Secrecy of Communication VS «Yarovaya package» and Its Impact on Civic Engagement
# TABLE OF CONTENTS

Introduction ..................................................................................................................................................3  
Part 1. SORM as the first step towards the «Yarovaya Package» ..................................................5  
Part 2. "Yarovaya Package" ......................................................................................................................12  
Part 4. Other provisions of the "Yarovaya Package". Fast facts .........................................................47  
Part 5. Security of communication services and Internet users is in the hands of the users. Risks and recommendations from NGO activists and civil activists. ........................................53  
Conclusion ................................................................................................................................................56  
General information and partners .............................................................................................................58
Introduction

Over the last few years the Russian government has been rigorously infringing the rights of the citizens, which includes the reinforcement of control over the secrecy of communication. As a result, the Government got almost unlimited access to personal data, correspondence, telephone communications and Internet connections of the citizens.

On July 20, 2016 "Yarovaya Package", composed of two laws, came into force. First of all, this law is designed for legalization of the existing control systems to track the citizens’ activity in the Internet and to wiretap their telephone calls. The law also enforces requirements to the Internet surveillance system, including requirements to the Internet providers.

The increasing government control over the private life raises a lot of concerns among members of the human rights community, as such intrusion on people's privacy of correspondence (right to respect for private life) does not comply with the international requirements, regulations of the United Nations and the European Court of Human Rights.

On the one hand, for the purpose of efficiently fighting against crime the Government, on the basis and according to explicit procedures, is entitled to infringe citizens' privacy of correspondence in order to obtain information regarding planned or committed crimes.

On the other hand, in the absence of the efficient judicial system and in the situation when the citizens are not able to detect whether they are being wired and to cease such practices in court in case these actions are illegal, total government control over the private life becomes unjustified and arbitrary, which testifies to the unjustified government intrusion on the private life of its citizens.

This total control cannot be justified only by combating terrorism, as long as this objective cannot be reached by establishment of a total surveillance.

Everyone who may fall victim of such control, shall have guarantees for the protection from arbitrary intrusion, which do not exist in Russia.

The present report is the first analytical investigation, which provides factual as well as legal information on the impact of the «Yarovaya Package» on civil activity. The report will focus on the newest history of formation and development of the state control institution, designed to supervise private life and secrecy of communication of its citizens, innovations of «Yarovaya Package» in relation to the judgment of the Grand Chamber of the European Court of Human Rights in Roman Zakharov v. Russia, which established that there were no guarantees against abuse of the people’s secrecy of communication, which is an integral part of their private life. Apart from that, the report provides recommendations for civil activists on information security measures in the current situation.

All the information provided in the report is available on open sources which have an unlimited free access.

This report will be useful to all, without exception, civil activists, representatives of non-commercial organizations, lawyers, information security specialists, Internet investigators and to anyone who takes care of his or her information security.
Part 1. SORM as the first step towards «Yarovaya Package»

Surveillance system of correspondence, telephone communications, postal, telegraph and other communications transmitted via electronic and postal means of communication was implemented in Russia long ago and is called "System for Operative Investigative Activities» (hereinafter referred to as SORM). This system, in fact, is an intrusion on people's privacy.

Since its implementation, Russian Government has adopted and implemented three technical systems: SORM-1, SORM-2 and SORM-3. They are designed to secretly obtain information about the citizens in the course of operative investigation activities or investigation of criminal cases conducted by law enforcement authorities (namely the Russian Federal Security Service (FSS), and in cases when FSS has operational and technical constraints on-site investigation is conducted by internal affairs agencies of Russia\(^2\), including on behalf of other agencies involved in the operative investigation activity)\(^3\).

SORM can be implemented in the course of operative investigation activities following a court decision, based on information obtained by law enforcement authorities regarding:

- **signs** of a criminal offence that had been committed or was ongoing, or was being plotted which requires preliminary investigation;
- **persons** conspiring to commit, or committing, or having committed a criminal offence;
- **events**, or **acts or omissions**, that threaten state, military, economic, information or environmental security of the Russian Federation.

Law enforcement authorities may apply SORM without a previous court decision in the following cases:

- urgent cases that may result in a serious or particularly serious offence,
- when law enforcement authorities receive information regarding events, or acts or omissions, that threaten state, military, economic, information or environmental security of the Russian Federation.

The above mentioned criteria are evaluative, and may of course result in the arbitrary application of SORM, which constitutes unjustified intrusion on private life.

\(^2\) Order of the President of the Russian Federation as of 01.09.1995 №891 "On the streamlining of organisation and implementation of special investigation activities with the use of technological equipment".

\(^3\) Article 6 of Federal Law as of 12.08.1995 N 144-FZ (rev. dd. 06.07.2016) "On operative investigation activity". 
In case when law enforcement authorities fail to obtain a court decision to implement SORM, they may conduct surveillance of correspondence acting on their own initiative within 24 hours upon notification provided to court. In general, SORM may be implemented by law enforcement authorities without a correspondent court decision for a period of up to 48 hours, after which such activities shall be ceased in case of failure to provide a correspondent court decision.

In case of court approval of SORM implementation, data obtained as a result of implementation of the system shall be used as evidence in case criminal proceedings are initiated.

Courts usually grant requests to authorities for restriction of constitutional rights to secrecy of correspondence, telephone communications, postal, telegraph and other communications transmitted via electronic and postal means of communication in the course of investigation or operative investigation activity. This information is confirmed by the official statistical data regarding courts activity

In accordance with the official statistical data, the number of applications to court from pretrial investigation agencies and investigation units constantly increases. From 2010 to 2014 the number of such applications increased more than twice.

Table 1. Court authorizations for restriction of constitutional rights to secrecy of communication in Russia

<table>
<thead>
<tr>
<th>Name of Procedure</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operative investigation activity</td>
<td>180.3 thousand / 95.1 %</td>
<td>205.2 thousand / 98.6 %</td>
<td>231.2 thousand / 99.2 %</td>
<td>244.7 thousand / 99.98%</td>
<td>290.8 thousand / 98.5%</td>
</tr>
<tr>
<td>Investigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Granted by court</td>
<td>103.0 thousand</td>
<td>121.8 thousand</td>
<td>141.8 thousand</td>
<td>170.5 thousand</td>
<td>No data available</td>
</tr>
<tr>
<td>Total number of applications:</td>
<td>203 thousand</td>
<td>327 thousand</td>
<td>373 thousand</td>
<td>415.2 thousand</td>
<td>-</td>
</tr>
</tbody>
</table>

The European Court of Human Rights (hereinafter referred to as ECtHR)\(^5\), upon review of SORM implementation in Russia in case of Roman Zakharov v. Russia\(^1\) concluded that Russian legal provisions do not provide for adequate and effective legal guarantees for the citizens, because the circumstances in which public authorities are empowered to resort to secret operative investigation activities are not defined with sufficient clarity, neither the provisions on discontinuation of secret surveillance measures and circumstances, when the intercept material shall be destroyed;

At the same time there is no effective supervision of proportionality and relevance of SORM implementation, and there are no effective remedies in place for the citizens. ECtHR decided that the existence of SORM in Russia constitutes a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular it constitutes an unjustified interference of Government with the exercise of the right to respect for private and family life.

---


\(^5\) Judgement of the Grand Chamber of the European Court of Human Rights as of 04.12.2015 on the case of Roman Zakharov v. Russia (Application №47143/06).
1.1. SORM-1

SORM - «System for Operative Investigative Activities» - was implemented in Russia for the first time in 1992. This system allows surveillance and wiretapping of telephone and other types of communications, obtainment of information using technical communication channels\(^5\).

In compliance with Order of the Russian Ministry of Communication №226 dated as of 24.06.1992, heads of communication companies and organizations of the Russian Federation shall provide the following information to operational and technical departments of the Ministry of Security of the Russian Federation under written or oral agreements: service rooms with necessary communication equipment and power supply; lines, channels, cable constructions and other necessary equipment, enabling their uninterrupted availability; necessary data from information and reference systems and settlement centers of the Ministry of Communication of the Russian Federation.

Technical requirements to the system of technical means, enabling operative investigation activities at electronic automatic telephone stations (SORM)\(^6\), were enacted on the 11th of November 1994 and became an integral part of the requirements to the procedure of granting licenses for communication services provision. In case of failure to comply with these technical requirements, the license could not be granted, while existing licenses could have been revoked.

SORM-1 is designed for obtainment of information regarding telephone communications of specific clients who are using landline connections of public telephone networks. Therefore, surveillance of telephone communications using SORM-1 can be conducted only in case a connection is made via automatic telephone station.

SORM-1 is not used currently due to the existence of more modern systems, SORM-2 and SORM-3, however its usage is technically possible.

It is worth mentioning that SORM-1 does not allow to monitor all the customers. SORM-1 functional requirements imply a simultaneous wiretapping of a certain number of customers depending on the automatic telephone station capacity. For instance, if the station’s maximum capacity is 10 000 customers, SORM is able to monitor no more than 128 customers. If the station’s capacity is higher, the maximum number of monitored customers is 1 024, while the maximum number of simultaneously monitored customers is even lower.

Requirements to electronic automatic telephone stations are the following\(^7\):

<table>
<thead>
<tr>
<th>Number of customers monitored</th>
<th>Number of customers simultaneously monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>28</td>
</tr>
<tr>
<td>256</td>
<td>56</td>
</tr>
<tr>
<td>512</td>
<td>112</td>
</tr>
<tr>
<td>1024</td>
<td>168</td>
</tr>
</tbody>
</table>


\(^6\) Technical requirements to the technical means of communication, enabling operative investigation activities at electronic automatic telephone stations (SORM) were approved by the Deputy Minister of Communications of the Russian Federation Krupnov A.E. on 19.09.1994; enacted on the 11th of November 1994 by the instruction of the Ministry of Communications of the Russian Federation “On implementation of SORM at communications networks of the Russian Federation”.

\(^7\) Ibid.
The system implementation algorithm is the following: law enforcement authorities shall be enabled to promptly access an automatic telephone station equipment, connect to communication channels, wiretap and record the information from their operational post, which may be located outside the territory of the automatic telephone station. Commutation providers shall be able to guarantee the transmission of this information to law-enforcement authorities via exchange channels at the distance of up to 16 km.

Law-enforcement authorities get access to the following information via SORM-1:

- **outgoing and incoming calls** (local, zonal, inter-city and international) from/to certain customers of a station, as well as control over calls to predetermined numbers of the telephone network when outgoing calls are coming from the customers of this telephone network;
- control over calls when customers are provided with additional services, readdressing a call or changing its numerical information (short-code dialing).

SORM-1 allows law enforcement authorities exercise full as well as statistical monitoring.

In the course of full monitoring law enforcement authorities get a real-time access to information regarding telephone connections of a supervised person, including time of the beginning and end of a conversation, and its content.

In the course of statistical monitoring law enforcement authorities get a real-time access to information regarding telephone calls of a certain customer to a certain number (without information regarding content of conversations), as well as to information regarding connections of certain customers to predetermined telephone numbers.

Data transmission technologies were developing over time, mobile communication became widely available, in light of the above the Government modernized the systems of control over private life of citizens and created SORM-2.

### 1.2. SORM-2

This system was officially implemented in Russia in 2000. In the beginning the system was designed to monitor not only telephone communications via land line, but also mobile communications.

**Information monitored:**
- telephone calls made via land line, and their content;
- IP telephony.

Since 2008 SORM-2 started to monitor the Internet, but to a limited extent:
- information regarding mobile Internet connections;
- location of mobile communication subscribers;

---

8 Order of the Russian Ministry of Communications №70 dated as of 20.04.1999 “Technical requirements to the system of technical means in the course of operative investigation activities on the telecommunication networks of the Russian Federation”;
Order of the State Committee of Telecommunications of the Russian Federation №15 as of 09.07.1999 “SORM technical requirements in trunking communication systems of mobile communication services”;
Order of the Russian Ministry of Communication №130 dated as of 25.07.2000 “Rules of Implementation of the system of technical means in the course of operative investigation activities on the networks of telephone, mobile and wireless connections and personal radio calls of public use”.

Right to privacy VS «Yarovaya package» and its impact on civic engagement, November 2016

- Internet users traffic, while the intercepted traffic was lately associated with a certain user;
- email addresses,
- information regarding web sites visited and credit card transactions;
- recording SMS content, as well as data transmitted via messengers, including WhatsApp\(^{10}\) and Skype\(^{11}\).

SORM-2 conducts analysis of a certain user depending on the application layer protocol, as well as identifies the location of a switched on mobile phone by its number.

Such data may be stored by law enforcement authorities for up to 3 years.

In order to implement SORM-2 communication providers needed to draft its implementation plan and have it approved by a local FSS branch\(^{12}\). All the associated works needed to be confidential and conducted by a restricted number of specialists upon FSS approval.

