

Could the Recently Enacted Data Localization Requirements in Russia Backfire?

Iva MIHAYLOVA^{*}

In the wake of ex-NSA contractor Edward Snowden's surveillance revelations to the global public, and despite an unimpeded cross-border data flow and knowledge transfer being a prerequisite for the development of the digital economy, governments around the world are increasingly tending to resort to mandatory local data storage and to restrictions and bans on data transfers in a rather drastic attempt to protect their citizens' data security and privacy. This article discusses the legal and economic aspects of the recently enacted data localization requirements in the Russian Federation, as well as the consequences for costs, uncertainty, and the hampering of business activities that may arise if they are applied unaltered. The principal conclusion reached is that a less extreme solution that adheres to or builds upon the existing global practices and takes into account non-economic goals should be considered.

1 INTRODUCTION

In 1908, Nicola Tesla stated that a technology would be invented that would make it 'possible for a business man in New York to dictate instructions, and have them instantly appear in type at his office in London or elsewhere. He will be able to call up, from his desk, and talk to any telephone subscriber on the globe, without any change whatever in the existing equipment. An inexpensive instrument, not bigger than a watch, will enable its bearer to hear anywhere [...]. Millions of such instruments can be operated from but one plant of this kind.'¹ Although a combination of events, innovation, and technology contributed over time to the very precisely described emergence of the Internet, its birthday is considered to be 1 January 1983, when the Transfer Control Protocol/Internetwork Protocol was introduced. It allowed all fragmented computer networks of different computers to communicate in a universal language. Since the mid-1990s, the Internet has significantly facilitated international trade and cross-border investments by providing a convenient and almost instant means of communication, such as Voice

^{*} Research Assistant, Swiss Institute for International Economics and Applied Economic Research (SIAW-HSG), University of St. Gallen, Bodanstrasse 8 CH-9000, St. Gallen, Switzerland, Phone: +41-71-224 23 39, Fax: +41-71-224 22 98, Email: iva.mihaylova@unisg.ch. The author is grateful to Professor Simon Evenett for valuable comments and suggestions.

¹ Walter W. Massie & Charles R. Underhill, *The Future of the Wireless Art*. Wireless Telegraphy and Telephony, 67–71 (1908).

over Internet Protocol (VoIP), blogs, discussion forums, social media, and online booking facilities. Looking back at its historic development brings to mind the question: 'How do governments adapt their resorting to protectionist trade measures to maintain or boost the competitiveness of their countries on the Internet-driven international markets?' Examples of such state interventions with an economic purpose are abundant. Possible forms include but are not limited to: forced intellectual property transfer from foreign companies as a condition for market access; state-imposed requirements for foreign entities to form a joint venture with local companies to enter the domestic market; and offsets² or local content conditions to be complied with by foreign companies as a condition for the award of a state contract.

As discussed by Jackson (1997), in addition to the economic purpose of the illustrated international trade policies, policies can also have non-economic goals.³ As examples of the latter, he mentions national security motives, the state's goal to avoid over-dependence on other nations, and the choice of policies that do not maximize wealth but give preference to other non-economic public choices, for example aesthetics, religion, and the agricultural way of life. National security has increasingly motivated countries to resort to mandatory data localization on local servers in recent years. These state interventions limit or ban data storage, processing, or transfer to specific locations or to specific groups of persons.

Notwithstanding the reasons for governments' resorting to mandatory data localization on local servers, the likely impact both when used for legitimate state goals and when used for the creation of unequal trade opportunities may be negative. In addition, not only the targeted foreign competitor may be affected, but also the local market players themselves. These conclusions imply that a careful analysis of the potential risks and the possible impact on international trade over time should be conducted when a government considers the introduction of data localization requirements.

This article discusses the legal and economic aspects of the recently approved data localization requirements in the Russian Federation. They have a clear non-economic rationale because their goal is formulated in terms of improved protection of the rights of the Russian citizens, as well as the privacy and security of their personal data. However, it cannot be ruled out that Snowden's surveillance revelations and the international sanctions against Russia related to the annexation

² For instance, the US Department of Commerce's Bureau of Industry and Security (BIS) monitors on an annual basis the offsets that US firms involved in defence exports face. It classifies them into three broad categories: 'direct offsets' (co-production, sub-contracting), 'indirect offsets' (purchases), and 'either or both' (credit assistance, investment, licensed production, training, technological transfer, other).

³ John Jackson, *The World Trading System: Law and Policy of International Economic Relations* (MIT Press 1997).

of Crimea and the events in Ukraine may also have coloured the approval of these data restriction measures. The emphasis of this study is on the considerable impact that they may have on the business activities of local and international entrepreneurs if applied in their present unamended form. Specifically, the research approach is to establish causality mechanisms and to support them with evidence. The study also formulates recommendations for policy makers and business leaders who seek to counter the losses caused by the approved mandatory data localization requirements.

