of relevant services to Russian users, although this results in a revenue decrease for the company while limiting consumer choice among potential providers.

4.4. *Impact on implementation of innovative technologies*

For Cloud computing services, new data localization regulations may have a substantial transformative effect. Local data storage requirements are in a state of confrontation with the architecture of cloud computing. Computing resources (compute capability, storage, networking, etc.) are used *where it is more efficient* and cheapest from a taxation perspective, hardware, labour and electricity costs. Such optimization opportunities become substantially limited when a cloud provider has to use data centres mostly in one country. So, whether the resulting architecture of the cloud will meet the definition of cloud computing[68], relating to scalability is a question to be resolved. Absent such a feature of the Cloud as scalability, then Cloud computing may lose one of its critical benefits: the benefits of scale allowing lower costs for providers while giving the realistic illusion of infinite resources availability for users.

Data localization requirements also have limiting possibilities for offering cloud services having a layered structure. Besides, some value-added cloud services, mostly SaaS, are built on top of other cloud services: IaaS and/or PaaS[69]. Data localization regulations diminish opportunities of SaaS providers to build upon globally-established platforms since their use will automatically imply the possibility of processing data in foreign data centres. Without specialized interfaces and configurations, it would be difficult to ensure collection and updating of personal data of Russian citizens in line with local legislation.

Data localization requirements also have an impact on usage of innovative technologies, associated with Big Data, e.g. e-Health platforms, where IBM Watson is one of the examples[70]. Such platforms frequently perform deep analytics of personal health data of various patients from different clinics all over the world for identification of the most preferable method of treatment of a disease for a particular patient or for R&D activities. Existing personal data protection legislation already provides substantial obstacles for effective implementation of such technologies (e.g., necessity of specific consent for "secondary" processing of such data, which is usually not obtained when such data is initially collected for treatment purposes; prohibition on processing of personal data sets, collected for incompatible purposes; restrictions on transborder transfer of personal data). Some countries even place specific restriction on the transfer of health data outside the borders; e.g. in 2012, Australia passed the Personally Controlled Electronic Health Records Act, which prohibits, with certain exceptions, the transfer of health records outside of Australia[71]. Not surprisingly, the Organization for Economic Co-operation and Development (OECD) recently initiated work on preparation of the Council Recommendation on Privacy-Protective Uses of Personal Health Data[72]. Of course, data localization requirements, requiring processing of such data via a primary local database, introduce further complications for the effective use of such technology. They increase costs and complexities for collection and maintenance of data and, in the worst scenario, may reduce the size of data sets available for processing, eroding the informational value that can be gained by cross-jurisdictional studies[73].

Finally, data localization provisions may impede development of the Internet of Things ("IoT") technologies. The term IoT signifies that almost every device and object could over time be connected to the Internet's network of networks. Some of the other terms used to describe this process are the Internet of Everything, Industrial Internet and Machine-to-Machine communication. The IoT likely has profound implications for all aspects and sectors of the economy, in industrial and commercial processes, consumer and home services, energy, transport systems, health care, infotainment and public services. Of course, not all the data collected by devices and objects amount to personal data, but much of this data can be attributed to a specific individual (e.g. data collected by RFID sensors of a car, data collected from smart watch or devices like Google Glass). Since collected data usually resides on a provider's (vendor's) servers located anywhere across the world, segmentation of data storage and processing is not a feasible alternative for

[68] While various definitions are proposed, yet the most widely cited is that of the US National Institute of Standards and Technology (NIST). In accordance with it, "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This definition includes five characteristics. First, it is an on-demand service, where users can obtain computing capabilities in the amount "as needed automatically". Second, the cloud service can be accessed via broadband network and standard protocols, which support heterogeneous clients and user equipment. Third, resource pooling allowing "to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand". Fourth, rapid elasticity meaning that "capabilities can be rapidly and elastically provisioned" in order to meet demand lows and peaks as required by the users. Fifth, the use of the service is automatically measured in an abstract unit, for example storage, processing or bandwidth, based on which the utilized service is billable. See: The NIST Definition of Cloud Computing. Special publication 800-145. September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[69] For details see: Cloud Computing Law / ed. By Christopher Millard. Oxford University Press. 2013. P. 32–34.