Communication providers were obliged to purchase all the equipment required for SORM-2 operation, otherwise, their licenses could be revoked\(^{13}\). The Government justified SORM implementation by the necessity to protect national security.

On January 1, 2006 the Russian Government issued a protocol for liaison between communication providers and authorized government bodies, FSS and the Ministry of Foreign Affairs, which conduct operative investigation activity. The regulations regarding SORM operation were strengthened\(^{14}\).

In particular, the new provision prescribes that every communication provider (Internet provider) shall ensure a timely update of its client’s database, including services provided. The above-mentioned information shall be stored by communication providers for 3 years, while FSS or MFA bodies shall be granted a 24 hours’ remote access to databases.

Regularly updated information about the clients includes the following:
- personal information, such as full name, place of residence and information regarding a primary ID provided upon subscription;
- information about legal entities, such as name (trade name) of the legal entity, its location, as well as the list of persons using its terminal equipment, certified by a designated official of the legal entity, containing full names, places of residence and information regarding a primary ID;
- information about all the subscribers, including database information regarding all the services provided, traffic and payments made.

\(^{10}\) At the moment in accordance with the information provided by the developers and investigators WhatsApp is a safe communication tool. 19.02.2014. Facebook announced the acquisition of WhatsApp. In April 2016 a new version of WhatsApp 2.16.12 included end-to-end encryption for all the users, which means that the data transmission via this messenger became secure. However there are no guarantees that the information transmission before this date was also secure.

\(^{11}\) http://alibi-detective.ru/informatciia/sorm-kto-i-zachem-provodit

\(^{12}\) Order of the Russian Ministry of Communications №130 dated as of 25.07.2000 “Rules of Implementation of the system of technical means in the course of operative investigation activities on the networks of telephone, mobile and wireless connections and personal radio calls of public use”.

\(^{13}\) For example, the award of the Arbitration Court of the city of Moscow as of 08.02.2006 on case №A40-79723/05-96-515.

\(^{14}\) Decree of the Government of the Russian Federation as of 27.08.2005 N 538 “On approval of Regulations for communication between communication providers and authorized government bodies, conducting operative investigation activities”. 

All the information shall be attached to a certain customer, and can be lately used by the special services to identify all the activities conducted by this individual in the Internet, including web pages visited and other information.
Some specialists claimed that FSS is not able to monitor all the Internet users traffic, that is why SORM-2 was programmed to monitor the Internet traffic in accordance with key words from a predetermined vocabulary.

Technical capabilities were restricted, and the record of traffic by communication providers was not included in the system; FSS was able to record it upon receiving such data via communication channels between FSS operational post and communication providers.

In 2013 Vympelkom announced that the annual investment in SORM equipment would be $100 million. MTS estimated that such expenses would be around RUB 300 million annually. It is obvious that the subscribers had to cover these costs.

1.3. SORM-3

SORM-3 system was implemented by decree №83 of the Russian Ministry of Communications as of 16.04.2014 and is applied since April 1, 2015. It is designed to integrate all the capacity of SORM-1 and SORM-2, as well as to further development of the Internet control.

SORM-3 implies that communication providers record (and subsequently transfer to law enforcement authorities) the following information:

- **the Internet:**
  - static and dynamic IP addresses of subscribers;
  - subscribers’ logins to access communication services;
  - emails of subscribers, in case email services are not encrypted;
  - subscribers’ emails from the following domains: mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com, aport.ru, rupochta.ru, hotbox.ru, in case such services are not encrypted;
  - telephone numbers (logins) for message services, including ICQ;
  - equipment MAC-addresses;
  - browsing history.

- **telephony:**
  - subscriber’s telephone number (calling and (or) called number);
  - subscriber’s mobile number;
  - subscriber’s location (including cases when the Internet phone such as Skype is used).

One SORM-3 system installed at one technical unit of a communication provider allows to control the citizens using more than 2000 above mentioned parameters, such as login, telephone number, etc. This means that SORM-3 system, as well as its previous analogues, is not designed to control all telephone or Internet connections, however it allows to monitor up to 2000 subscribers at one technical unit of a communication provider. In case a communication provider has many technical units of SORM-3 installed, it is technically possible to control the secrecy of communication of all subscribers of a certain communication provider.

There have been cases when mailboxes, belonging to famous civic activists and located at insecure mailbox servers, were hacked and the content of correspondence was published at the Internet.

Such unauthorised information distribution was reducing the effectiveness of work of civic activists, because their opponents were getting informed about their plans and were trying to take appropriate actions.

While there was no illegal information detected in such correspondence, activists had to rearrange their campaigns.
SORM-3 operation principle is the transmission of selected information by a communication provider to a system installed at the operational post of law enforcement authorities. Equipment installed by a communication provider records all the data packages received and stores them for no less than 12 hours, while FSS can copy all the data during this period for later analysis.

The system establishes certain technical requirements to data transmission speed from operator to operational post of law enforcement authorities. SORM-3 has increased capacity comparing with the previous versions, for instance it has a wider range of information collected as well as a wider range of types of communication which the system is able to monitor.

It should be pointed out that SORM-3 can access the content of mailboxes only in case an email service is not using encryption. This is why it is important to use encrypted email services to avoid unauthorised access to a mailbox. SORM-3 does not have decryption systems for protected communication channels.

As we see, a monitoring system for messages and calls of Russian citizens existed before July 2016 when "Yarovaya Package" was adopted. By-law documents were regulating the system functionality. As soon as "Yarovaya Package" was adopted, the system was legally established.

FSS was provided with an instrument to obtain a huge amount of information about Russian citizens, however SORM functionality was restricted by its technical capacity and impossibility to access the information transmitted via encrypted communication channels. "Yarovaya Package" took a step forward to change this situation.
Part 2. "Yarovaya Package"

2.1. "Yarovaya Package": what, why and how?

Laws, officially authored by a State Duma deputy I.A. Yarovaya, became publicly known as laws regarding total surveillance of citizens in the Internet.

The content of these laws is correspondent with its widespread name, however, their scope is much wider.

On July 24, 2016 the State Duma adopted these federal laws in their final reading:

- "On the Amendments of the Federal Law "On Countering Terrorism" and separate legal provisions of the Russian Federation as regards additional measures to counter terrorism and to ensure public safety" (№374-FZ as of 06.07.2016);
- "On the Amendments of the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation with regard to establishment of additional measures to counter terrorism and to ensure public safety" (№375-FZ as of 06.07.2015).

5 days later these laws were already approved by the Federation Council of the Federal Assembly, on the 6th of July 2016 they were signed by the President of the Russian Federation, and entered into force on the 20th of July 2016.

SORM was legalized since this day in accordance with Federal Law №374-FZ as of 06.07.2016. Surveillance of citizens started to be conducted on the basis of the Federal Laws.

Draft laws were submitted to the Federal Parliament by Deputies of the State Duma I.A.Yarovaya, A.K. Pushkov, N.V. Gerasimova; by a member of the Council of Federation V.A. Ozerov and adopted by the State Duma in their first reading in May 2016, and 1,5 months later they were adopted in their final reading. The law package was named "Yarovaya-Ozerov Package", however in the media it was called "Yarovaya Package" (hereinafter referred to as the Law).

The Laws adopted not only regulate FSS rights to control the secrecy of communications of the citizens, but also establish additional restrictions for personal rights of individuals, such as:

- restrictions on the right for secrecy of communication (right to respect for private life);
- strengthening of rights of law enforcement authorities to access email communications of individuals, including by FSS of Russia (hereinafter referred to as FSS);
- obligation for Internet providers to store information regarding individual communications, as well as content of correspondence; apart from that, an obligation to provide the authorities with decoding keys in case information is transferred via the Internet;
- restrictions for missionary activities;
- liability for individuals aged 14 and above for failure to inform the Government on planned crimes;
• creating opportunity for establishment of intergovernmental bodies to counter terrorism, while decisions of such bodies shall be binding on all private persons and bodies;
• obligation for local government bodies to conduct counter-terrorism propaganda.

Although the main objective of "Yarovaya Package" laws is the fight against terrorism, in general they are designed for further restriction of individual rights and freedoms in Russia, creation of a control system over secrecy of communication of the citizens, their actual deprivation of any guarantees from excessive and unjustified intrusion of the Government on their private lives.

In the last year, adoption of anti-terrorist laws in almost always result in further restrictions on the rights of citizens and creation of a total government control over their activities.

The idea of the fight against terrorism is exploited by the Russian authorities to justify their actions, intended to “tighten the screws” and to strangle civil rights and liberties.

The Law is designed to strengthen the Government control over personal data.

Firstly, in compliance with this Law FSS was granted with a right to receive any information about the citizens from the State databases and extrabudgetary funds, including personal information.

As long as FSS of Russia performs various functions, such as customs control, fight against terrorism and crime, intelligence services, provision of information security, this Law grants FSS with unlimited opportunities not only in obtaining information, but also in its usage.

This means that any information regarding kinship relations, taxes paid, property, transactions with property, payments made by Government, registration at the place of residence and any other information which other State bodies possess, may be made available to FSS of Russia, which results in a total control of this body over the citizens.

The Government grants the same rights to the Foreign Intelligence Service of the Russian Federation.

Secondly, obtainment of computer information becomes one of the types of operative investigation activities, i.e. activities, conducted by law enforcement authorities of the Government in public or privately, including cases when there are no grounds for initiation of a criminal case, but there is information that a criminal offence has been committed or is ongoing, or is being plotted.

Thirdly, air operators are obliged to comply with the requirements of the Russian Government for such databases and their maintenance, which means that apart from the customs control FSS of Russia in entitled with unlimited access to track movements of the citizens in real time.

The same regulations come into force in Lithuania starting from January 1, 2017.

"Lithuanian authorities claimed that information collection is necessary to investigate criminal offences that had been committed or were ongoing, or were being plotted.

New regulations will affect all the passengers who are entering or leaving the Republic. The information to be collected by the operators include full name, date of birth, gender and citizenship, as well as a unique passenger code, information regarding visa or other document granting permit to stay at the territory of the country. Law enforcement authorities will be also provided with information regarding
contact address of a passenger, his/her registration status, all the information regarding the ticket, luggage and seat number, as well as contact information of a person who purchased the ticket. Airlines will be obliged to provide the police with all the information related to the flight.

Collection of passenger information in Lithuania is prescribed by the Transport Code. In accordance with this document, airlines shall collect passenger information at least 48 hours before the flight. They shall register the information and provide it to law enforcement authorities.

Regulations, which oblige operators to collect passenger personal data, were adopted in the EU in April 2016. EU Justice and Home Affairs Council justified the regulations with a necessity to counter terrorism. The authorities think that collection of air passengers’ information shall contribute to the crime prevention and identification of signs of terrorism or planned crimes. This information shall also be helpful for law enforcement authorities in the course of their investigations.

At the adoption of the regulations members of the EU Council guaranteed protection of passenger personal data, as well as relevant fundamental human rights. The chairman of the European Parliament, Martin Schulz, informed that the information will be stored for no more than six months. Database access was promised to be restricted, while there were responsible individuals in charge.\(^\text{15}\)

The difference between collection and usage of such information in Russia from countries of the EU is that in the context of a developed democracy illegal usage of such data is impossible. Collection and usage of such information is strictly controlled in Europe. Citizens have a possibility to challenge unlawful actions in courts, which in accordance with investigators are more independent, while a system established to prevent cases of unjustified restrictions of civil rights is generally effective.

**The Head of the Center for Support of Indigenous Peoples of the North, Rodion Sulyandziga, claimed that before his flight abroad on the 18th of September 2014 the Russian border service in Sheremetyevo Airport took his passport and gave it back later with one page cut out. The border service department initiated an administrative case against him regarding a document deterioration, so Sulyandziga could not leave the country because his passport was invalid. As a result, he could participate in the first World Conference on Indigenous Peoples organized by the UN.**\(^\text{16}\)

In Russia such guarantees do not exist, therefore information regarding flights may be used in the way that law enforcement authorities consider convenient or appropriate. The citizens will not be aware why, by whom and when such information was received in fact, how it was used, while there are no effective measures in place to prevent an open sale of this information on the black market.

**Fourthly,** all the complex of measures implemented results in arbitrary intrusion of the Government, while there are no protection mechanisms from it: the Government establishes a total control over its citizens while there are no effective legal mechanisms in place to prevent unjustified intrusion.

### 2.2. "Yarovaya Package" and total surveillance of citizens in the Internet at the territory of the Russian Federation.

Laws adopted legalize SORM and implement new restrictions for citizens, as well as for telephone and Internet communication providers.

Restrictions of civil rights and problems, resulting from the adoption of "Yarovaya Package", have not been fully appreciated even by its authors.

---


\(^\text{16}\) http://www.bbc.com/russian/international/2014/09/140922_un_indigenous_russia_conference
First aspect. Requirement to store all the information regarding usage of telephone and Internet services provided to the citizens

From July 20, 2016 life of everyone, who is using communication services at the territory of Russia, changed. There is no privacy anymore. At all.