2 RECENT DATA LOCALIZATION LEGISLATION IN RUSSIA: AN OVERVIEW

The commercialization of the Internet in the 1990s provoked rapid growth of global data volumes and the tendency for geographical diversification of data storage. For example, big social networks store personal data of their users on various geographically remote servers – one for their messages, another one for their photos, and so on. However, the productivity and welfare gains that the Internet brings have become increasingly associated with data security challenges. Consequently, governments around the world feel increasingly obliged to introduce non-economic international trade policies that address this phenomenon. A rather extreme solution to which they are ultimately resorting more frequently is the implementation of data localization requirements.

The Russian Federation, ranking first on the list of the most connected emerging markets,⁴ approved two⁵ federal laws in 2014 containing data localization requirements with a great impact on national and international trade flows – Federal Law No. 242-FZ ('Data Localization Law') and Federal Law No. 97-FZ ('Online Content Law').

The purpose of this section is to provide an overview of both of these recent legislative acts. It presents first the key elements of the content of the Data Localization Law, because it affects a considerably wider group of businesses. The Online Content Law, due to its less stringent requirements, is discussed next.

⁴ James Manyika, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jauch, Sree Ramaswamy, & McKinsey Global Institute, *Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy*, April 2014, http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age (accessed 8 Jul. 2015).

⁵ On 1 Jul. 2014, in the State Duma, a data localization law was registered for discussion under the number 467078-6. It proposes that all official sites of state and municipal authorities should be placed on local servers. The content of this law will not be analysed in the present article, because it is more remotely related to its purpose with an emphasis on the state's data localization measures that affect the business activity of local and international entrepreneurs considerably.

Finally, a comparison is drawn with regard to the common features of and differences between the Data Localization Law and the Online Content Law.⁶

On 21 July 2014, the President of the Russian Federation signed⁷ the Data Localization Law. It extends Federal Law No. 152-FZ 'On Personal Data' with new personal data storage requirements. Concretely, it demands operators⁸ to 'ensure the recording, systematisation, accumulation, storage, adjustment (update, modification), extraction of personal data'⁹ of citizens of the Russian Federation by means of data bases, situated on the territory of the Russian Federation'. The newly introduced data localization requirement is expected to affect banks, IT and telecommunication companies, social media, Internet stores, and online travel agencies, as well as other companies, regardless of the type of industry in which they operate, due to the broadly set data localization criterion based on citizenship. In other words, both local and foreign companies with business activities in Russia will be affected provided that their operation involves the storage of personal data of their Russian customers on foreign servers.

The explanatory note to the draft variant of the Data Localization Law¹⁰ as registered for parliamentary discussion on 24 June 2014 by the Deputies of the State Duma, Mr Dengin, Mr Lugovoy, and Mr Yuschenko, formulates its goal in terms of improved privacy and security of the personal data of Russian citizens. In particular, Mr Dengin¹¹ motivated the proposed draft bill as follows:

Our credit cards, personal data, passport information, our correspondence with you, the [...] postal service where we register, [...] and write to someone, including in social networks, all this information about us is accumulated, aggregated and sent abroad, predominantly into the United States and into Europe. Nobody knows what structures do with this data [...].

In line with the expressed data security concerns, the Data Localization Law authorizes the Federal Service for Supervision of Communications, Information

⁶ In this article, the Data Localization Law and the Online Content Law are collectively referred to as 'both data localization laws'.

⁷ Laws in the Russian Federation must be approved on three readings by the State Duma (the Lower House of the Russian Parliament), by the Council of the Federation (the Upper House of the Russian Parliament), and subsequently by the Russian President.

⁸ Article 3, para. 2, of Federal Law No. 152-FZ defines the concept 'operator' as 'a state authority, municipal authority, juridical or physical person, that organizes and (or) processes personal data, as well as defines the purpose and the content of the processing of personal data'.

⁹ Article 3, para. 1, of Federal Law No. 152-FZ defines the notion 'personal data' as 'any information referring to a particular or identifiable on its basis physical person [...], including her/his surname, given name, patronymic, year, month, day and place of birth, address, marital status, social and property status, education, occupation, and income level, etc.'.

¹⁰ The draft bill was registered at the State Duma under No. 553424-6 and can be retrieved from: <http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=553424-6&02>.

¹¹ See the transcript of Meeting No. 178 of 1 Jul. 2014 of the State Duma at: <http://api.duma.gov.ru/api/transcript/172503-6>.

Technology and Mass Media (Roskomnadzor) to limit the access to sources that contain unlawfully processed personal data and to maintain a register of infringers of the rights of the owners of personal data. In this relation, the operators are requested to provide Roskomnadzor with 'information concerning the location of the information databases that contain personal data of citizens of the Russian Federation'. On 31 December 2014, the Russian President signed Federal Law No. 526-FZ, which altered the initially fixed starting date in the Data Localization Law for the storage of personal data of Russian citizens on local servers from 1 September 2016 to 1 September 2015.