[70] IBM Watson brings together clinical, research and social data from a diverse range of health sources, creating a secure, cloud-based data sharing hub, powered by advanced cognitive and analytic technologies. It is expected that IBM Watson will dramatically improve the ability of doctors, researchers and insurers to surface new insights from the all personal health data being created daily. URL: http://www.ibm.com/smarterplanet/us/en/ibmwatson/health/.

[71] See: § 77 of Personally Controlled Electronic Health Records Act, 2012. URL: http://www.comlaw.gov.au/Details/C2012A00063/Html/Text#_Toc327957207.

[72] Council Recommendation on Privacy-Protective Uses of Personal Health Data: Draft Discussion Paper. Working Party on Security and Privacy in the Digital Economy of the Committee on Digital Economy Policy. DSTI/ICCP/REG(2015)6, June 2015.

[73] A. Chander, U. P. Le, Op. Cit. P. 42.

many of the services, due to associated costs. It is much easier to limit functionality of IoT-type of products for a certain territory or even exclude such products from the distribution in the relevant country.

Taking into account that Big Data, Cloud Computing, and Internet of Things present interrelated technologies, e.g., IoT can be regarded as a source of data for subsequent processing and analysis by means of Big Data technologies performed on the basis of Cloud computing capabilities; this could lead to a negative impact with each component negatively influencing the other ones. Therefore, data localization provisions are not friendly to all those technologies; however, they can get along provided that enough investment has been made. Whether transnational companies will be willing to make those investments or will largely ignore the new data localization requirements will depend on the level of enforcement and the value of Russian data (which depends on the value of the Russian market) for such companies and associated costs.

4.5. *New taxation opportunities*

New data localization provisions bring foreign companies, at least those willing to comply with the legislation of countries of their operations, in this case on Russian soil. The presence of the servers, processing personal data of Russian citizens, most of which will have the status of "clients", can be regarded as an establishment, thus enabling more efficient taxation of their virtual activities. According to the current OECD Model Tax Convention, a permanent establishment is defined as "fixed place of business through which the business of an enterprise is wholly or partly carried on.[74]" The commentaries concede that a server hosting an application and making it accessible is a piece of equipment that has a physical location and, as such, can constitute a "fixed place of business"[75]. In the context of the digital economy, a company that provides a service in a country by using data collected through regular and systematic monitoring of users in that country could be deemed to have a virtual permanent establishment there. Although there is no position of Russian tax authorities on this matter yet, for sure, these ideas will become very attractive for Russian fiscal authorities and Ministry of Finance at some point in the future.

Besides, data localization provisions create a basis for implementation of new taxes, specifically oriented on Internet activities. As an example of potential tax, it is possible to mention initiatives expressed in France to introduce a special tax depending on the data collected and its geographical origin[76]. Without data localization provisions, such kinds of taxes would be difficult to administer.

It is possible to outline even more consequences of implementation of data localization provisions, and it is clear that subsequent years will reveal unexpected developments. But one thing is clear: the data localization concept is too complicated to be perceived only through the lens of privacy protection. The reality is always a little more complicated than people think. Therefore, it is submitted that positions that draw data localization in a solely negative light[77] are superficial and fail to see possible positive outcomes in areas not related to privacy.

5. Conclusion

The trend towards sovereignty of the Internet is present not only in Russia: many other countries, including those in Europe, are trying to increase control over information processes in their national segments of the Internet. Russia has adopted an unprecedented personal data localization mechanism, which does not have analogues in foreign countries and which has attracted a great deal of attention from foreign companies operating in the Russian market. The Russian mechanism of data localization is unique since it is applicable to all the personal data, not only to some types of it. Moreover,; it is aligned with other provisions of personal data legislation, including those which regulate transborder transfer of personal data. It is also accompanied with web site blocking provisions, providing incentives for compliance for companies valuing their reputation.