The requirement to store information regarding connections, as well as regarding their content, affect two big groups of telephone and Internet providers:

1. communication providers (operators of fixed-line and mobile services, Internet providers);
2. organizers of information distribution in the Internet (including individuals or entities, ensuring functionality of information systems and (or) software programs for computers, used for receiving, delivery and (or) processing of electronic messages of Internet users), i.e. these are Internet platforms for information exchange, information portals, ensuring receiving, delivery and (or) processing of electronic messages, special Internet services, including operators of various messengers; email web pages; internal portals with a function of communication between its users; Internet forums).

While communication providers conduct their activities on a basis of a license, organizers of information distribution in the Internet shall inform Roskomnadzor regarding the start of their activities in that capacity acting on their own initiative or on a petition of Roskomnadzor, based on a petition of FSS of Russia or other agency conducting operative investigation activity.

Vadim Ampelonsky, representative of Roscomnadzor commented to RBC on 18.06.2014 that “organizers of information distribution” in the Internet are not only popular social platforms, such as VK or LiveJournal.com, but also personal blogs in case they have a function of information exchange between its users, such as comments, forums, etc.

In that way, “organizers of information distribution” in the Internet are, for example, “Sputnik i Pogrom” (sputnikipogrom.com), Alexey Navalny website (navalny.com), «Perzident Roissi» (kermlinrussia.com), Nikolay Starikov website (nstarikov.ru), etc.

Due to ambiguity of the term "organizer of information distribution in the Internet", basically any website or service with a function of information exchange between users can be considered eligible.

Meanwhile such huge international companies as Google, for example, are not included in the list yet.

17 Paragraph 1 Article 10.1 of Federal Law as of 27.07.2006 N 149-FZ (rev. dd. 06.07.2016) "On Information, Information Technologies and Information Protection".
19 Paragraph 2 Article 10.1 of Federal Law as of 27.07.2006 N 149-FZ (rev. dd. 06.07.2016) "On Information, Information Technologies and Information Protection"; Decree of the Government of the Russian Federation as of 31.07.2014 N 746 “On approval of Regulations for organizers of information distribution in the Internet of notification of the Federal Service for Supervision of Communications, Information Technology and Mass Communications regarding the start activities to ensure functionality of information systems and (or) software programs for computers, used for receiving, delivery and (or) processing of electronic messages of users of the information and telecommunication network of Internet, as well for keeping the register of the above mentioned organizers".
In case organizers of information distribution in the Internet ignore Roskomnadzor requirement, they will be subject to pay an administrative fine in the amount from RUB 1 000 to 3 000 for individuals, from RUB 10 000 to 30 000 for officials, from RUB 100 000 to 300 000 for legal entities. This regulation entered into force on 01.08.2014, and there have already been judicial decisions enforced in relation with it. "Yarovaya Package" has not amended this regulation, however it established new obligations for organizers of information distribution in the Internet.

Beeline, MTS, Megafon and all other providers will need in total 40.6 million of 10 TB hard disk drives (HDDs) and 30.5 millions of 1.6 TB solid-state drives (SSDs). Apart from that, the companies will need 565 thousand items of various network equipment: switchboards, routers and firewalls.

At the same time, at the international market in the first quarter of 2016, in accordance with Trendfocus, there were sold 30.7 million of SSDs, with a total capacity of 10 EB. The number of HDDs, sold in 2015, totaled 469 millions, with a total capacity of 538 EB in accordance with Trendfocus.

"It is evident that not all the equipment required in accordance with the regulations is produced in Russia. Moreover, certain types of hardware and software complexes, for example the ones required for acquisition, inventory and storage of domains of information are not produced neither in Russia, nor in the world," - informed Dmitry Solodovnikov, MTS representative.

Not all the organizers of information distribution in the Internet are included in the Roskomnadzor list. For example, VK social network (vk.com) and mail.yandex.ru were the first ones to be included, however there is no information in the list regarding mail.ru service and facebook.com.

On the 12th of August, 2014 rules of interaction between organizers of information distribution in the Internet and bodies conducting operative investigation activity (hereinafter referred to as OIA) or ensuring security of the Russian Federation, established by the Russian Government, came into force. From this date in case an organizer of information distribution in the Internet is included in the Roskomnadzor list, it shall upon requirement of FSS or OIA bodies use equipment and programmes allowing to monitor correspondence of individuals and organizations in the Internet (and starting from 01.07.2018 also the content of such correspondence), as well as keep such methods and mechanisms confidential.

In case of failure to comply with provisions of the Code of the Russian Federation on Administrative Offences from the 1st of August 2014 administrative punishment in a form of administrative fine shall be imposed in the amount from RUB 3 000 to 5 000 on individuals; from RUB 30 000 to 50 000 on officials; from RUB 300 000 to 500 000 on legal entities.

---

21 For example, judgement of the Seventh Court of Appeal as of 12.05.2016 N 07AP-2621/2016 case N A45-27089/2015.
23 As of 23.10.2016.
24 Decree of the Government of the Russian Federation as of 31.07.2014 N 743 “On approval of Regulations for communication between organizers of information distribution in information and telecommunication network of Internet and authorized government bodies, conducting operative investigation activities or ensuring security of the Russian Federation”.
**Second aspect. Storage of information regarding receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other messages of clients of telephone services, as well as of the Internet.**

In compliance with the "Yarovaya Package" providers of telephone services, as well as Internet providers shall record information regarding receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other messages of customers of telephone services, as well as the Internet for three years from the time of such actions. These include providers of telephone service (fixed-line and mobile), Internet providers and providers of Internet messengers.

This means that the information regarding web pages visited by a user, the calls he/she made, to whom he/she sent email, to whom he/she wrote in Viber, Skype or any other messenger, will be recorded and stored by a provider for 3 years. It basically means the establishment of a total government control over private lives, which cannot be justified in a constitutional and democratic state.

Under the law all the information regarding information transmissions can be stored, and not on a selective basis, as it was in cases of SORM-1, SORM-2, SORM-3. This regulation came into force on the 20th of July 2016, and since this date communication providers shall "watch" after their subscribers and record information regarding all their connections. However, even before the adoption of the "Yarovaya Package" such control system existed, but it had some limitations, as shown before.

"Yarovaya Package" does not establish any administrative liability for communication providers in case of refusal to collect and store such information, because it is pointless: the Government has a "zero tolerance" policy for communication providers in case they commit any breach: their license is revoked straight away, and they have to terminate their business activity.

"Yarovaya Package" obliged communication providers to provide information to bodies, conducting operative investigation activity, or ensuring state security of the Russian Federation, regarding subscribers of communication services and services provided to them, as well as other information, necessary for implementation of their tasks. From July 20, 2016 FSS of Russia received unlimited access to information about the citizens, as long as now FSS is entitled to receive this information on its own initiative even beyond operative investigation or criminal procedural activities. FSS is able to receive such information outside any judicial control, which means that the citizens will not know, what kind of information FSS have received about them and how it used this information, while FSS itself will exercise control over the legality of provision of such information.

"Yarovaya Package" increased the fines for communication providers, in case they fail to identify their subscribers according to the established procedure, or in case they identify them in violation of such procedure. From July 20, 2016 the amount of the fine is the following: from RUB 2 000 to 5 000 for individuals; from RUB 5 000 to 50 000 for officials; from RUB 100 000 to 200 000 for legal entities.²⁶

Subscribers identification and access to such information are necessary for intelligence services to identify exactly to which individual a conversation or correspondence belongs.

At the same time in compliance with "Yarovaya Package" regulations, communication providers (Internet providers, telephone communication providers and others) shall terminate services provision to citizens, in case following a request for identification from a body, conducting operative investigation activity, a provider is not able to identify the subscriber within 15 days from the date of such request.

This requirement will allow law enforcement authorities (including cases when there is no criminal proceeding in place) to identify which individual or entity is using a certain communication access point (Internet, telephone, etc.), and in case this individual or entity is not identified by a provider, to deny access to such subscriber to communication services without resort to court, which in fact means denial to access telephone of Internet services. In case a communication provider does not perform its obligations to collaborate and update subscriber’s information, or fails or denies to contact the subscriber, such subscriber will be denied access to communication services.

From July 20, 2016 organizers of information distribution in the Internet in Russia (including operators of web portals, email services, messengers, other informational resources and services) shall store information regarding receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of Internet users, as well as information regarding these users for one year from the time of termination of such actions. Reduced period of information storage comparing with communication providers is basically the only difference between communication providers and organizers of information distribution in the Internet.

It is worth mentioning that organizers of information distribution in the Internet were obliged to store this information on the 1st of August 2014, however the established
In the end of November 2016 it became known that the British Parliament passed the Investigatory Powers Act, which grants intelligence services and law enforcement authorities of the country with surveillance power over its citizens. Such situation for Europe is extraordinary, because there are no existing analogues of such strict legislation in the Western Europe. However, the Act has not been signed by Queen Elizabeth II, therefore it has not entered into force.

The law requires Internet and mobile communication providers to store subscribers’ information for 12 months, namely the information about telephone calls of the British citizens, as well as their browsing history. Governmental organisations as well intelligence services will get access to this information, while the warrant for such access is required only in a few cases. For example, when the police demands to disclose a journalist’s source.

Moreover, law enforcement services will be entitled to directly hack people’s computer systems and mobile phones. However, such actions will require a special warrant, which shall be issues by a body composed of a commissioner and a panel of judges nominated by the State.

Michelle Stanistreet, Head of the National Union of Journalists (UK & Ireland) stridently opposed the approved bill, calling it “draconian” and “an attack on democracy”. Human rights institutions have also opposed the Act, as well as the world biggest IT companies, such as Google, Microsoft and Apple. British authorities have assured that the new draft bill is just an updated version of the previous law dated 2000, which prescribes investigative powers.

storage period was 6 months from the time of clients’ actions. Upon approval of the "Yarovaya Package" the storage period of information for organizers of information distribution in the Internet was increased to 1 year. In such a way, from August 1, 2014 any messengers (viber, signal, facebook messenger and others) shall track all subscribers’ connections, information transmission via messengers and in the Internet, while their providers shall collect identification information of their users and store this information for 1 year (from July 20, 2016).

Russian intelligence services are entitled to receive any personal information of VK social network users upon request and without a court decision. Evgeny Krasnikov, the spokesman of "Vkontakte", announced this during a forum in Kazan.

"Vkontakte“ provides the intelligence services with any information regarding any user upon the first request.

Answering the journalists’ question about how the heads of the social network refer to the need to provide the correspondence of users to law enforcement agencies without a court order, Krasnikov noted that he fully supports this measure.

“I would love to hope that our law enforcement agencies and power structures, who can obtain any personal information of our users, are doing it for the benefit and protection of our country, if a drain of such communication helped to prevent serious consequences, acts of terrorism, then maybe it’s for the best,” — said the representative of “Vkontakte”.

While "Vkontakte“ does not see anything wrong with such practices and is even proud of it, Apple is fighting attempts made by intelligence agencies to find out information about their users. Recently, the FBI demanded the Corporation to hack iPhone of a shooter from San Bernardino, because it may contain information about other terrorists and a phone of a drug dealer from Brooklyn. However, the company refused to provide this information and stated that such access to personal data contradicts two amendments to the U.S. Constitution.

---

On the 13th of August 2014\textsuperscript{30} Russian Government established \textbf{types of information which shall be collected and stored by organizers of information distribution in the Internet.}

It includes:

1) user information, including a login; network address information, which was used for user’s registration, exact time of registration; other user’s information, provided upon registration; in case of registration cancellation, information regarding the case (including user ID in the communication Internet service, exact time and network address, which was used for cancellation);

2) registration form information, in case there is one;

3) information regarding sign-ins of users (i.e. entry of information by a registered Internet user into a communication Internet service to get access to the service functionality), namely:
   - information regarding sign-ins of users (including date, exact time, network addresses used);
   - other information, recorded by a communication Internet-service upon user's sign-in using sign-ins of other communication Internet-services;

4) information regarding telephone numbers, emails or other information, provided by a user upon registration, which was amended or supplemented later;

5) information regarding paid services, provided to a user (exact time of services provision, provider of paid services, information recorded by the Internet service regarding payment (currency, transaction number, payment system used and payment system identification numbers);

6) information practically collected by a communication service about a user in case the communication service allows receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of Internet users without previous registration or sign-in;

7) information regarding receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of Internet users (including exact time of receiving, delivery and (or) processing of electronic messages indicating recipients, as well as information for uncertain number of Internet users);

8) information practically collected by a communication service about organization of receiving, delivery and (or) processing of electronic messages, using electronic payment technologies,

\textbf{In compliance with the law, there are 6 federal government authorities, enabled to conduct operative investigation activities (hereinafter referred to as OIA):}
- internal affairs bodies;
- the Federal Security Service of Russia;
- the Federal Protective Service of Russia;
- the Federal Customs Service of Russia;
- the Foreign Intelligence Service of Russia;
- the Federal Penitentiary Service of Russia.
Each authority is enabled to conduct OIA only for the purposes of execution of its tasks.\textsuperscript{31}

\textsuperscript{30} Decree of the Government of the Russian Federation as of 31.07.2014 N 759 “On Regulations for organizers of information distribution in the information and telecommunication network of Internet of storage of information, related to receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of users of the information and telecommunication network of Internet, as well as information regarding these users, provision of such information to the the authorized state bodies, conducting operative investigation activity or ensuring state security of the Russian Federation”.