Data localization requirements have also recently been enacted by the Online Content Law, which entered into force on 1 August 2014. It stipulates that 'organizers of dissemination of information in Internet'¹² must 'store on the territory of the Russian Federation information about facts related to the receipt, transmission, delivery and (or) processing of voice information, written texts, images, sounds and other electronic messages of users of the Internet and information about these users for six months' starting from the moment at which the described activities are terminated. The interpretation of this definition leads to the conclusion that email service providers, social media, and forums may be identified as key organizers of the dissemination of information.

The two data localization laws share the common condition that data must be stored on local servers. A key difference between the Data Localization Law and the Online Content Law is that the latter specifies a concrete time interval during which specific data must be retained locally. This condition makes it less stringent. Furthermore, in contrast to the Online Content Law, the Data Localization Law explicitly defines its data storage requirement with respect to the criterion of nationality.

3 ASSESSMENT AND RECOMMENDATIONS

The purpose of this section is to explore the evidence of three cause-and-effect relationships concerning the enacted data localization requirements in Russia, namely:

- (1) In the absence of a state-backed financial scheme, the introduction of any data localization requirement inevitably leads to compliance costs.

¹² Law No. 97 of 5 May 2014 defines 'organizers of dissemination of information in Internet' as persons whose activities ensure 'the functioning of information systems and (or) programmes for electronic computational machines, designed for and (or) used for reception, transmission, delivery and (or) processing of electronic messages of Internet users'.

- (2) Missing, non-transparent and logically inconsistent legal regulation creates uncertainty.
- (3) Business activities may be hampered, because the new data localization requirements do not take into consideration the specific conditions under which the affected businesses operate.

3.1 COSTS

The most imminent effect of the application of data localization requirements is their direct costs. Recently, the European Centre for International Political Economy (ECIPE) conducted a study based on the GTAP¹³ 8 general equilibrium model to quantify the economic losses of data localization requirements in seven jurisdictions. A conclusion in its simulation-based experiment on the impact of several economic shocks provoked by data limitations is that their effect is substantial. For example, the impact on the gross domestic product (GDP) is negative in all cases: Brazil (-0.2%), China (-1.1%), the EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%), and Vietnam (-1.7%).¹⁴ The negative impact is even higher if the same countries are assumed to have introduced data localization requirements across all the sectors of the economy: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), and Korea (-1.1%).¹⁵ The interested reader is referred to Table 1 for further details related to the empirical strategy. In addition, a recent ECIPE policy brief quantifies the losses of the Russian Data Localization Law. The numerical results of the study demonstrate that they reach -0.27% of the GDP, which, if combined with the IMF 2015 forecasts, will contract the Russian economy by -4.1% in 2015.¹⁶ Based on a simulation, the ECIPE finds evidence that the Russian manufacturing sector is more affected than the service sector. As noted by the authors, their results do not completely reflect the economic losses of the introduction of data localization legislation, because they do not consider 'technological progress, competitive behaviour and Russian firms' innovative capacities'.¹⁷

The findings of the ECIPE's study are in line with the costs concerns of the affected businesses provoked by the recently approved mandatory local storage of

¹³ See for more details: <https://www.gtap.agecon.purdue.edu/models/default.asp>.

¹⁴ Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Vershelde, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 03/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (accessed 8 Jul. 2015).

¹⁵ *Ibid.*

¹⁶ Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Vershelde, *Data Localisation in Russia: A Self-Imposed Sanction*, ECIPE Policy Brief No. 06/2015, http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf (accessed 8 Jul. 2015).

¹⁷ *Ibid.*

personal data of Russian citizens. In this regard, Mr Sergei Obukhov, Deputy of the State Duma, commented: ‘This draft bill [related to the Data Localization Law] is devastating for the small IT business. Today the cost of hosting services in Russia is more than, for example, in Germany, and if big companies can solve these problems, the small ones hardly can, many representatives of the small business will be affected – web masters, hosting re-sellers, online shops, online media ...’.¹⁸

None of the data localization laws contains any regulation concerning who will bear their direct costs and on whether the Government plans to reimburse or co-finance them. In addition, at the time of writing this article, no guidance has been provided by the Government on the exact data categories to be stored mandatorily, the forms of acceptable data formats, and the security protocols. A non-exhaustive list of such direct data retention costs may include: initial capital expenditures, costs related to customer inquiries, data provision requests from state bodies, maintenance of a required security level, maintenance of data in a format requested by the state authorities, data destruction after the mandatory storage period has elapsed, and routine hardware replacement. The size of these direct costs is highly dependent on the requirements of the Russian Government.

In conclusion, since no concrete data retention and security conditions have so far been suggested by the Russian Government, the operators are left with little opportunity to assess and ensure that the compliance with the state’s requirements does not constitute an excessive financial burden. Consequently, under these circumstances, it is the end consumer who may ultimately bear the direct costs of the new data retention scheme in Russia.

3.2 UNCERTAINTY

One of the purposes of legal regulation is to provide logical and transparent compliance guidelines for the affected parties. Failure to elaborate this point creates uncertainty. Therefore, as the next step of the analysis, the content of both data localization laws is examined with regard to its logical consistency and transparency.

