The Yarovaya Law: One Year After

April 2017
THE YAROVAYA LAW

ONE YEAR AFTER

Almaty • Bishkek • Minsk • Moscow • Ottawa • Tbilisi

Follow Us

DR Analytica

Facebook: /digital.report
Twitter: @DigitalReportRU + @DigitalReportEN

• Monitors the developments in digital economy, information security, telecommunication, e-government and other ICT areas across Eurasia. This monitoring allows our analysts to assess the ICT markets and environments in the targeted areas and industries, and provide clients with comprehensive analyses of the regional trends.

• Is an international consulting group, specializing in the analysis of ICT markets throughout the Eurasian region. Our services include risk assessment, analytics, and solutions that meet both strategic and tactical demands of customers, including cybersecurity.

All rights reserved © 2017
EXECUTIVE SUMMARY

In April 2016, the “Yarovaya Law” was introduced in the Russian Parliament. Aiming to increase public safety, it has become one of the most controversial Russian laws of the last decade.¹ Despite its adoption in July 2016, many Russian organizations, both public and private, continue to oppose its implementation, in an ongoing process that has led to some modifications of the initial measures. The opposition has been raised from organizations including the Russian Association of Electronic Communications, the Regional Public Center for Internet Technologies, Yandex, Mail.Ru Group, and others. DR Analytica looks at these developments to explain the law’s impact on the ICT sector in the Russian Federation and its near abroad.

Table of Contents

EVOLUTION TIMELINE 3
WHAT IS THE YAROVAYA LAW? 4
IMPLEMENTATION AND EFFECTS 5
REGIONAL IMPACT OF THE “YAROVAYA LAW” 6
CONCLUSION 7
WHAT WE CAN DO FOR YOU? 8
REFERENCES 9
The Yarovaya Law: One Year After

**EVOLUTION TIMELINE**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 April 2016</td>
<td>The Russian MP Irina Yarovaya in the cooperation with Senator Viktor Ozerov, introduces two bills that propose serious changes to Russian ICT legislation. The motivation behind the legislation is to improve measures against and toughen penalties for terrorism and extremism.</td>
</tr>
<tr>
<td>13 May 2016</td>
<td>The bills are adopted in the first reading.</td>
</tr>
<tr>
<td>24 June 2016</td>
<td>The bills are adopted in the second and third readings.</td>
</tr>
<tr>
<td>7 July 2016</td>
<td>The bills are signed by President Putin.</td>
</tr>
<tr>
<td>19 July 2016</td>
<td>Federation Council member Anton Belyakov, from the &quot;A just Russia&quot; party, introduced a bill to postpone the entry of these amendments into force until 2023.</td>
</tr>
<tr>
<td>20 July 2016</td>
<td>Most of the changes introduced through these bills come into force.</td>
</tr>
<tr>
<td>19 January</td>
<td>The Russian Ministry of Communication proposes to reduce tenfold the amount of information that should be stored by the &quot;Yarovaya Law&quot;.</td>
</tr>
<tr>
<td>4 April 2017</td>
<td>The State Duma Council send Senator Belyakov’s bill to the higher executive bodies for further debate.</td>
</tr>
<tr>
<td>14 April 2017</td>
<td>The Federal Security Service (FSB) and the Ministry of Communication estimates the cost of compliance to communications operators will be USD $79.5 billion.</td>
</tr>
</tbody>
</table>
What is the Yarovaya Law?

The two bills, which became known as the “Yarovaya Law”, consist of:


The first bill supplemented the Criminal Code of Russia with three new offenses:

- Failing to report a terrorist crime;
- Promoting extremist activity; and
- Commissioning an act of international terrorism.

The second bill compels telecommunications operators to store subscriber calls and messages, and related data for a period determined by the Government of the Russian Federation (but no more than 6 months) in accordance with Article 64 of the Federal Law “On Communications”, and to store data related to receiving, transmitting, delivering, and processing messages and calls for three years.