\textsuperscript{31}
including information:
- about money transactions (and correspondent payment system identification numbers, currency, amount paid for services or goods (if there are ones),
- other data, indicated upon payment, transactions made and payment system identification number (an "electronic wallet"),
- amounts of income or expense, as well as other data indicated at the time of transaction).

When Microsoft purchased Skype, it started to transmit the traffic via its servers, a source in a company dedicated to computer security said, which means that theoretically law enforcement authorities may have access to Skype users’ correspondence without any previous requests sent to the headquarters of the American corporation.

Maksim Emm, CEO of Peak Systems, claims that there exists a technical possibility to receive information regarding Skype users and their conversations. "Microsoft has a certain patent, which enables it to copy this information, as well as intercept VoIP calls, - says Emm, - It means that the corporation upon a court decision may provide personal data of users as well as their conversations"\(^\text{31}\).

Communication Internet services since August 2014 are obliged to collect and provide FSS of Russia, as well as other bodies, conducting OIA, and Roskomnadzor, upon their request with information regarding users’ registration and cancellation of registration, regarding all connections, including voice, text, image and video transmissions; information regarding money received via electronic wallets and payment made in the Internet. At the same time provision of such information to "appropriate" authorities by organizers of information distribution in the Internet shall be classified, the organizers are not allowed to disclose any facts or content of such collaboration.

"Yarovaya Package" enshrined the rule that organizers of information distribution in the Internet shall provide such information to the bodies, conducting operative investigation activity, and FSS of Russia upon their first request, "in cases specified by federal laws".

However, the "Yarovaya Package" granted FSS with an exceptional authority to receive information from organizers of information distribution in the Internet. In accordance with it, FSS is entitled to receive information, required for implementation of their task, from government bodies, enterprises and organizations regardless the form of ownership, free of charge, except for cases when federal laws prohibit transmission of such information to federal security services\(^\text{32}\).

From July 20, 2016 FSS of Russia in enabled to receive any information regarding private life of citizens without resort to court, in case it considers that such information shall be provided to ensure the state security, an expansive interpretation of this term may be applied to any area of social life.

It is interesting that from April 20, 2015\(^\text{33}\) Roskomnadzor was granted with a right to receive from organizers of information distribution in the Internet information regarding receiving, delivery and (or) processing of voice information, written text, written text, images, sounds, video or other electronic messages of users of the information and telecommunication network of Internet, as well as information regarding these users”.

---

31 https://www.gazeta.ru/business/2013/03/22/5112641.shtml
33 Decree of the Government of the Russian Federation as of 08.04.2015 N 327 “On establishment of Regulations for monitoring of organizers of information distribution in the information and telecommunication network of Internet, related to receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of users of the information and telecommunication network of Internet, as well as information regarding these users”. 
images, sounds, video or other electronic messages of Internet users, as well as information regarding these users. In the course of revision, it shall identify the name of the information system and (or) software programmes for computers, used by organizers of information distribution in the Internet for receiving, delivery and (or) processing of electronic messages of Internet users, domain name and (or) network address of the information resource.

Such information can be received only in the course of desk or tax review of an organizer of information distribution in the Internet, conducted by FSS of Russia or OIA bodies, or in case Roskomnadzor is planning to monitor execution of its own order issued to organizers of information distribution in the Internet. Such revisions do not require previous authorization of procurator's offices, and may be performed in respect of an organizer, included the Roskomnadzor list, as well as an organizer, not included in the list. The revision shall be conducted within 30-60 working days, which is 20 days more than a standard revision period, established for private entrepreneurs and legal entities

Upon the results of Roskomnadzor revision, three copies of an act are drafted, one copy is provided to the authority, which initiated the revision.

<table>
<thead>
<tr>
<th>Roskomnadzor used this way to receive information about a civil activist Temur Kobaly in December 2015.</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the 23rd of December 2015, V.S. Mikhailov, Deputy Head of the Division of Roskomnadzor in the Volgograd region and the Republic of Kalmykia, as a part of Roskomnadzor new rights, sent an information letter to Krasnooktyabrsky District Court of Volgograd with the following information collected:</td>
</tr>
<tr>
<td>- regarding sign-ins of Timur Kobaly, VKontakte social network user (<a href="http://vk.com/id556535">http://vk.com/id556535</a>) over a certain period of time from certain IP addresses;</td>
</tr>
<tr>
<td>- regarding time and place of Internet connections from identified IP addresses, including physical addresses of Internet access points used for the connections.</td>
</tr>
</tbody>
</table>

In that way, information regarding user's activity in the Internet may be legally provided to FSS of Russia, other law enforcement authorities, conducting OIA, as well as Roskomnadzor. In compliance with the "Yarovaya Package", such information may be provided to FSS of Russia and Roskomnadzor without a previous court authorization for restriction of rights on secrecy of correspondence in Russia.

**Third aspect. Storage of text messages of Internet users, voice information, images, sounds, video and other electronic messages of Internet users**

Only on July 1, 2018 the requirement of the "Yarovaya Package" to store of all text messages, images, sounds, video and other electronic messages of Internet or communication services users by communication providers (including providers) and organizers of distribution of information in the Internet within **6 months at the territory of the Russian Federation** will come into force. This means that content of telephone calls, email or messengers correspondence, Internet calls and their content, SMS texts, transmission or browsing of any information in the Internet becomes available to the Government by default, namely to FSS of Russia

---

34 Part 1 Article 13 of Federal law as of 26.12.2008 №294-FZ (rev. dd. 06.07.2016) "On protection of rights of legal entities and individual entrepreneurs whilst exercising governmental control (supervision) and municipal control".

35 NGO Lawyers Club Archive.

36 Subparagraph 2 Paragraph 1 of Federal law as of 07.07.2003 №126-FZ "On Communication"; Subparagraph 2 Paragraph 3 Article 10.1 of Federal law as of 27.07.2016 №149-FZ (rev. dd. 06.07.2015) "On Information, Information Technologies and Information Protection".
Such information, as set out in the Law, shall be stored exclusively at the territory of the Russian Federation and at the expense of communication providers and organizers of information distribution in the Internet. This regulation overlaps with a rule, enforced on September 1, 2015\textsuperscript{37}, which obliges personal data operators store personal data exclusively at the territory of the Russian Federation and inform Roskomnadzor on the storage addresses (data centres addresses).

After Russian President Vladimir Putin signed the “anti-terrorism” package of amendments proposed by Senator Viktor Ozerov and MP Irina Yarovaya, the combined market value of the “Big Four” Russian mobile carriers dropped by RUB 66 billion (about USD 1 billion).

- MTS market capitalization shrunk by RUB 16 billion in less than 24 hours to RUB 470 billion.
- Shares of Rostelecom dropped almost by 5% on Thursday, and continue to hold the lowest mark since March on Friday. In less than two trading days the company’s capitalization fell by RUB 11 billion to the mark of RUB 225 billion.
- Megafon suffered the maximum loss: Yarovaya amendments overlapped with the closure of the register to receive dividends on shares. In two days the carrier’s shares plummeted by 8.1% to their 4-year low. The market capitalization of Megafon dropped by RUB 35 billion to the level of RUB 403 billion in accordance with the Moscow stock exchange. The lowest loss yet has affected Vimpelcom. Its shares on Nasdaq fell by only 1% during Thursday trading. The company became cheaper by USD 70 million (RUB 4.5 billion), and is worth USD 6.91 billion\textsuperscript{38}.

Implementation of the provision from the “Yarovaya Package” regarding collection and storage of personal information of subscribers of communication services and the Internet will enable the Government to track any person, who will enter the Internet or make a call at least once in his/her life. FSS of Russia will know about this the same day, and from July 1, 2018 it will also know about the content of a conversation or an email, and no one knows how the intelligence service will use this information.

Before the adoption of the "Yarovaya Package" Nikolay Nikiforov, Minister of Communications and Mass Media of the Russian Federation, objected the provision regarding obligatory storage of information during three years:

"We think that this law must not be adopted in its current version. We think that this draft bill shall be amended. We are talking now about storing all the telephone calls and information transmitted during three years, as the draft law currently prescribes. To be honest, we do not quite understand the objective of storing such a huge amount of information. We think that it will result in considerable financial costs for our communication providers, while this law will be virtually impossible to comply with, which will finally result in a collapse of all those companies, that will not be able to comply with its requirements."

\textsuperscript{37} Article 2 of Federal Law as of 21.07.2014 N 242-FZ "On amendments to several legislative acts of the Russian Federation in connection with clarifying the procedure of processing personal data in information and telecommunication networks"

\textsuperscript{38} As of 08.07.2016. Source: http://www.finanz.ru/novosti/aktsii/sotovye-operatory-na-$1-mldr-sutki-posle-zakona-yarovoy-1001294041
However, other ministers and MPs of the Russian Parliament did not listen to Nikiforov.

The “Big Four” Russian mobile carriers opposed this provision on many occasions: MTS, Vimpelcom (Beeline), Megafon and Tele2 informed that implementation of the law would cost them at least RUB 2.2 trillion, while all the market participants will have to invest RUB 5 trillion39 or recosting around USD 35 thousand (around EUR 52040) for each citizen.

It is evident that clients of the communication providers will bear the costs, which will result in increased tariffs for communication services. But this is not the most important. Unlimited access for Government representatives, unknown to public, to almost all the private information is a distinct feature of authoritarian and totalitarian regimes, which have nothing in common with the idea of democracy.

At the end of October 2016 the Ministry of Economic Development and Trade of Russia announced that communication providers’ investments in the infrastructure development may be reduced to zero in 2017-2019 due to the "Yarovaya Package" implementation. This information is contained in the forecast of socio-economic development of Russia for 2017-2019.

It explains that that due to the required capital investments, related to implementation of the anti-terrorist package, accumulated investments in the industry for the development of permanent assets (signal construction, commissioning of means of communication), planned earlier, may be reduced to zero41.

Costs related to the implementation of the "Yarovaya Package", in accordance with the "Big Four", exceed annual income of the companies in several times. To compare, as of 2015 the income of Vimpelcom (Beeline) totaled RUB 278 billion (USD 4.6 billion), of Megafon - RUB 313 billion (USD 5.2 billion), of MTS - RUB 391 billion (USD 6.4 billion), of T2 RTK Holding (Tele2 Brand) - RUB 95 billion (USD 1.6 billion). Total income of the four federal mobile providers totaled USD 17.8 billion.42

"We allow the possibility that due to additional costs, which the providers will bear, prices of mobile communication services for all the clients will increase at least by 2-3 times. Apart from that, these costs will exceed in dozens of times the cost of a large-scale investment programme of construction and expansion of the networks, conducted by Tele2, and will result in delays or freezing up of the infrastructure development", - commented Konstantin Proshkin, Tele2 representative, to Interfax43.

Megafon representatives share the same opinion: "In case of amendments adoption tariffs for mobile communication services will increase by approximately three times", - said Yulia Dorokhina, Head of the Press Office of the company, to RIA Novosti44.

In August 2016, one month after the adoption of the "Yarovaya Package", its possible technical services contractor was announced, the National Center of Informatization of the Rostec State Corporation, which may become a united centre to receive the information from communication providers, to store it and to provide it to FSS of Russia45.

---

40 Euro exchange rate as of 22.10.2016
1 http://www.interfax.ru/russia/524706
42 http://www.vedomosti.ru/technology/articles/2016/04/18/638014-trehletnee-hranenie-zvonkov
43 http://www.interfax.ru/
44 https://ria.ru/
45 http://www.vedomosti.ru/technology/articles/2016/08/22/653913-million-nadezhnie-ruki
This was the initiative of the Ministry of Industry and Trade of the Russian Federation, responsible for creation of a storage system as a part of the implementation of the "Yarovaya Package". In accordance with the idea of Rostec, it may become an operator of the storage services for data to be monitored in compliance with the "Yarovaya Package".

On the 21st of November the Russian Ministry of Industry and Trade organized a meeting, where the Ministry of Communications and Mass Media made clear its point that subscribers’ data may be stored exclusively by communication providers, in accordance with the current legislation, while FSS expressed a concern regarding additional security issues connected to creation of such storage. FSS mentioned that additional guarantees to prevent an authorised access to this information are required. In connection with the above Rostec was requested to prepare a detailed estimation of project risks and costs. At the same time this project is not considered as a priority.