3.2[a] *Assessment of the Transparency of the Data Localization Laws*

Cambridge Dictionaries Online defines ‘transparent’¹⁹ as ‘clear and easy to understand or recognize’. This definition implies that if a legal act is transparent, it

¹⁸ Excerpt from the transcript of Meeting No. 180 of 4 Jul. 2014 of the State Duma, <http://api.duma.gov.ru/api/transcript/553424-6> (accessed 8 Jul. 2015).

¹⁹ See <http://dictionary.cambridge.org/dictionary/english-german/transparent>.

will not be necessary to interpret what the legislator's purpose or idea might be on the basis of other existing legislative acts and case law.

The approved texts of the Data Localization Law and the Online Content Law define the prerequisites for the storage of personal data of Russian citizens on local servers, but they do not contain an explicit clause that prohibits the cross-border transfer²⁰ of such data. If this was the case, it would contradict Article 12 of the Federal Law No. 152-FZ 'On Personal Data', which sets the conditions for the transfer of personal data to two groups of recipients: (1) to foreign countries that provide adequate protection of the rights of the subjects of the personal data and (2) to foreign countries that do not provide adequate protection of the rights of the subjects of the personal data. Furthermore, it would violate the commitments of Russia ratified in 2013 under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108. The combination of these particular facts allows for the interpretation that the new mandatory data localization requirement will be complied with if the storage of personal data is duplicated on the respective foreign and Russian servers. Consequently, although not explicitly and transparently stated in both data localization laws, the aim of the legislator may be not to block the outflow of personal data of Russian citizens but to ensure that the state authorities avail themselves of the same information set as the foreign jurisdictions.

3.2[b] *Assessment of the Logical Consistency of the Data Localization Laws*

The concept 'logical consistency' is defined by Tarski²¹ as follows: 'A deductive theory is called CONSISTENT or NON-CONTRADICTIONARY if no two asserted statements of this theory contradict each other, or in other words, if of any two contradictory sentences ... at least one cannot be proved'.²² He defines 'contradictory' as follows: 'With the help of the word not one forms the NEGATION of any sentence; two sentences, of which the first is a negation of the second, are called CONTRADICTIONARY SENTENCES'.²³ Therefore, the logical consistency of both data localization laws has been assessed by analysing whether in their current content there exists a conjunction of statements A_j and

²⁰ Article 3, para. 11, of Federal Law No. 152-FZ defines the concept 'cross-border transfer of personal data' as 'transfer of personal data by an operator through the state borders of the Russian Federation to a state body of the foreign state, to physical or juridical persons, belonging to a foreign jurisdiction'.

²¹ Alfred Tarski, *Introduction to Logic and to the Methodology of Deductive Sciences* (3rd ed., Dover Publications, Inc. 1946).

²² *Ibid.*

²³ *Ibid.*

their respective denials not- A_j , equivalently denoted as $\neg A_j$, because both statements for each separate case j cannot be true at the same time.

The analysis of the content of the Data Localization Law for the simultaneous existence of conjunctions of statements A_j and their denials $\neg A_j$ did not find the latter. Consequently, no evidence for the existence of logical inconsistencies was found. The explanation for this finding is the above-mentioned broadness with which the concepts have been defined, which, although not detrimental to the logic within/of the law itself, affects its enforceability. If the logical consistency of the content of the Data Localization Law is to be assessed from a broader perspective, in connection with other federal laws, for example the Federal Law No. 152-FZ 'On Personal Data', or with international legal acts, such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, it is not clear whether it contains $\neg A_j$ because it is not explicitly stated. Consequently, if future amendments of the Data Localization Law related to its enforceability are elaborated in the wrong way, potential logical inconsistencies may emerge.

The Online Content Law contains $\neg A_j$ statements by exempting certain categories of operators from data retention obligations. These cases themselves do not contradict the A_j in the Online Content Law. However, a question to be clarified in the future by policy makers is whether it is possible for a sub-set of these exemptions as per the Online Content Law to fall under the category of mandatory data storage as per the provisions of the Data Localization Law. Such cases should be explicitly described in the Online Content Law to prevent potential logical inconsistencies and to help the organizers of the dissemination of information on the Internet, who are also data operators, to assess and plan their data storage costs.

3.2[c] *Potential Tax Implications*

Another point of uncertainty that might be activated in connection with the data localization requirements in Russia is potential tax claims. A leading law company motivates the causality mechanism in this case with the international taxation²⁴ concept of permanent establishment²⁵ as follows: '[c]urrently, Russian law has no

²⁴ As noted by Julie Roin in the *Research Handbook in International Economic Law*, edited by Andrew T. Guzman and Alan O. Sykes (Elgar Publishing 2007), '[t]he term "international taxation" is an oxymoron. There is no such thing as "international taxation" because no international governmental organization has the power to levy a tax. Rather, the term refers to the uneasy interface between national tax rules and transnational taxpayers, transnational transactions and the income earned through such transnational transactions'.