Some of the original provisions of the “Yarovaya Law” were excluded from the final versions. For example:

- The first draft contained a provision for preventing people from leaving Russia who had received the official warning about committing related crimes but had neither been charged nor convicted. By the second reading, this amendment only prohibited those who had been convicted of crimes such as terrorism or extremism from leaving Russia.
- By the second reading, the provision to strip those people of their Russian citizenship who commit or support terrorism or extremist crimes had also been removed.
IMPLEMENTATION AND EFFECTS

According to the “Yarovaya Law”, by 1 July 2018, all telecommunication and internet service providers must retain the content of user communications for six months and related metadata for three years. However, on 19 July 2016, Federation Council member, Anton Belyakov, from the “A Just Russia” party introduced a bill to postpone the entry of these amendments into force until 2023.

As a result, this bill was accepted by the State Duma Council and on 4 April 2017 and a draft sent to the President, the State Duma commission, factions of the Duma, the Federation Council, and other higher executive bodies for further debate. These bodies are expected to present their comments and/or suggestions to the State Duma Committee on Security and Anti-Corruption by 4 May 2017. Further updates on this bill may occur during the spring session (May 2017) of the State Duma.

The main technical problem for the law’s implementation is a lack of equipment and technology that enables storing such big data. Thus, criticism of the law was not about the increased restrictions on information freedom, but the inability of services providers to comply with the law as well as the enormous costs that would be incurred in so doing. These costs, it was argued, would lead to the bankruptcy of many Internet companies.

The bigger telecom operators, such as MegaFon, MTS, Veon (former VimpelCom) and Tele2, estimated that more than 2.2 trillion rubles (about $39 billion USD) will be required to organize the storage of message content. This amount is equal to 10% of the Russian state budget. On 14 April 2017, the FSB and the Ministry of Communications estimated that the cost of compliance for communication operators will amount to USD $79.5 billion, which is three times more than the gross revenue was for the entire Russian telecommunications industry in 2016. Moreover, the Ministry of Communications noted that the state does not plan to offer telecom operators compensation for implementations aimed at complying with the “Yarovaya Law”. As a result of these steep costs, the operators have been proposing different alternatives to mitigate the proposed legal requirements and lower the associated costs. One such alternative is a gradual implementation of the law’s provisions. Nevertheless, the exact costs can be determined only after the government specifies terms and volumes of data storage, as well as what information should be collected and stored.

In January 2017, The Russian Ministry of Communications proposed to reduce tenfold the amount of information that should be stored by the “Yarovaya Law”. At the same time, while the business sector representatives, in cooperation with the Ministry of Communications, are looking for compromises, the position of the legislative and the judicial branches remains unchangeable: it is impossible to repeal a “fundamental law that protects Russians from the global threat of terrorism.”

Moreover, The Russian Federal Security Service (FSB) opposed the pilot testing of the “Yarovaya law” and the phased-out introduction of legislated requirements. The FSB believes that all the technical details for implementing the law have already been created. By 30 June 2017, the FSB plans to submit a regulatory act specifying details on how and in what format data could be stored by Russian operators.
Our review of the “Yarovaya Law” one year after its introduction has revealed two simultaneous trends: while on the one hand, critics of the law are trying to reduce its effects, by proposing amendments which might liberalize it or exclude some of its provisions, on the other hand, the adoption of the Yarovaya Law inspired Russian legislators to produce new bills and laws that increase state control over the Internet and ICT industry. Some of these legal acts and activities are presented below:

- The Russian Ministry of Communication developed rules for restricting access to undesirable content that allows Roskomnadzor to block websites. New instruction will help to avoid situations when blocking one blacklisted website leads to the disruption of all websites on the same IP address.
- The Federal Antimonopoly Service (FAS), Roskomnadzor, and other agencies are working on a new bill, which will be submitted this spring. The document will allow the courts to slow down access to sites that violate Russian law.
- The Russian government will establish a new cyber intelligence unit within the Federal National Guard Troops Service, also known as the Russian Guard. The unit will identify threats to Russian information security, react to cyber-attacks, and monitor social networks for extremist propaganda online. There is a plan to create an integrated system for web space monitoring. It is worth noting that the Russian Guard is gradually transforming into a security agency.
- At the end of March 2017, as part of the “Yarovaya Law” implementation, the Ministry of Communications prepared a draft amendment to the rules for telecommunications services providers. The draft includes a proposal to require subscribers to list all possible users of communication devices and verify their personal data.