In August 2016 the Russian Ministry of Industry and Trade proposed a second option supported by FSS of Russia: for the purposes of implementation of the "Yarovaya Package" use the existing SORM system, already installed at the communication providers networks and designed to wiretap.

---

48 http://www.interfax.ru/russia/524706
Basing on the possible implementation scheme of the law, which is discussed by the functionaries\(^49\), it will not require any budget investments: equipment will be purchased by providers, while investors will pay for the data storage centres creation.

**Below you will find a possible scheme of the "Yarovaya Package" implementation:**

---

---

**Ways of Yarovaya**

How can the law "On Countering Terrorism" be technically implemented

**Equipment of communication provider**

- **DATA SOURCES**
  - text messages, voice information, images, sounds, video, etc.
- **TAP**
  - provides a copy of information transmitted in passive mode without affecting its quality
- **AGGREGATOR**
  - converts information from various sources, puts information into IP package for its transportation
- **EXTRACTOR**
  - parses information received, deciphers encrypted Internet traffic, encrypts voice information

**Transportation to Data Centre**

**DATA-PROCESSING SOFTWARE**

receives information from transportation network in real time, analyzes and processes data, linking it to a specific subscriber, identifies information, so it could be further selected and provided to competent authorities

**DATA STORAGE SYSTEM**

ensures secure data storage, archive, backup and deletion. It may be built on the basis of data management system technologies or big data technologies. It provides State authorities with access to

---

**SOURCES:** INFORMATION PROVIDED BY ORGANISATIONS AND COMPANIES INVOLVED IN EXECUTION OF ASSIGNMENTS FROM THE RUSSIAN PRESIDENT IN THE AREA OF COUNTERING TERRORISM

---

Source: Vedomosti newspaper № 4143 as of 22.08.2016, article named: "FSS to choose".

---

\(^49\)http://www.vedomosti.ru/technology/articles/2016/08/22/653895-kto-zarabotaet-zakone-yarovoi/#/galleries/140737492892707/normal/1#!/23%2Fboxes%2F140737492892706
Provision regarding storage of information about all telephone conversations and communication sessions will come into force on the 1st of July 2018 only, at the present moment SORM-3 system is in place, which allows to record information about connections and some other information. In connection with the above, "Yarovaya Package" obliged communication providers to store packages of recorded information for 6 months, and not for 12 hours as prescribed by SORM-3 requirements.

Regulations analyzed above, in case of their implementation, will have the most negative effects, including not only unjustified access of the Government to people's private life, but will also allow to monitor content of conversations and correspondence of civil activists and NGO staff legitimately.

Arbitrary application of rights, common for Russia in the recent years, absence of an independent court, unlimited power of the intelligence services suggests that the "Yarovaya Package", as well as many other recent legislative initiatives (including the foreign agents and undesirable organizations laws, etc.), will be applied arbitrarily.

Activities of civil society institutions shall be open, however a total control is unacceptable in a democratic state. NGOs shall provide required information to society themselves. Government may control activities of its citizens, however it shall do it in a restricted number of cases, prescribed by the law, in accordance with a strictly established procedure and with guarantees of a strict and effective social control of the legitimacy of such procedures.

Each regulatory impact shall be reasonable, necessary and justified, as long it is an intrusion in private life of individuals and legal entities, including NGOs.

With "Yarovaya Package" we are coming back to a situation when the Government was monitoring every step of a Soviet citizen and reacted with legal and illegal measures. The Law is based on an assumption that everyone living at the territory of the Russian Federation shall be under suspicion, regardless of the fact whether he or she is an offender or not. In compliance with the "Yarovaya Package" all the Russian citizens are potential offenders, thus, in accordance with the authors of the Law, a total control of the
Government over their conversations and communication sessions in the Internet may contribute to security of the state. Such logic is a hallmark of those states, where democracy does not exist, and the society does not impact or monitor legitimacy of Government actions.

It is evident that law enforcement authorities may use information received about civil activists to prevent them from leaving the country, to prevent organization of public actions or public gatherings, as well as to the civil society from realizing its full potential in relation to current challenges confronting society and Government.

"Yarovaya Package" brings back a political police to Russia: by legalizing an unlimited access for law enforcement authorities to people’s personal information, and the Government will use this information to "clear away" the political arena, suppress civil activity and monitor anyone who it will consider undesirable.

In relation to that, the fight of the Russian Government with mythical "foreign agents" (non-government organizations, which, in the opinion of the Government, receive foreign funding and conduct "political activities") may be just the first step towards suppression of the civil initiative.

The Government will certainly use the access to unlimited surveillance powers after receiving them.

Fourth aspect. Development of legal instruments under "Yarovaya Package".

On the 7th of July 2016 the Russian President approved instructions to the Russian Government in collaboration with FSS to develop drafts of normative instruments to minimize the risks connected with the implementation of "Yarovaya Package" by November 1, 2016. The instructions included the following:

- to specify the stages of the implementation of provisions, which require considerable investments and modernization of technological equipment of business enterprises, falling within the "Yarovaya Package" including a requirement to use national equipment only;
- to specify the rights of the Russian Government, as well as federal executive bodies in relation to the "Yarovaya Package";
- to decide on application of legal provisions regarding liability for using uncertified codification (encryption) resources at communication networks and (or) while transmitting messages to the information and telecommunication network of Internet. Such provision already became effective from July 20, 2016, however the interested authorities will decide on its application by November 1, 2016;
- to decide on the application of "Yarovaya Package" package provision regarding termination of communication services provision in case of failure to receive confirmation regarding consistency of personal data of actual users with information indicated in user agreements.

It is evident that "Yarovaya Package" was adopted prematurely, with no previous consideration of meaningful ways for its implementation, which will be identified in the course of its implementation.

Only on the 18th of November 2016 it became public that the Russian Ministry of Communications started developing draft legal acts to reinforce the implementation of
"Yarovaya Package". Meanwhile, these drafts of regulatory legal acts have not been published yet\(^{50}\).

The drafts are being developed in collaboration with FSS of Russia, and are supposed to be approved by relevant authorities in time to be enforced in June 2017, one year after the adoption of "Yarovaya Package".

**Firstly**, it is planned to approve the decree of the Russian Government, which regulates the procedure for "Yarovaya Package" implementation by organizers of information distribution in the Internet.

Authors of the draft decree are basing on relevant amendments required to legal regulations for collaboration between organizers of information distribution in the Internet and authorized government bodies, conducting operative investigation activity or ensuring state security of the Russian Federation, while the objective of this project is to create a legal framework for collaboration between organizers of information distribution in the Internet and authorized government bodies, conducting operative investigation activity or ensuring state security of the Russian Federation, at the same time fulfilling the requirements to organizers of information distribution in the Internet, established by Federal Law № 374-FZ (which forms part of "Yarovaya Package").

**Secondly**, it is planned to develop a draft of a Russian Government decree regarding Rules of Interaction between organizers of information distribution in the Internet and bodies conducting operative investigation activity, approved by the Russian Government Decree as of 27.08.2005 № 538. It will regulate communication procedures with the state authorities for public communication providers connected with execution of their obligations under "Yarovaya Package"\(^{51}\).

**Thirdly**, it is planned to draft and approve a decree of the Russian Government on procedures for organizers of information distribution in the Internet, connected with performance of their additional obligations, established by the "Yarovaya Package" and related to receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of users of the Internet, as well as information regarding these users.

In accordance with an explanatory note submitted by the authors of the act, "an additional amendment to the legal regulations of collaboration between organizers of information distribution in the Internet and authorized Government bodies, conducting operative investigation activity or ensuring state security of the Russian Federation, is required", namely amendment of Regulations for storage of information, related to receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of users of the information and telecommunication network of Internet, as well as information regarding these users, provision of such information to the authorized state bodies, conducting operative investigation activity or ensuring state security of the Russian Federation, approved by a decree of the Russian Government as of July 31, 2014 № 759.

The objective of this act, in accordance with its authors, is "to create a legal basis for receiving, delivery and (or) processing of voice information, written text, images, sounds, video or other electronic messages of users of the Internet, as well as information regarding these users, and text messages of Internet users, voice information, written

\(^{50}\) As of 27.11.2016.

text, images, sounds, video or other electronic messages of users of the Internet, established by Federal Law № 374-FZ\textsuperscript{52}.

**Fourthly,** in accordance with the legal act of the Ministry of Communications of Russia, it is planned to establish requirements for producers of SORM hardware, for which amendments will be applied to Decree of the Ministry of Communications of Russia as of 16.04.2014 № 83, establishing Rules of Application of switching systems, including software designed to execute established actions in the course of operative investigation activities\textsuperscript{53}.

In accordance with the explanatory note submitted by the authors of the act, in case the project is not approved, "authorized government bodies, conducting operative investigation activity, may be deprived of an opportunity to timely receive all necessary information regarding parameters controlled\textsuperscript{54}.

**Fifthly,** under the Decree of the Ministry of Communications of Russia in relation to producers of OIA technologies amendments will be applied to the Rules of Application of switching systems, including software designed to execute established actions in the course of operative investigation activities\textsuperscript{55} in connection with clarifying the requirements to OIA technologies regarding the following:

- minimum number of control parameters values, selected and transferred to the Operational Post;
- volume of storage for selected information in a nonvolatile memory, designed for load-balancing in a connection channel with the Operational Post;
- ensuring information recording at a recording device;
- other requirements.

Draft project has not been published, however, in accordance with its authors, the objective of the regulations proposed is to ensure integrity, resistance and security of the consolidated telecommunication network of the Russian Federation upon application of OIA technologies at communications networks to ensure conducting of operative investigation activities on a full scale\textsuperscript{56}.

The above mentioned amendments are required under "Yarovaya Package", due to additional obligations of communication providers:

- to terminate provision of communication services to a subscriber in case of inconsistency of actual personal data with information indicated in the user’s agreement, upon a corresponding request from an authorized government body;

\textsuperscript{52} http://regulation.gov.ru/projects\#npa=59198  Project dated 18.11.2016 №02/07/11-16/00059198

\textsuperscript{53} Namely, in Part III. Rules of Application of switching and routing systems of information packages at communication networks, including software designed to execute established actions in the course of operative investigation activities, established by Order of the Russian Ministry of Communications №83 as of 16.04.2014.

\textsuperscript{54} http://regulation.gov.ru/projects\#npa=59193  Project dated 18.11.2016 № 02/08/11-16/00059193

\textsuperscript{55} Namely, in Part II. Rules of Application of equipment of transit, terminal transit and terminal communication nodes of networks of fixed telephone lines, including software designed to execute established actions in the course of operative investigation activities established by Order of the Russian Ministry of Communications №268 as of 19.11.2012.

\textsuperscript{56} http://regulation.gov.ru/projects\#npa=59209  Project dated 18.11.2016 №02/08/11-16/00059209
Right to privacy VS «Yarovaya package» and its impact on civic engagement, November 2016

- to store the information, related to receiving, delivery and processing of voice information, written text, images, sounds, video or other messages of communication services subscribers, as well as text messages, voice information, written text, images, sounds, video or other messages;
- to provide authorized government bodies, conducting operative investigation activity or ensuring state security of the Russian Federation with the above mentioned information, information regarding subscribers of communication services and services provided, as well as other information, necessary for implementation of their tasks in cases specified by federal laws.

Table 2. Comparison of responsibilities of communication providers and organizers of information distribution in the Internet:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Communication provider (fixed-line and mobile telephone services, Internet)</th>
<th>Organizer of information distribution in the Internet (portals, forums, email web portals, messengers and others).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Storage Period</td>
<td>3 years</td>
<td>1 year</td>
</tr>
<tr>
<td>Storage Period of communications</td>
<td>Up to 6 months</td>
<td>Up to 6 months</td>
</tr>
<tr>
<td>content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liability for breach</td>
<td>Licence revocation</td>
<td>Penalty</td>
</tr>
<tr>
<td>SORM Application before &quot;Yarovaya</td>
<td>Yes, long before &quot;Yarovaya Package&quot;</td>
<td>From August 2014</td>
</tr>
<tr>
<td>Package&quot; enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SORM Application after &quot;Yarovaya</td>
<td>Yes</td>
<td>Yes, if the organizer is included in Roskomnadzor list</td>
</tr>
<tr>
<td>Package&quot; enforcement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fifth aspect. Obligation of organizers of information distribution in the Internet to decipher users’ messages

In the course of SORM implementation, Russian authorities realized that web browsing history is not available in case encryption technologies were used, while content of messages and voice calls is neither available in case developers of such messengers use encryption.

On January 29, 2016 it was announced that even before "Yarovaya Package" adoption the President of Russia signed a list of instructions on the results of the meeting with participants of the First Russian Internet Economy Forum⁵⁷, including an instruction to FSS of Russia and the Ministry of Communications in collaboration with the relevant federal government executive bodies to provide proposals for amendments to requirements for encryption of information, transmitted by communication networks in

⁵⁷ http://kremlin.ru/acts/assignments/orders/51235
the Russian Federation, with a liability assigned for failure to comply with such requirements, by June 01, 2016.