²⁵ A 'permanent establishment' ('PE') is a standard term in international taxation and is defined in the OECD Model Tax Convention, *Commentaries on the Articles of the Model Tax Convention*

concept of a “server-based” taxable permanent establishment. However, many tax concepts developed by OECD countries are currently being implemented in Russia. In the long-term companies operating Russia-based databases in connection with their commercial activities might face the risk of “server-based” permanent establishment claims in Russia, especially in the e-commerce and cloud computing market segments’.²⁶ This factor should be considered if an analysis of the long-term adverse effects of the data localization legislation in Russia is conducted.

3.3 HAMPERED BUSINESS ACTIVITIES

The new data localization requirements do not take into consideration the specific conditions under which the affected businesses operate. For example, the aeroplane industry is crucially dependent on its interconnectedness in the global network of information systems. In its recent letter to the Presidential Commissioner for Entrepreneurs’ Rights, the Russian Association of Air Transport Operators (AATO) expressed its concerns that the data localization requirements may lead to the termination of sales of aeroplane tickets for the flights of the Russian aviation companies because they cannot adapt their activities until 1 September 2015, the date on which the Data Localization Law enters into force. On the one hand, they have to obtain the consent of the global distribution systems used for international aeroplane ticket sales, such as Sabre, Gabriel, and Amadeus, for the placement of data in Russia or integrate their activity with dozens of third parties located

(OECD 2010) as ‘a fixed place of business through which the business of an enterprise is wholly or partly carried on’. The Committee on Fiscal Affairs of the OECD discusses in the OECD Model Tax Convention, *Commentaries on the Articles of the Model Tax Convention* (OECD 2010) the importance of the following elements of the PE definition:

‘the existence of a “place of business”, i.e. a facility such as premises or, in certain instances, machinery or equipment; this place of business must be “fixed”, i.e. it must be established at a distinct place with a certain degree of permanence; the carrying on of the business of the enterprise through this fixed place of business. This means usually that persons who, in one way or another, are dependent on the enterprise (personnel) conduct the business of the enterprise in the State in which the fixed place is situated.’

A PE’s purpose is to establish a threshold level of a business activity above which a source state, any state that is not the state of residence of the physical or juridical persons that carry out the respective business activities, can impose taxes on their income. Stated equivalently, if a PE exists, the source state has the right to impose tax on non-resident profits and income. Conversely, if it is proven that a PE does not exist, the general norm is only the residence state to tax business profits. In conclusion, the purpose of the PE concept is to limit or avoid cases of double taxation on the inter-state level.

²⁶ Baker & McKenzie, *Information Letter July 2014*, <http://www.bakermckenzie.com/alrussiapersonaldatajul14> (Accessed 8 Jul. 2015).

around the world that use global distribution systems.²⁷ On the other hand, there is a lack of an automated information system in Russia that is able to meet the demand of all Russian aviation companies.²⁸ The AATO assesses the fulfilment of either or both requirements within such a short period as impossible.

4 ASSESSMENT FINDINGS AND RECOMMENDATIONS

This article has analysed some essential items that should be on the agenda of the Russian Government in relation to the recently enacted data localization requirements. A list of key assessment findings and recommendations can be summarized as follows:

- (1) A number of key definitions discussed in section 3 are either too broad or missing. Because of this fact, the following recommendations are made:
 - To produce, with the participation of the operators and the organizers of the dissemination of information on the Internet, an industry-wide consultation article. The suggested article should be used for the approval of secondary legal acts to complement both data localization laws or to amend them directly.
 - To narrow as much as possible the range of entities that can access Russian citizens' metadata and to specify in detail which bodies can access which categories of personal data. This step is necessary because Article 3, paragraph 1, of Federal Law No. 152-FZ 'On Personal Data' does not contain an exhaustive list of all the categories of personal data. For example, it does not specify nationality as a personal data category, while this particular piece of information is crucial for the implementation into practice of the new mandatory data storage rules by the operators in accordance with the Data Localization Law.
 - To introduce a mechanism that guarantees that the locally stored data of Russian citizens will be used only for non-economic purposes, such as national security and/or lawful enforcement of criminal cases.

²⁷ Business Aviation Portal ATO.ru, *The Application into Practice of Law No. 242-FZ of 21.07.2014 could lead to Russian Airlines Ticket Sales Termination as of 1 September 2015*, <http://www.ato.ru/content/%20primenenie-na-praktike-zakona-ot-21072014-no242-fz-mozhet-privesti-k-ostanovke-s-1> (Accessed 8 Jul. 2015).

