Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# Russian data retention requirements: Obligation to store the content of communications

*Mikhail S. Zhuravlev* *, *Tatiana A. Brazhnik*

*National Research University Higher School of Economics, Russian Federation*

*Keywords:*
Data retention
Russian legislation
Yarovaya package
Content of communications
Data retention directive
Telecom operators
Internet communication services
Privacy
Public security

A B S T R A C T

This paper presents an analysis of Russian data retention regulations. The most controversial point of the Russian data retention requirements is an obligation to keep the content of communications that is untypical for legislation of European and other countries. These regulations that oblige telecom operators and Internet communication services to store the content of communications should come into force on July 1, 2018.

The article describes in detail the main components of the data retention mechanism: the triggers for its application, its scope, exemptions and barriers to its enforcement. Attention is paid to specific principles for implementation of content retention requirements based on the concepts of proportionality, reasonableness and effectiveness.

Particular consideration is given to the comparative aspects of the Russian data retention legislation and those applying in different countries (mainly EU member states). The article focuses on the differences between the Russian and EU approaches to the question of how to strike a balance between public security interests and privacy. While the EU model of data retention is developing in the context of profound disputes on human rights protection, the Russian model is mostly concentrated on security interests and addresses mainly economic, technological aspects of its implementation.

The paper stresses that a range of factors (legal, economic and technological) needs to be taken into account for developing an optimal data retention system. Human rights guarantees play the key role in legitimization of such intrusive measures as data retention. Great attention should be paid to the procedures, precise definitions, specification of entitled authorities and the grounds for access to data, providing legal immunities and privileges, etc. Only this extensive range of legal guarantees can balance intervention effect of state surveillance and justify data retention practices.



## 1. Introduction

The issue of retaining communications data in order to protect national security is relevant for many countries, especially those that are focused on countering terrorist threats. Legal aspects of the topic are contradictory and debatable. On the one side, the interests of security should be taken into consideration, on the other side – privacy, the secrecy of communication and other protected rights and freedoms. It is obvious that the solution to the problem lies in finding a legal compromise based on the optimal balance between rights and legitimate interests

* *Corresponding author.* National Research University Higher School of Economics, Russian Federation, 3 Bolshoi Tryokhsvyatitelsky Pereulok, room 107, Moscow, 101000, Russia.
*E-mail address:* mzhuravlev@hse.ru (M.S. Zhuravlev).

https://doi.org/10.1016/j.clsr.2017.11.011

of all stakeholders involved but this is more easily stated than achieved.

Concerning data retention a set of important legal questions arise:

1. What persons are obliged to store data?
2. What data should be stored?
3. What is duration of data storage?
4. Where to store the data?
5. How to ensure information security of the stored data?
6. Who has the right of access to the stored data?
7. What are the grounds for access to the stored data?

In addition to purely legal aspects, numerous related technical and economic issues can be highlighted. These issues create problems relating to the technological enforceability of legal requirements and the financial arrangements associated with its implementation. Such factors should be taken into account when assessing the legitimacy of the data retention model basing on the principles of reasonableness, effectiveness and proportionality.

In 2016, the Russian authorities adopted a number of laws[1] extending the requirements for telecom operators and Internet communications services to store data about the communications of users. Similar provisions exist in the legislation of other countries[2], but the special feature of the Russian legislation is an obligation to store not only metadata (data about the fact of communications – time, duration, type of communications, geolocation, etc.) but also the content of communications. Adoption of these laws caused extremely sharp criticism from both business and civil society. Up to now, the requirement for content retention has not entered into force. This is due to take place on July 1, 2018. However, there are some suggestions for postponement because of difficulties with implementation of these requirements[3]. Development of detailed proposals for the implementation of content retention requirements is one of the current debates within and between IT industry and competent governmental bodies.

The purpose of this article is to provide legal analysis of the Russian legislation on data retention with reference to the similar legislation within the EU and other countries as well as developing some recommendations for legitimate implementation of data retention requirements with a strong adherence to the principles of reasonableness, economic viability and protection of human rights.

## 2. Criticism of content retention requirements

The Russian Federal law of 06.07.2016 №374-FZ "On amendments to the Federal law On combating terrorism "and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and public security" ('Yarovaya law') establishes an obligation on telecom operators and organizers of information dissemination on the Internet[4] (hereinafter – OID) to store on the territory of the Russian Federation text messages, voice information, images, sounds, video, other communications of users (hereinafter – the content of communications) for up to six months after the end of their reception, transmission, delivery and (or) processing (Articles 13 and 15). This obligation should enter into force on July 1, 2018. The law also establishes an obligation to keep metadata, although this duty is not new for Russian legislation, the 2016 Act merely expands the duration for storage of metadata. Particular interest is focused on the content retention duties.

Although the law establishes the general principles of content retention, detailed rules relating to procedure, duration and volume for storage of this information remain to be drawn by the Government of the Russian Federation. Until this secondary legislation is elaborated and enacted, the content retention requirements will not have actual effect.

The adoption of these legal provisions has caused criticism both from individuals and from the IT industry. Critical reviews include the following arguments:

1. storing the contents of all communications of each user is an unreasonable and disproportionate restriction of the right of citizens to privacy, it creates new information security threats and increases the risks of abuses by public authorities;
2. the cost of ensuring the storage of user's data according to assessments of four major Telecom operators[5] (MegaFon, MTS, Tele 2, Beeline) – at least 2.2 trillion roubles for big market players; according to assessments of the Federal Security Service and Ministry of Communications[6] – about 4.5 trillion roubles for the entire industry (3 trillion includes the cost of equipment, 1.5 trillion will be spend on related infrastructure); the working group under the Russian Government with participation of IT-industry estimated the total costs at 5.2 trillion roubles that is equal to 1/3 of the

[1] Federal law dated as of 06.07.2016 № 374-FZ "On amendments to the Federal law "On countering terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public security", *Rossijskaya Gazeta*, № 149, 08.07.2016 (In Russian) (Hereinafter – 'Yarovaya law' or 'Yarovaya package', named for Irina Yarovaya – parliament member who proposed these amendments).

[2] See Mandatory data Retention Around The World. [online] Available at: https://www.beencrypted.com/mandatory-data-retention/ [Accessed: 30.10.2017].

[3] The government discussed a postponement of 'Yarovaya law' for 5 years. (In Russian) [online] Available at: http://www.rbc.ru/politics/04/07/2017/595b2df89a794768b832dbf1 [Accessed: 30.10.2017].

[4] This entity has appeared in Russian legislation in 2014 as an attempt to regulate communication services on the Internet (like Skype, Facebook, Whatsapp, etc.). See Art. 10.1 of the Federal law dated as of 27.07.2006 № 149-FZ "On information, information technologies and protection of information", *Rossijskaya Gazeta*, № 165, 29.07.2006 (in Russian).

[5] Authorities will compensate the costs of telecom operators on "Yarovaya package". (In Russian) [online] Available at: https://www.vedomosti.ru/technology/articles/2017/02/07/676439-vlasti-rashodov-yarovoi [Accessed: 30.10.2017].

[6] Federal Security Service and Ministry of communications estimated the costs of "Yarovaya package" at 4.5 trillion rubles. (In Russian) [online] Available at: http://www.rbc.ru/technology_and_media/13/04/2017/58ef849a9a7947134a887f98 [Accessed: 30.10.2017].

Please cite this article in press as: Mikhail S. Zhuravlev, Tatiana A. Brazhnik, Russian data retention requirements: Obligation to store the content of communications, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.011