It seems that such regulation regarding encryption of messages transmitted in the Internet appeared in the "Yarovaya Package" pursuant to execution of this instruction.

While receiving information from communication operators (including providers) as a part of SORM maintenance, FSS of Russia and bodies, conducting OIA, did not have a technical capacity to follow technological developments of companies, providing new modern software for the market. Consequently, the Government came to a simple solution of this issue and obliged developers and messengers’ operators to provide FSS of Russia with encryption codes for electronic messages and voice calls.

Such requirement is intended to place private correspondence outside of any protection. In accordance with the authors of the law, protected communications in Telegram or other messengers, will be rendered meaningless: the Government, upon receiving the keys, will be able to read any correspondence of anyone and further use such information on its own discretion, including for the purposes of secret activities of its bodies.

In accordance with the "Yarovaya Package" an organizer of information distribution in the Internet upon receiving, delivery and (or) processing of electronic messages of users of the Internet using additional messages encryption and (or) upon providing to users of Internet an opportunity of additional messages encryption shall provide a federal executive body responsible for IT security with information necessary for decryption of received, delivered and (or) processed electronic messages58.

The Law is applicable to such popular messengers, as ICQ, Viber, WhatsApp, Telegram and other messengers, applying various encryption schemes for information transmitted (including end-to-end encryption, when only a sender and a recipient are able to read a message or listen to a voice call, while the operator is not able to do that).

Apart from that, a popular Internet-protocol HTTPS, providing a safe data transmission in the Internet, also fell within the scope of the "Yarovaya Package".

VPN systems are one of the targets of the "Yarovaya Package".

On July 07, 2016 the President of the Russian Federation instructed the Government in collaboration with FSS address the issue of development and maintenance of a list of organizers of information distribution in the Internet, which are obliged to provide federal executive bodies with information necessary for decryption of received, delivered and (or) processed electronic messages in case of additional encryption upon a corresponding request. Due date - by November 0159. Such list has not been created yet.

Neither the project, not the legal act have been published, and it is early to claim that the order of the Russian President has been executed.

However, on the 12th of August 2016 the Federal Security Service of Russia published a decree60 establishing a procedure for provision by the organizers of information distribution in the Internet of decryption codes of such messengers.

58 Paragraph 4.1 Article 10.1 of Federal law as of 27.07.2016 №149-FZ (rev. dd. 06.07.2015) "On Information, Information Technologies and Information Protection".
59 http://kremlin.ru/events/president/news/52486
60 Decree of FSS of Russia as of 19.07.2016 № 432 "On establishment of the procedure for provision by organizers of information distribution in the information and telecommunication network of Internet of information necessary for decryption of received, delivered and (or) processed electronic messages of users of the information and telecommunication network of Internet to the Federal Security Service of the Russian Federation".
The order is aimed to facilitate the provision of keys to FSS of Russia for further decryption of HTTPS traffic and other encrypted users’ data if needed. This regulation comes into force now, one year and a half before the enforcement of a regulation regarding the obligation to store all the traffic for the period of up to six months.61

This regulation establishes a procedure for provision of encryption keys by servers’ owners and other Internet services. The procedure is quite logical and simple:

- an organizer of information distribution in the Internet provides decoding information upon request of an authorized department, signed by a director (deputy director);
- such request shall be sent by a registered letter with the activated option of the receiving acknowledgement;
- the request shall include the format and the address for provision of the decoding information;
- the information shall be transmitted on by mail a hard copy or by email. As an option, access of specialists to the decoding information can be provided upon FSS approval.

The Organizational and Analytical Department of Technical and Information Service of the Federal Security Service of the Russian Federation was appointed as an authorized department for the collection of keys.

For information, hard copies include magnetic disks, magnetic cards, magnetic tapes and magnetic drums.

In case a server owner refuses to provide a key, required for decoding HTTPS or other encrypted traffic, it can be charged with a penalty in the amount of one million rubles.

Before the publication of the specific procedure of keys submission, representatives of several Internet companies expressed doubts about enforceability of the law as regards submission of decryption keys. They say that in case of HTTPS protocol keys can not be stored due to technical requirements.62

**Is it possible to decipher Internet traffic?**

Data encryption mechanism in the Internet is used by many banks, sale and hotel booking web sites. Now they are obliged to submit to the Government decryption keys, transmitted by their systems to the Internet.

Software developers reacted negatively to the new regulations. For instance, Pavel Durov, Telegram developer, claimed that Telegram does not provide third parties, including governments, with data or encryption keys. Laws, adopted by countries, will not affect this policy.

In reality, there is no way to find out whether messenger services have provided FSS of Russia with their encryption keys. Privacy can be ensured only if an encryption algorithm does not allow access for messenger operators to encryption key for users messages.

The Russian Association for Electronic Communications (RAEC), which is the main lobbyist of the Internet business in Russia, has alerted that this law jeopardizes secrecy of communication and bears a risk for confidential information leaks.

The Association claims that the major part of encryption standards does not allow storage of users' keys, which means that messages cannot be deciphered without changing the existing algorithm. At the same time, such changes pose a real threat to the cyber security\(^63\).

The storage of traffic without its deciphering is useless. Experts claim that the current deciphering scheme discussed by the government officials will allow in the future not only to prevent potential threats, but also to develop behaviour profiles of Internet users, including their psychological state and taste preference\(^64\).

There are two main encryption procedures of the information in the Internet: end-to-end technology applied by almost all the messengers, and SSL-certificates\(^65\).

On the one hand, with the "Yarovaya Package" the Government obliged developers and messengers' operators to provide FSS with decryption codes.

On the other hand, the Government started to search for a company which is able to find an encryption key for messages sent using messenger services. A Russian company "Con Certeza"\(^66\) will facilitate it, as long as it has been engaged in the development of hardware for communication providers, required for SORM implementation, for a long time. For instance, the company already offers the following SORM systems to communication providers.

<table>
<thead>
<tr>
<th>Name IS SORM</th>
<th>Fixed-line connection</th>
<th>Mobile connection</th>
<th>Broadband</th>
<th>Mobile Internet (GPRS, 3G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yantar</td>
<td>Information on telephone connection ownership and use (detailed report)</td>
<td>Information on mobile radio connection ownership and use (detailed report)</td>
<td>Information on data transmission ownership and use</td>
<td>Information on telematics service ownership and use</td>
</tr>
<tr>
<td>Yashma</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yantar-PD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^63\) [https://www.gazeta.ru/tech/2016/06/24/8325293/svyazj.shtml]
\(^64\) [http://kommersant.ru/doc/3094848]
\(^65\) [http://kommersant.ru/doc/3094848]
\(^66\) [http://www.concerteza.ru/]

"Modern applications for encrypted communication store encryption keys with participants of conversations, and not with a service provider. This means that the implementation of this provision is technically impossible", - told the Gazeta newspaper Vladimir Gabrielyan, Vice President and Technical Director of Mail.Ru Group.

Artyom Baranov, leading virus analyst of ESET, supports this point of view. He explained to Gazeta newspaper that several messengers (for example, Viber and WhatsApp) have recently implemented end-to-end encryption, which means that only a user has access to his/her messages transmitted, while messengers' providers do not store private keys. Telegram uses such technology in its secret chats.
In accordance with kartoteka.ru, 76% of shares of OJSC "Con Certeza" belong to Mikhail Lemeshev, and 24% of shares belong to OJSC "NLP Group", also owned by Mikhail Lemeshev and OJSC "Con Certeza". At "NLP Group" website several projects developed in collaboration with MTS are mentioned, while two interlocutors of Kommersant specialized at telecommunication, claim that the Group was founded by former MTS employees and mainly provides services to this mobile operator. Head of OJSC "Con Certeza" Andrey Lemshev was mentioned twice in MTS procurement documents as MTS employee. MTS declined to comment on that.67

The company is ready to review the main messengers - WhatsApp, Viber, Facebook Messenger, Telegram, Skype for iOS and Android, and prepare an expert opinion on the possibility to intercept the sensitive data, i.e. users’ communication identifiers, passwords, messages when dealing with a traffic copy, and demonstrate a prototype, if possible. The company is ready to conduct these works within 2 months and to start with Viber. Total cost of works for each messenger may be estimated at up to RUB 360 thousand.68 Hacking of encryption systems is the first way for the Government to get decryption keys for protected channels of information transmission in the Internet.

In accordance with the media sources, it is theoretically possible to intercept encrypted traffic, including of those messengers, which are using end-to-end encryption. Messengers exchange public parts of cryptographic keys before the beginning of correspondence, which can be replaced, thus messages can be deciphered. There are technologies, developed for protection from these types of attacks, - Key Pinning, attachment of specific certificates to a specific web site or application.69

The second way for the Government to get access to users encrypted information is installation of hardware at operators’ networks, designed for MITM attacks (Man in the Middle). This is one of the decryption options discussed by IT specialists. This equipment pretends to be the web page requested for a user, and a user - for the web page. In this

"Basing on its description, Con Certeza investigation will be focused on the possibility to get information about a communication of identifiable users taking place, their correspondence, and in case of a successful implementation of MITM, substitution of its content", - notes Alexander Lyamin, CEO of Qrator Labs.

For the purpose of implementation of "Yarovaya Law" provisions, FSS and the Ministry of Trade are discussing a set of technical solutions to access all the Internet traffic of Russian citizens, including traffic interception and deciphering using MITM attacks (when this equipment pretends to be a web page requested for a user, and a user - for a web page).

However, earlier at committee stage of the Law, Kommersant interlocutors expressed doubts regarding application of this technology for the messengers, using end-to-end encryption.68

---

67 http://www.kommersant.ru/doc/3106585
68 http://www.kommersant.ru/doc/3106585
69 http://www.kommersant.ru/doc/3106585
manner, a user will establish SSL connection with this equipment, and this equipment will later establish connection with a server initially requested by the user. The equipment will decipher the traffic intercepted, and before sending it to the user will encrypt it once again with a SSL certificate, issued by the Russian certification centre (CC). In order to avoid notifications about a non-secure connection at the user’s browser, the Russian CC shall be included in the Trusted Root Certification Authorities at the user's computer 70.

The Russian Government is deciding how the Internet traffic will be deciphered. FSS of Russia opts for its decryption in real time and its analysis in accordance with key parameters. Other departments at the same time insist on decryption of traffic only of those users, who has drawn attention of law enforcement authorities 72.

The third way to ensure messengers monitoring is the implementation of the "Yarovaya Package" provision regarding administrative liability for usage of uncertified codification (encryption) resources while transmitting messages to the information and telecommunication network of Internet, if the law prescribes its obligatory certification 73. Such liability shall be imposed in the form of a fine in the amount from RUB 3 000 to 5 000 for individuals, from RUB 15 000 to 30 000 for officials, from RUB 60 000 to 300 000 for legal entities.

On July 07, 2016, after signing the "Yarovaya Package", the President of the Russian Federation instructed FSS of Russia to approve a procedure for certification of codification (encryption) resources while transmitting messages to the information and telecommunication network of Internet, by creating a list of resources to be certified, as well as procedure of submission of keys to a federal executive body responsible for IT security of the Russian Federation 74.

The second task FSS executed by issuing a correspondent order on the 19th of July 2016 75, while in relation to the messengers FSS decided not to certify such encryption resources.

On July 20, 2016, FSS announced it, noting that "a procedure for obligatory certification of codification (encryption) resources, while transmitting messages to the information and telecommunication network of Internet, massively applied for protection of information, which do not constitute State secrets, including in user devices and mobile-communication base stations, computers, equipment of the information and telecommunication network of Internet for their alignment with security requirements is not required" 76.

70 http://kommersant.ru/doc/3094848
71 http://kommersant.ru/doc/3094848
74 http://kremlin.ru/events/president/news/52486
75 Decree of FSS of Russia as of 19.07.2016 № 432 "On establishment of the procedure for provision by organizers of information distribution in the information and telecommunication network of Internet of information necessary for decryption of received, delivered and (or) processed electronic messages of users of the information and telecommunication network of Internet to the Federal Security Service of the Russian Federation".
76 http://www.interfax.ru/russia/519643
The forth, indirect way to exert pressure on messengers and to make them give up from using data encryption, was the idea offered by the Media Communication Union, comprising MTS, Beeline and an organization affiliated with Megafon.

In August 2016 they offered to oblige messengers to identify their users, but not with their databases, but with mobile communication providers data. A relevant agreement shall be concluded between a messenger and a user in this case.

In accordance with the offers of this draft bill, messengers shall prevent the exchange of illegal information, which means that they shall have access to the content of users’ correspondence. As a disciplinary measure against messengers’ refusal to control distribution of illegal information, communication providers (Beeline, MTS, Megafon and others) may restrict access to such messengers upon Roskomnadzor decision.