²⁸ *Ibid.*

- According to the Law for Protection of Entrepreneurs' Rights,²⁹ Roskomnadzor routine checks should not take place more than once in three years, must not surpass twenty days, and should have their schedule coordinated with the Prosecutor's Office. To avoid arbitrary decision-making, the frequency, coordination with other state bodies, and maximum duration of Roskomnadzor routine checks under the Data Localization Law must be specified.³⁰
 - Given the unprecedented innovation of information and communication technologies and the speed with which old technologies become obsolete and new ones enter the market, to consider the question of whether state-monitored review periods for formats, work-flows, and so on should be introduced as texts in both data localization laws.
- (2) In the case of Russia, the data localization requirements may have additional future costs in the form of tax claims. This scenario becomes more likely if the concept of taxable server-based permanent establishment (PE), which is non-existent in the Russian legislation at the moment, is approved. Given the tax implications in the event of the introduction of such a state measure, it is recommended to choose the leading model from the international tax treaty practice on which it will be based: the United Nations Model Convention for Tax Treaties between Developed and Developing Countries ('United Nations Model Convention') or the OECD Model Tax Convention ('OECD Model Convention'). 'The United Nations Model Convention generally favours retention of greater so-called source country taxing rights under a tax treaty – the taxation rights of the host country of investment – as compared to those of the "residence country" of the investor. This has long been regarded as an issue of special significance to developing countries, although it is a position that some developed countries also seek in their bilateral treaties.'³¹ In contrast, the OECD Model Tax Convention establishes more beneficial conditions for the

²⁹ Federal Law No. 294-FZ, published in *Rossiyskaya Gazeta*, 4823 (30 Dec. 2008), <http://www.rg.ru/2008/12/30/prava-kontrol-dok.html> (accessed 8 Jul. 2015).

³⁰ The rules for the implementation of the Online Content Law have already been approved on 8 Apr. 2015 with Decree No. 327. They deviate from the ones established in the Law for Protection of Entrepreneurs' Rights rules: Roskomnadzor does not coordinate its checks with the Prosecutor's Office; an upper limit of thirty days for the duration of its checks is specified; and a pre-notification period of not less than twenty-four hours before their start is necessary.

³¹ *United Nations Model Double Taxation Convention between Developed and Developing Countries* (New York 2011).

residence state.³² In practice, however, jurisdictions do not apply the residence or the source principle in a pure form. Hybrid forms of taxation combining features from both tax principles are currently widespread and this option may also be preferred by the Russian Federation.

- (3) Until now, no concrete data retention and security cost-related clarification has been issued by the Russian Government. Consequently, it is not possible to assess whether the compliance with the state's considerable data requirements constitutes an excessive financial burden.

Because of the uncertainty related to the future data localization costs, it is recommended to estimate the industry-wide and macroeconomic impact of the data localization legislation with GTAP 8 analogously to the ECIPE but to introduce additional variables responsible for long-term causality that it does not consider. In this way, the full effect of the data localization legislation will be assessed. The long-term variables suggested by the ECIPE are related to competitive behaviour as well as research and development.

- (4) A key aspect of the digital, or Internet, economy is its cross-border nature, which relies heavily on unobstructed information and knowledge transfer. For example, the aeroplane industry is crucially dependent on its interconnectedness in global distribution systems, such as Amadeus, Sabre, and Gabriel. For the implementation of the new data localization laws to be feasible, the cross-border nature of business activities should be considered by policy makers.
- (5) Since an effectiveness assessment is essential for any public policy, it is further recommended to promote the production and dissemination of periodic, peer-reviewed, independent studies on the topic concerning the economic, data security, and international trade-related impacts of the data localization rules in Russia.

5 CONCLUSION

The increasing impact of the Internet on international trade and growth is inevitably associated with security challenges and intensified competition. Consequently, governments around the world feel more compelled to protect their

³² PwC, *Permanent Establishments 2.0, At the Heart of the Matter*, 2013, http://www.pwc.com/en_GX/gx/tax/publications/assets/pwc-permanent-establishments-at-the-heart-of-the-matter-final.pdf (accessed 8 Jul. 2015).

local businesses and citizens. A rather extreme solution to which they are ultimately resorting more frequently is the implementation of data localization requirements. This study discussed the legal and economic aspects of the recently approved data localization requirements in the Russian Federation. It also formulated recommendations for policy makers and business leaders who seek to counter their losses.

Two questions arise with regard to the recently approved data localization requirements in Russia. First, can other countries offer Russia less extreme solutions in terms of uncertainty and financial expenditure?³³ Second, how can Russia benefit from subject-related international cooperation?

Concerning the first question, a possible solution could be to specify in the Data Localization Law, analogously to Australia's Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, a fixed time period for mandatory personal data storage. This amendment proposal is motivated by the fact that in the version of the Data Localization Law discussed in this article, this information, which is important in terms of uncertainty and financial expenditure, is missing.

The Russian Federal Law No. 152-FZ 'On Personal Data' does not contain an exhaustive list of all the categories of personal data. For example, it does not specify nationality as a personal data category, while this particular type of data will be necessary for the implementation of the data localization requirements in the Data Localization Law. In this respect, a legislative amendment suggestion that may reduce the extremeness and improve the clarity of the data localization requirements in Russia comes from the Chinese practice. In China, the Ministry of Industry and Information Technology has banned the collection of personal data without 'specific and clear purpose',³⁴ thus imposing an upper limit on the categories of personal data that may be collected and stored.