While it is difficult to argue that data localization provisions substantially enhance security and protection of data subjects *per se*, it is necessary to admit their potential value in the sphere of public law. Thus, personal data legislation may be used as a conduit for reaching national security and fiscal objectives. Local storage and processing of personal data of users, collected in Russia, create a good basis for taxation, either for existing types of taxing or for newly crafted ones.

While the real effect of data localization provisions in the public law sphere remains to be seen, the costs of their implementation are rather tangible already. Many companies have started to adapt their infrastructure to the new requirements at what may cost millions of dollars, depending on the size of the company and complexity of the information flows within its databases. Access to innovative information technologies, such as Cloud computing, Big Data and Internet of Things, and their usage can become more complicated due to associated extra costs for collection and maintenance of data in Russia. At the same time, restrictions on the usage of "classical" models of relevant technologies may lead to their mutation into something new, more resilient to data localization requirements, and such technologies may be of interest to other countries, willing to adopt similar regulations.

The estimated losses for the Russian economy in general, as predicted by ECIPE, do not look persuasive, since the relevant research lacks reliable and verifiable data. Hopefully, there will be other researches in this area, which can provide more detailed conclusions based on more substantive analysis.

[74] Article 5 of OECD Model Convention with Respect to Taxes on Income and on Capital 2014. URL: http://www.oecd.org/ctp/treaties/2014-model-tax-convention-articles.pdf.

[75] Report to the Minister for the Economy and Finance, the Minister for Industrial Recovery, the Minister Delegate for the Budget and the Minister Delegate for Small and Medium-Sized Enterprises, Innovation and the Digital Economy Task Force on Taxation of the Digital Economy. P. 113. URL: http://www.hldataprotection.com/files/2013/06/Taxation_Digital_Economy.pdf.

[76] Report to the Minister for the Economy and Finance, the Minister for Industrial Recovery, P. 121 ff.

[77] The examples of such approach can be seen in works of ECIPE and paper of A. Chander and U. P. Le.

In conclusion, it is necessary to mention two principle matters. At first, such regulations invited many foreign companies into a dialogue with the Russian government, which were reluctant to conduct such dialogues until now. Second, data localization provisions have attracted substantial attention to the problems of privacy in general and personal data legislation concepts from all the stakeholders: government officials, business and users. In a world where the enormous increase in the collection and use of data, new and unanticipated uses became a norm, while increased complexity and the pervasive nature of the Internet of things and Big Data present new challenges to the traditional principles, such attention is very much welcome. Maybe, as an initially unexpected outcome, these new data localization regulations, even if proven ineffective in the future, will serve as a driver for re-shaping existing outdated data privacy regulations and crafting something more suitable for the modern IT-environment.

Therefore, Russian data localization laws are neither a step forward, nor a self-imposed sanction: it is a bold step in an unknown direction which, if proven successful, may serve as a model for many other countries not satisfied by the existing models of Internet governance.

*The author is Ph.D. and senior legal researcher of the Center on Information Law, the National Research University "Higher School of Economics"; **Member of the Advisory Board for Federal Service for Supervision of Communications, Information Technology and Mass Media;** legal attorney of IBM Russia/CIS*; author of books on IP and contract law (including "The Law of Electronic Commerce in Russia and Abroad", "Licensing of software in Russia. Legislation and case law", "Freedom of contract and its limits" (in co-authorship with Prof. A. Karapetov, Ph.D.) and Commentary to the Federal Law of Russian Federation No. 149-FZ "On information, information technologies and protection of information") and articles on various IP and contract law matters.*

e-mail address: garantus@rambler.ru.

The views expressed are the personal views of the author and are not intended to reflect either the opinion of IBM or any other organization on relevant matters. This paper is an output of a research project implemented as part of the Basic Research Program for year 2015 at the National Research University "Higher School of Economics".