However, the draft bill has not been officially developed yet, neither included in the Russian Parliament.

There is no information so far regarding cases when provisions of the "Yarovaya Package" were imposed on anyone. The question regarding decryption of messengers’ traffic is still open. It is also unclear in which manner the Government will implement "Yarovaya Package" towards them. In order to escape the "Yarovaya Package" implementation, some companies leave the Russian market. Other companies disregard this Law, stating that a company is not registered in Russia. It is possible that communication providers and organizers of information distribution in the Internet will implement this Law voluntarily, or maybe some of the companies decided to disregard its requirements as long as it is possible.

77 http://www.np-mks.com/founders/

International standards.
In accordance with Article 19 of the Universal Declaration of Human Rights, everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.\(^79\)

The International Covenant on Economic, Social and Cultural Rights in Article 19\(^80\) also confirmed this right.

On July 05, 2012, the Human Rights Council of the United Nations for the first time considered realization of rights and freedoms in the Internet and adopted a historic resolution "The Promotion, Protection and Enjoyment of Human Rights on the Internet"\(^81\), where it explained that the right to freedom of opinion and expression in the Internet derives from the right to freedom of opinion and expression. It affirmed that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

It can be assumed then that a right to privacy of communication shall be protected in the Internet in the same way as it is protected offline.

On the 16th of May, 2011 the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, submitted to the UN Human Rights Council a report, where the Rapporteur expressed concerns regarding "actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner. For example, States have used popular social networking sites, such as Facebook, to identify and to track the activities of human rights defenders and opposition members, and in some cases, have collected usernames and passwords to access private communications of Facebook users".

The Special Rapporteur informed that "a number of States are also introducing laws or modifying existing laws to increase their power to monitor Internet users’ activities and content of communication without providing sufficient guarantees against abuse... Furthermore, steps are also being taken in many countries to reduce the ability of Internet users to protect themselves from arbitrary surveillance, such as limiting the use of encryption technologies".

The Special Rapporteur also noted that "there are insufficient or inadequate data protection laws in many States stipulating who is allowed to access personal data, what it can be used for, how it should be stored, and for how long. The necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of personal data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over..."

---

\(^81\) A/HRC/RES/20/8
information of their users. Moreover, with the increasing use of cloud-computing services, where information is stored on servers distributed in different geographical locations, ensuring that third parties also adhere to strict data protection guarantees is paramount.

The Special Rapporteur noted that "the protection of personal data represents a special form of respect for the right to privacy... States parties are required to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties. In addition to prohibiting data processing for purposes that are incompatible with the Covenant, data protection laws must establish rights to information, correction and, if need be, deletion of data and provide effective supervisory measures. Moreover, as stated in the Human Rights Committee’s general comment on the right to privacy, “in order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.”

The Special Rapporteur notes that the right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals’ right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.

The European Union (hereinafter referred to as "EU"), to which Russia is not a State party, on the 3rd of July 2014 published the Human Rights Guidelines on Freedom of Expression Online and Offline, where it explained that "freedom of opinion and expression are indispensable for individual dignity and fulfilment, they also constitute essential foundations for democracy, rule of law, peace, stability, sustainable inclusive development and participation in public affairs".

EU is basing on the following: "States also have an obligation to protect the right to privacy: no one should be subject to arbitrary or unlawful interference with their privacy. States must ensure that their legal systems provide adequate and effective guarantees of the right to privacy, which are applicable to all under their jurisdiction and can be properly enforced".

The EU specifically indicates that "the obligations of States under international human rights law.. the right to privacy and the protection of personal data, extend to the online sphere in the same way as they apply offline. The right to freedom of expression, the right to privacy and the protection of personal data may suffer violations as a result of unlawful or arbitrary surveillance, interception of communications or collection of personal data, in particular when carried out on a..."
mass scale. States must ensure that any measures taken to protect certain information gathered and processed in the interest of national or public security are in accordance with their obligations under international human rights law.

The EU "will promote and facilitate the exchange of good practices to ensure that the legislation and procedures of States regarding the surveillance of communications and the interception and collection of personal data are based on the rule of law, subject to independent, effective and domestic oversight mechanisms and uphold obligations under international human rights law, including the principles of proportionality and necessity".

The Council of Europe, to which Russia is a State party, insist that the governments-members of the Council of Europe shall comply with the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms, including the right to respect for private and family life, guaranteed by Article 8 of the Convention.

In accordance with this article, everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Court of Human Rights (hereinafter referred to as ECtHR), ruling on applications alleging violations committed by the governments which have ratified the Convention, considered the case "Roman Zakharov v. Russia" (Application no. 47143/06).83

On the 4th of December 2015, the Grand Chamber of the ECtHR issued the first judgement, containing a comprehensive review of SORM-2 application practice, while such practice without providing due guarantees do not comply with the provision of Article 8 of the Convention.

Although the applicant was not able to prove that his mobile telephone communications were intercepted, ECtHR considered that the request was sufficiently reasoned. Having regard to the secret nature of the surveillance measures provided for by the contested legislation, the broad scope of their application, affecting all users of mobile telephone communications, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, the Court considered an examination of the relevant legislation in abstracto to be justified. The Court therefore found that the applicant did not have to prove that his telephone calls had been intercepted, neither he had to prove the risk of being subjected to interception measures, because the Russian legislation does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, while the mere existence of the contested legislation amounts in itself to an interference with the exercise of applicant’s rights under Article 8 of the Convention.

Article 23 § 2 of the Russian Constitution guarantees for everyone the right to respect for privacy of correspondence, telephone, postal, telegraph and other communications. That right may be restricted only on the basis of a court order.

83 http://hudoc.echr.coe.int/eng?i=001-159324#sitemid:[e001-159324=]
The circumstances of the case

Roman Zakharov, the applicant, the editor-in-chief of a "Liniya Poleta" aviation magazine and the chairperson of the St Petersburg branch of the Glasnost Defence Foundation, claimed that in accordance with the Russian legislation, the mobile network operators had installed technical facilities using telecommunications networks enabling operational-search activities to be carried out (so called SORM-2). While the Russian legislation do not provide for sufficient guarantees, such facilities allow arbitrary surveillance of mobile telephone communications.

Trial procedures in the Russian courts

In December 2003 the applicant brought judicial proceeding against three mobile network operators, claiming that there had been an interference with his right to the privacy. He also asked to invite the Ministry of Communications and Information Technologies and the St Petersburg and Leningrad Region Department of the FSS as a third party to the proceedings. He asked the court to issue an injunction ordering the removal of the SORM-2 equipment installed, because it allows law enforcement authorities to intercept all telephone communications without prior judicial authorisation.

In December 2005 the Vasileostrovskiy District Court of St Petersburg dismissed the applicant’s claims, because the applicant had failed to demonstrate any facts which would warrant a finding that his right to the privacy of communications had been violated. The Court also found that the equipment to which he referred had been installed to enable law-enforcement agencies to conduct operational-search activities in accordance with the procedure prescribed by law, and the installation of such equipment had not in itself interfered with the privacy of the applicant’s communications.

In April 2006 the Judicial Board of Civil Cases the St Petersburg City Court upheld the applicant’s judgment on appeal. Having exhausted domestic remedies, on the 20th of October 2006 Roman Zakharov lodged an application to ECtHR, regarding alleged violation of Article 8 of the Convention (Right to respect for private and family life) and Article 13 of the Convention (Right to an effective remedy), basing the latest on the fact that no remedies were available under Russian law to challenge that legislation.

Trial procedures in ECtHR

On the 20th of October 2006 the application was lodged. On the 11th of March the Chamber, to which the case had been allocated, relinquished jurisdiction in favour of the Grand Chamber under Article 30 of the Convention, in accordance with which if a case pending before a Chamber raises a serious question affecting the interpretation of the Convention or the Protocols thereto, or where the resolution of a question before the Chamber might have a result inconsistent with a judgement previously delivered by the Court, the Chamber may, at any time before it has rendered its judgement, relinquish jurisdiction in favour of the Grand Chamber, unless one of the parties to the case objects.

On the 24th of September 2014, a hearing the Grand Chamber took place, and on the 4th of December 2015 a judgement was adopted in the case.
Position of ECtHR

Convention requirements: interceptions of mobile telephone communications pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country. However, there is a risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it. This is why legislation shall provide adequate and effective guarantees against abuse, to allow the application of secret surveillance measures only when it is justified by the above-mentioned purposes.

Compliance of the Russian legislation with the Convention requirements

The Russian law provides guarantees against abuse, however they are not sufficient. Although the possibility of improper action can never be completely ruled out whatever the system of secret surveillance is, a system, such as the Russian one, which enables the secret services and the police to intercept all the mobile telephone communications, is particularly prone to abuse.

In particular, the Court concluded that Russian legal provisions do not provide for adequate and effective legal guarantees in the following areas:

- the circumstances in which public authorities are empowered to resort to secret operative investigation activities (for example, interception of telephone calls), are not defined with sufficient clarity, neither the provisions on discontinuation of secret surveillance measures and circumstances, when the intercept material shall be destroyed;
- the authorisation procedures for interception of telephone calls are not capable of ensuring that secret surveillance measures are ordered only when it is justified and necessary;
- the supervision of legitimacy of secret operative investigation activities conducted is ineffective;
- no effective remedies in place.

The Court noted that the effectiveness of the existing remedies in Russia is undermined by their availability only to persons who can prove the interception of their communications. In the absence of notification regarding interception of telephone calls or some form of access to official documents relating to the interceptions such a burden of proof is virtually impossible to satisfy.

ECtHR provided detailed grounding in its judgement, identifying the defects of the Russian legislation in the area of supervision of mobile telephone communications interception. They include:

1. Circumstances when the law enforcement authorities are enabled to intercept telephone and other conversations.

Russian law does not clearly specify the categories of persons whose telephone and other conversations might be subjected to interception measures. In particular, in accordance with the legislation a court may grant authorisation to intercept the communications not only of a suspect or an accused, but also of "other persons if there are reasons to believe that information relevant to the criminal case may be discussed" (Article 186 of the Code of Criminal Procedure), and “a person who may have information
relevant to the criminal case”, or “of events or activities endangering Russia’s national, military, economic or ecological security” (Article 8 of the Law on Operative Investigation Activity).

The Russian legislation does not give any indication, how such broad terms shall be understood in law-enforcement practice, which leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance.

2. Discontinuation of telephone calls interception.

Russian law does not clearly identify situations when telephone calls interception shall be discontinued. Requirement of an immediate termination of interception, when it is no longer required, is contained only in the Code of Criminal Procedure (Article 186), but not in the Law on Operative Investigation Activity. As a result, telephone calls interception under the Law on Operative Investigation Activity (in particular, in connection with obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation) is conducted without providing sufficient guarantees against abuse.

3. Destruction of materials collected.

In accordance with the Russian legislation, materials collected as a result of intercepting telephone communications must be stored for six months.

There is no requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained.

The Russian law is not sufficiently clear on the circumstances in which the intercept material, used in evidence in the trial, may be stored after the end of the trial or shall be destroyed.

4. Authorisation procedure for telephone calls interception.

This procedure, specified by the Russian legislation, does not provide sufficient guarantees, that interception will be authorised, only when it is necessary and justified.

In particular, regardless of the Constitutional Court guidelines (see Decisions № 86-O as of 14 July 1998, № 345-O as of 2 October 2003 and № 1-O as of 8 February 2007), the Russian courts do not examine whether there are grounds for suspecting the person in respect of whom operational-search measures were requested of a criminal offence or of activities endangering national, military, economic or ecological security of the Russian Federation. Russian courts neither estimate whether interception measures are necessary and justified. In particular, requests for operational-search measures often lack materials, providing grounds for application of interception measures, while the judges do not request to provide them. Usually, to receive a court authorisation for interception the law enforcement authorities need to refer to information obtained about events or activities endangering the national, military, economic or ecological security of the Russian Federation.

Therefore, Russian courts do not verify the existence of a reasonable suspicion against the person concerned and proportionality of intrusion in right for privacy of telephone communications.

Moreover, the Law on Operative Investigation Activity does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant interception authorisations of all mobile telephone communications in the area where a
criminal offence has been committed, without mentioning a specific person or telephone number, neither the duration of the interception measure. In accordance with the Law on Operative Investigation Activity in cases of urgency it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. This procedure is not capable of ensuring that it will be used only in cases when it is truly justified.

Finally, the Court concluded that the technical facilities enabling operational-search activities to be carried out at telecommunications networks (SORM-2) gives the security services and the police technical means to circumvent the legal authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action regarding secret surveillance can never be completely ruled out whatever the system, a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.

5. Supervision of the implementation of secret surveillance measures

Supervision of the implementation of secret surveillance measures does not comply with the requirements of the European Convention, in accordance with which a supervisory body shall be independent, vested with sufficient powers and competence to exercise an effective control and open to public scrutiny.