The Vietnamese practice may also be helpful for the reduction of the cost and uncertainty dimensions of the Russian data localization rules. In 2013, the Government of Vietnam, with Decree 72 on Management, Provision, and Use of Internet Services and Information Content Online, approved a concrete

³³ Table 2 in Appendix 2 contains the example mentioned in this section of less extreme solutions implemented in other countries, based on the Global Trade Alert database (www.globaltradealert.org). Please note that the GTA provides information on government policies that treat domestic and foreign commercial interests asymmetrically. Refer to Appendix 1 for a description of the colour coding used in the Global Trade Alert database. The section 'Conclusions' also contains examples of less extreme solutions implemented in other countries with symmetric treatment of domestic and foreign commercial interests. In this case, the data sources are mentioned in the main text.

³⁴ Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Verschelde, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 03/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (accessed 8 Jul. 2015).

quantitative requirement for the introduced licensing regime. In particular, organizations and enterprises that establish news websites, social networks, as well as providers of information services on mobile networks and game service providers must have ‘at least 01 server system in Vietnam serving the inspection, storage, and provision of information at the request of competent authorities, and settlement of customers’ complaints about the service provisions in accordance with regulations of the Ministry of Information and Communications’. Thus, a clear lower limit of mandatory servers to be installed locally is stipulated. Hence, cost planning and compliance with the rule are facilitated.

A question related to the mandatory number of data servers is their financing, inclusive of subsidization. For example, the French Government has invested in the creation of two cloud computing enterprises.³⁵ Collin and Colin (2013) propose the introduction of a special data tax on the ‘collection, management and commercial exploitation of personal data generated by users located in France’.³⁶ They claim that the level of the tax can successfully influence business decisions on whether to locate services involving data inside or outside the country. The Australian Government is also currently considering how to contribute to the financing of the data retention rules that it has recently implemented. According to the acting first assistant secretary of the Attorney-General’s Department, ‘the government had decided to contribute to the initial costs of adjusting to the scheme such as reconfiguring networks “rather than bearing the entire costs of data retention”’.³⁷

Personal data collected by different industries bear different levels and types of risk. Therefore, regulation related to selected industries of major vulnerability or importance for the national economy, sovereignty, or security may be introduced. For example, the Australian Government in 2012 requested health records not to be stored or transferred outside the country. Similarly, in China, the general rule is that personal financial information that is collected locally must also mandatorily be stored, processed, and analysed locally. The Republic of Korea has also imposed restrictions involving personal financial data. Banks are prohibited from

³⁵ Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet* (April 2014), Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378, <http://ssrn.com/abstract=2407858> (accessed 8 Jul. 2015); and Pierre Collin and Nicolas Colin, *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*, January 2013, http://www.hldataprotection.com/files/2013/06/Taxation_Digital_Economy.pdf (accessed 8 Jul. 2015).

³⁶ *Ibid.*

³⁷ The Guardian, *Data Retention Laws: Cost of Setting up Metadata Storage Scheme is Still Unclear*, 17 Dec. 2014, <http://www.theguardian.com/australia-news/2014/dec/18/data-retention-laws-cost-of-setting-up-metadata-storage-scheme-is-still-unclear> (accessed 8 Jul. 2015).

outsourcing the processing of data of Korean customers to third parties – it must be processed in-house by the banks, either locally or abroad.³⁸

The Chinese ‘Telecommunications and Internet Personal User Data Protection Regulation’ of China requests data processors to conduct periodic risk impact assessments.³⁹ This approach could be used in Russia for the creation of a rating for a group of essential businesses working with personal data. In the case that the Russian Government decides to subsidize part of the data retention costs, the financing rules could be linked to this rating.

Concerning the second question, on subject-related international cooperation, Russia may benefit from participation in the expansion of the Information Technology Agreement (ITA) in the World Trade Organization (WTO) into the International Digital Economy Agreement (IDEA).⁴⁰ This suggestion is made by Lee-Makiyama,⁴¹ who calculates that this would expand the current agreement by 40%. If considering this option only in the light of the recent data localization measures in Russia, the most relevant measure from which the affected companies could benefit is to extend the ITA by following Lee-Makiyama’s proposal to include services trade in computer and related services and telecommunication services (rather than other measures that enhance the international trade in goods, for example extended product coverage by category on the HS code four-digit level and the establishment of a system of mutual recognition on a product-by-product basis).

Unobstructed cross-border information and knowledge transfer is a key success factor for the expansion of digital economies worldwide. This article has discussed the legal and economic aspects of the recently enacted data localization requirements in the Russian Federation, as well as the costs and uncertainty consequences that they may have if applied unaltered. The principal conclusion reached is that a less extreme solution that adheres to or builds upon the existing global practices and takes into account non-economic goals should be considered.

³⁸ Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Verschelde, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 03/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (accessed 8 Jul. 2015).

³⁹ *Ibid.*

⁴⁰ At the time of writing this paper, the ITA comprises seventy-four participants, accounting for 97% of the world trade in information technology products, which have undertaken to eliminate completely duties on IT products listed in the ITA agreement. See for more details World Trade Organization, *15 Years of the Information Technology Agreement. Trade, Innovation and Global Production Networks*, http://www.wto.org/english/res_e/publications_e/ita15years_2012full_e.pdf (accessed 8 Jul. 2015).