**REGIONAL IMPACT OF THE “YAROVAYA LAW”**

The “Yarovaya Law” also influenced neighboring legislators. For example, in the Kyrgyz Republic the Law “On Amendments to some Legislative Acts (The Civil Procedure Code of the Kyrgyz Republic, the Law of the Kyrgyz Republic “On Countering the Extremist Activity”)” was adopted. This law enables temporary restriction of access to materials containing extremist content.

The Unified Switching Center of Electronic Communication was created in Tajikistan. The purpose of the center is to ensure national and information security and to control “gray traffic” and telephone conversations. However, experts think this law increases state control over telecom operators, rather than combating terrorism.

Ukraine is now developing its own bill that will enable law enforcement bodies greater access to personal information of citizens. Operators and providers would be required to store data for 90 days.

The “Yarovaya Law” triggered a regional trend in increasing state control over the ICT sector. States are aiming to increase state security under the umbrella of combating terrorism and other societal threats.
CONCLUSION

A year after the introduction of the “Yarovaya Law”, the cost of “security” seems to be high. It appears that Russian authorities are trying to achieve state security at the expense of societal freedoms and industry. According to a recent study by Digital.Report entitled The Cost of Freedom and Security 2016 Index of ICT legislations in Eurasia, involving the survey of 50 ICT experts, the “Yarovaya Law”, in fact, does not actually enhance the security of Russia if the issue is considered systemically. The expert community believes that while state security may have increased, at first glance, it was achieved at the expense of reducing freedoms and high implementation costs to industry. As a result, the cumulative effect on security overall was still negative. Therefore, it appears that the Russian state is the only beneficiary of the “Yarovaya Law” and only in the sphere of security, despite the official position that the law aims to protect citizens from terrorism.

YAROVAYA LAW GRADING AT A GLANCE

DR Analytica’s 2016 ICT Index “Cost of Freedom and Security” found that the only positive ranking for the “Yarovaya Law” was in State Security, whereas the lowest ranking was in the Economic Effect for Industry.

<table>
<thead>
<tr>
<th>FREEDOM</th>
<th>SECURITY</th>
<th>ECONOMIC EFFECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATE</td>
<td>-1.00</td>
<td>1.75</td>
</tr>
<tr>
<td>BUSINESS</td>
<td>-3.88</td>
<td>-1.13</td>
</tr>
<tr>
<td>SOCIETY</td>
<td>-3.00</td>
<td>-1.38</td>
</tr>
<tr>
<td>INDIVIDUAL</td>
<td>-3.88</td>
<td>-1.50</td>
</tr>
</tbody>
</table>

We will continue to monitor the Yarovaya Law. Watch for an update after the Spring session of the State Duma.
WHAT WE CAN DO FOR YOU?

DR Analytica is your gateway to ICT markets and services in Eurasia.

1. REAL-TIME MONITORING
   Stay up-to-date on all of the latest regulatory and legislative developments in Eurasia. Our Weekly Digest and quarterly country analysis cover telecommunications, information and cyber security, data retention and privacy, E-government, and intellectual property. Clients also benefit from real-time alerts to keep informed about breaking developments.

2. SPECIALIZED ANALYSIS
   Discover a gateway to specialized data and analysis of how changes in laws and regulatory requirements affect markets for ICT services in Eurasia. We collect original and unique market data through open sources and privileged access. Our unique, client-customized and data-driven reports provide clear and concise impact assessments to assist clients with strategy development and investment decisions.

3. EXCLUSIVE CONSULTING
   We work with leading legal and industry experts throughout Eurasia providing exclusive research and advisory services tailored against our clients’ exacting requirements. Our unparalleled reach into industry, policy and decision-making communities offer clients exclusive access and discrete advice necessary to support key market decisions.

4. TAILORED CYBERSECURITY - YOUR “SWORD AND SHIELD”
   We provide specialized and discrete services for clients requiring state-of-the-art cybersecurity solutions and advice. Working with the best leading experts and solution providers, we offer the evaluation of threats and risks, in-depth penetration testing and provision of discrete, vetted recommendations that address clients’ specific needs. Clients benefit from detailed assessments of existing vulnerabilities, and strategies and solutions to address them.
REFERENCES


12 RosBalt.ru, “Rosgvardia Has Acquired Cyber Intelligence” [in Russian], March 16, 2017, [http://www2.rosbalt.ru/russia/2017/03/16/1599053.html](http://www2.rosbalt.ru/russia/2017/03/16/1599053.html)