⁴¹ Hosuk Lee-Makiyama, *Future-Proofing World Trade in Technology: Turning the WTO Agreement (ITA) into the International Digital Economy Agreement (IDEA)*, ECIPE Working Paper No. 04/2011, https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/future_proofing_e.pdf (accessed 8 Jul. 2015).

Appendix 1: Data Localization Barriers: Quantified Losses

Table 1 presents the key results of the ECIPE Occasional Paper No. 03/2014 (Figures 1, 4, and 5 and Table 2). Its purpose is to quantify the losses of the data localization requirements introduced in seven jurisdictions: Brazil, China, the European Union (EU), India, Indonesia, South Korea, and Vietnam. Simulations using a computable general equilibrium model, GTAP 8, are the research method applied. The costs of data regulation are estimated in two scenarios. Scenario 1 is based on the data localization requirements as they are proposed or enacted. Scenario 2 extends the first one by studying the impact of the actual proposed or enacted data localization requirements on all the economic sectors of the respective country. The effect of data localization legislation on the gross domestic product (GDP), on investments, and on exports is explored. The total and per capita costs and welfare effects are also calculated. The per capita effect is derived on the basis of the average worker's salary in the selected countries.

Table 1: Key results of the ECIPE Occasional Paper No. 03/2014

<i>Simulated scenario</i>	<i>Brazil</i>	<i>China</i>	<i>EU28</i>	<i>India</i>	<i>Indonesia</i>	<i>Korea</i>	<i>Vietnam</i>
1. GTAP-simulated effect on GDP. Changes in %							
Scenario 1	-0.2	-1.1	-0.4	-0.1	-0.5	-0.4	-1.7
Scenario 2	-0.8	-1.1	-1.1	-0.8	-0.7	-1.1	-1.7
2. GTAP-simulated effect on investments. Changes in %							
Scenario 1	-4.2	-1.8	-3.9	-1.4	-2.3	-0.5	-3.1
Scenario 2	-5.4	-1.8	-5.1	-1.9	-2.6	-3.6	-3.1
3. GTAP-simulated effect on exports. Changes in %							
Scenario 1	-4.2	-1.8	-3.9	-1.4	-2.3	-0.5	-3.1
Total exports	-0.5	-1.7	-0.4	0.0	-1.7	-0.3	-0.5
Exports of goods	-0.6	-1.9	-0.2	0.0	-1.8	-0.4	-0.6
Exports of services	-0.3	-0.6	-1.0	0.0	-1.1	0.1	0.7
4. GTAP-simulated welfare losses from data legislation and privacy barriers, measured in current US\$							
Scenario 1	-4.7 bn.	-61.6 bn.	-80 bn.	-3.1 bn.	-2.7 bn.	-5.3 bn.	-1.5 bn.
Scenario 2	-15 bn.	-63.8 bn.	-193 bn.	-14.5 bn.	-3.7 bn.	-15.9 bn.	-1.5 bn.

<i>Simulated scenario</i>	<i>Brazil</i>	<i>China</i>	<i>EU28</i>	<i>India</i>	<i>Indonesia</i>	<i>Korea</i>	<i>Vietnam</i>
Scenario 1 (per capita effect)	-48.9	-80.7	-333.9	-6.7	-24.9	-218.6	-31.5
Scenario 2 (per capita effect)	-156.1	-83.6	-805.6	-31.5	-34.1	-655.7	-31.5

Appendix 2: GTA colour codes

-
- | | |
|---------|--|
| ▲ Red | (i) The measure has been implemented and almost certainly discriminates against foreign commercial interests. |
| ▲ Amber | (i) The measure has been implemented and may involve discrimination against foreign commercial interests; OR
(ii) The measure has been announced or is under consideration and would (if implemented) almost certainly involve discrimination against foreign commercial interests. |
| ▲ Green | (i) The measure has been announced and involves liberalisation on a non-discriminatory (i.e., most favoured nation) basis; OR
(ii) The measure has been implemented and is found (upon investigation) not to be discriminatory; OR
(iii) The measure has been implemented, involves no further discrimination, and improves the transparency of a jurisdiction's trade-related policies. |
-

Source: The Global Trade Alert (GTA) database (<http://www.globaltradealert.org>).

Appendix 3: GTA reports on data localization

Table 2: This table contains examples of data localization requirements implemented globally, reported by the Global Trade Alert (GTA) and mentioned in the ‘Conclusions’ section of this paper. Please note that the GTA’s reporting window starts in November 2008 (the date of the first crisis-related G20 summit held in Washington DC).

Country and GTA Colour Code	Description of the measure	GTA Link
Australia ▲ Red	Introduced personally controlled electronic health records	http://www.globaltradealert.org/ node/7804
China ▲ Red	Financial institutions’ protection of personal financial information	http://www.globaltradealert.org/ node/7735
Vietnam ▲ Red	Data localization and licensing of Internet service providers	http://www.globaltradealert.org/ node/7730