Firstly, the prohibition on logging or recording data of a subscriber supervised and any other data related to interceptions of mobile telephone communications makes it impossible to discover interceptions carried out without proper judicial authorisation.

Secondly, the supervision is carried out by the Prosecutor General and prosecutors appointed by the Prosecutor General. The procedure of prosecutors’ appointment raised doubts as to their independence from the executive authorities. Apart from that, as a part of their prosecuting functions, prosecutors give their approval to all requests regarding interception of telephone or other communications. This blending of functions within one prosecutor’s office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors’ independence.

Thirdly, the scope of prosecutors’ supervision of interceptions is limited: for example, the information about the security services’ tactics, methods and means is outside the scope of prosecutors’ supervision. Apart from that, there is no specific provision in the Russian legislation requiring destruction of the intercept material, recognized by prosecutors as unlawfully obtained.

Fourthly, the results of prosecutors’ supervision are not published or otherwise accessible to the public. Lastly, the Russian Government did not submit any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach of law. It follows that the Government did not demonstrate that prosecutors’ supervision of secret surveillance measures is effective in practice.
6. Notification of interception of communications and available remedies.

The Court examined the effectiveness of the following remedies: an appeal, a cassation appeal or a supervisory-review complaint against the judicial decision authorising interception of communications; a judicial review complaint under Article 125 of the Criminal Procedure Code; a judicial review complaint under the Judicial Review Act (Acts and Decisions Violating Civil Rights and Liberties) as of April 27, 1993 (№ 4866-1) and Chapter 25 of the Code of Civil Procedure as of March 08, 2015 (№ 21-FZ); a civil tort claim under Article 1069 of the Civil Code; and a criminal complaint under Articles 137, 138, 285 and 286 of the Criminal Code.

The Court concluded that the effectiveness of these remedies is undermined by their availability only to persons who can prove the interception of their communications. In the absence of notification or some form of access to official documents relating to the interceptions such a burden of proof is virtually impossible to satisfy.

In view of the above considerations, Russian law does not provide for effective remedies to a person who suspects that his telephone or other conversations have been subjected to secret surveillance, which constitute one of the most important safeguards against the improper use of secret surveillance measures. It is important to note, that the Court did not decide whether these remedies will be effective in cases where an individual learns about the interception of his or her communications in the course of criminal proceedings against him or her, when these materials were used as an evidence.

ECTHR conclusion:

1. The Russian legislation does not provide for adequate and effective guarantees against arbitrariness and the risk of abuse in the course of telephone or other communications interception.

2. Russian law does not meet the “quality of law” requirement and is incapable of keeping the “interference” to what is “necessary in a democratic society”.

The Court has accordingly found a violation of Article 8 of the Convention, and decided that there was no need to examine the complaint under Article 13 of the Convention.

Dmitry Dedov, ECHR judge from Russia, relinquished jurisdiction in favour of the Grand Chamber, but expressed a separate opinion.

In such a manner, a short review of international human rights standards demonstrates that neither SORM, no "Yarovaya Package", adopted in continuation and establishing a total control over all the users of the Russian Internet, do not comply with international standards and constructive obligations, accepted by the Russian Federation.
Of note was the fact that, notwithstanding of ECtHR judgement as of December 2015 regarding non-compliance of the Russian SORM-2 system with the Convention requirements, the Russian Government, as in response to this judgement, in July 2016 adopted "Yarovaya Package", the requirements of which contradict with ECtHR conclusions in case of Roman Zakharov v. Russia, which represented a original response to the requirement of compliance with ECtHR conclusions in Russia.

Implementation of "Yarovaya Package" is a violation of the human right to respect for private and family life, so privacy disappeared a while ago, while an unaltering watch of the "Big Brother" is following everyone, collects information and in the absence of effective control measures uses it in a way that people will never know what kind of information about them the Government has collected, to whom it was conveyed and how it was used.

Total control over the citizens is not compliant with the fundamentals of a legal and democratic state, which, as it shall be recognized, is enshrined in the Constitution.

Implementation practice of "Yarovaya Package" not only provides for unlimited opportunities to control private life of its citizens, but will also result in the establishment of a closed society, and may further result in suspicion of everyone in commitment of crimes and in devaluation of the principle of the presumption of innocence in the course of trials.
Part 4. Other provisions of the "Yarovaya Package". Fast facts

"Yarovaya Package" provided for other innovations in the Russian legal framework, which could not have appeared in a legal state.

4.1. Failure to report a crime is a new crime


Failure to inform law enforcement authorities about person(s) conspiring to commit, or committing, or having committed one of the sixteen criminal offences, stipulated by the Criminal Code of the Russian Federation is considered a crime. One of these 16 crimes is an attempt on the life of a State or public figure, the forcible seizure of power or forcible retention of power.

Legal liability in this cases arises from the minimum age of criminal responsibility (14 years old), while for a crime itself from 16 years old.

Such failure to inform is punishable by a penalty from RUB 100,000 or other income of a convicted offender for the period of up to six months, or by compulsory work for not more than one year, or imprisonment for up to one year.

On the one hand, the Government transferred its responsibility to combat the crime to the citizens. The question which arises here is whether the Government is able to independently execute one of its main functions, the fight against crime.

On the other hand, introduction of such legal component of a crime is a logical development of the fight with foreign agents, spy mania, defeat of the civil society and similar state policy.

The law prescribes to the citizens to be vigilant, to virtually do whistleblowing. The adoption of the law itself has connotations of the 1930s, when the Government exacted reprisals against its own citizens, and many people were sentenced for the failure to report a crime. In those times the Government succeeded in creation of a climate of fear, while people lost a desire to enjoy their civil rights, and were converted into mere components of the Government system.

At the time of writing, there had been no convictions under this article.

4.2. Opportunity to create collegiate state bodies to prevent terrorism, while their requirements are obligatory for everyone

"Yarovaya Package" prescribes that "Government bodies can be formed" by representatives of other Government bodies, local Government bodies "and other persons" for the purposes of terrorism prevention, as well as for minimizing and addressing its consequences. They are formed under a decision of the President of the Russian Federation.
The Law does not prescribe neither the functions of the authority, nor the procedure for its operation, it does not incorporate it in the executive structure of the Government, and thus the legal status of such body shall be arbitrarily defined by the Russian President.

In addition to the above, the law obliges all citizens, organizations and state authorities execute instructions of this body. In case of failure to execute instructions of this body, citizens, organizations and state authorities shall be held liable.

At the time of writing, the law did not prescribe any specific liability for failure to execute instructions of the above-mentioned body, however such liability may be prescribed in the future. Formation of such body, which decisions are binding on everyone, substitutes the decisions of the existing state bodies, empowered to counter terrorism and executing these functions.

Obviously, such a provision of "Yarovaya Package" was adopted to change the idea of “anti-terrorist operations”. In the past such measures were undertaken in case "it was impossible to prevent an attack by other measures"\(^{84}\). That is to say that the law provided for special cases when a counter-terrorism operation was conducted as a last resort. Such criterion does not exist anymore. A decision of responsible authorities is enough to launch an operation. Such operation is conducted to "intercept terrorist acts and related criminal activities"\(^{85}\). It is obvious that FSS of Russia or the Anti-Terrorist Committee will have an opportunity to assume the leading role in such a body and conduct their activities regardless of the human rights.

4.3. Strengthening of criminal responsibility for juveniles

Article 92 of the Criminal Code of the Russian Federation prescribes possibility of release to be imposed for juvenile offenders sentenced to imprisonment for serious and/or particularly serious offences by placing them in a closed-type special education institution.

"Yarovaya Package" increased the number of legal components, which do not allow implementation of such measure of educational influence, from 19 to 28.

4.4. Strengthening of criminal responsibility for persons who have attained the age of 14 years old.

"Yarovaya Package" increased the number of legal components of a crime, which include criminal responsibility for persons who have attained the age of 14 years old, from 23 to 33.

4.5. Strengthening of criminal responsibility for organisation of illegal migration\(^{86}\).

The Law considerably strengthens responsibility for organisation of illegal migration prescribing a punishment, which is exclusively a penalty of up to five years’ imprisonment, without an option of a fine or compulsory, corrective or forced labour (as prescribed before).

\(^{84}\) Paragraph 1 Article 12 of Federal Law as of 06.03.2006 №35-FZ (rev. dd. 03.07.2016) "On Countering Terrorism".
\(^{85}\) Paragraph 1 Article 12 of Federal Law as of 06.03.2006 №35-FZ (rev. dd. 06.07.2016) "On Countering Terrorism".
\(^{86}\) Article 322.1 of the Criminal Code of the Russian Federation.
4.6. Amendment of the time limit for filing charges

The Law prescribes extension of the time limit for filing charges (up to 45 days) against a person, suspected of committing a crime under one of the fifteen articles of the Criminal Code of the Russian Federation, and with respect to which a repression measure has been taken (for example, imprisonment). In case the suspect has not been indicted, the detention should be immediately terminated.

The current time limit is 30 days.

4.7. Mitigation of judicial control guarantees over actions of pretrial investigators in the course of investigation of criminal cases

The Law enables persons conducting the initial inquiry or investigators to conduct searches of persons or homes and seizures without a judicial decision in case of urgent situations which admit no delay.

Currently there is a requirement, that persons conducting initial inquiry or investigators shall inform the public procurator and the judge of such action within 24 hours. The Law extends this period for up to 3 days.

In general, this mitigates guarantees for protection against abuse for any citizen of the Russian Federation.

4.8. Restrictions to activities of religious organizations

The Law introduces restrictions for missionary activities and establishes the following criteria:

1) these are activities of a religious association (conducted directly by religious associations or persons and (or) legal entities designated by them);
2) they are aimed at distribution of information regarding their doctrine;
3) such information distribution is conducted among people who are not members (disciples) of this religious association;
4) the purpose of these activities is to engage such people in the religious organization as participants (disciples);
5) such activities are public, and are conducted through the media, the Internet or any other legitimate means.

Before “Yarovaya Package” adoption, the laws, restricting missionary activities, were enforced in 9 constituents of Russia: Autonomous Regions of Kursk, Smolensk, Voronezh, Kostroma, Pskov, Novgorod, Jewish Autonomous Region, Republic of North Ossetia – Alania. Now, due to the adoption of “Yarovaya Package” such restrictions shall be abolished as useless and contradictory with the Federal legislation87.

It is hard to imagine, in which way restrictions for missionary activities contribute to the fight against terrorism. Meanwhile this law is clearly a yet another blow to the freedom of conscience and of religion, because it prohibits to conduct missionary activities without a full package of documents (every missionary shall have a decision by the general meeting of members of the religious group regarding provision to him of

relevant authority, specifying the details of the written confirmation of receipt and registration of notification on creation and beginning of activities of the religious group, issued by a territorial body of the federal authority of the state registration). Such requirement shall not apply only to the head of the religious organization, member of its collegiate body and (or) its minister of religion. Missionary activities may be conducted only by those religious groups or organizations, which are registered in that capacity in the territorial administration of the Ministry of Justice of the Russian Federation.

It is prohibited to conduct missionary activities on land plots, where buildings or constructions, belonging to other confession, are located, without a written permission of the governing body of the correspondent religious association.

Missionary activities may be undertaken unhindered only at pilgrimage sites; at cemeteries and crematoriums; at the premises of educational organisations, historically used for the performance of religious services, as well as at premises rented or owned by a religious association.

Conduction of missionary activities is prohibited at residential property.

The Law prescribes that in case a religious organisation invites foreign citizens to conduct professional religious activities, an employment or civil law contract shall be concluded between such religious organization and a foreign citizen. Foreign citizens are prohibited to conduct professional religious activities in case a correspondent contract has not been concluded.

"Yarovaya Package" introduces new definitions of administrative offences:
- conduction of missionary activities in violation of the legislation on freedom of conscience and religion, and on religious organizations, shall be punished with a fine in the amount from RUB 5 000 to 50 000 for individuals; from RUB 100 000 to 1 000 000 for legal entities. In case such a violation is conducted by a foreign citizen or a stateless person, the amount of the fine may vary from RUB 30 000 to 50 000 with administrative deportation from the territory of the Russian Federation, or without a deportation.

It is clear that the Law might have been adopted to contribute to the support of the monopolistic position of the Russian Orthodox Church and restriction of activities of other religious organisations.

The largest practice of implementation of "Yarovaya Package" provisions is related to missionary activities conducted by religious organisations, distinct from the Russian Orthodox Church.

In over 3 months of "Yarovaya Package" existence as a law, dozens of representatives of religious organisations have been fined under its provisions:

July 2016
On the 27th of July 2016, 7 days after the adoption of "Yarovaya Package" proceedings for an administrative offence were initiated against Vadim Sibirev, a devotee of Krishna, for giving Krishna religious literature at the street in the city of Cherkessk (Karachaevo-Cherkessia). On the 15th of August 2016, the case was dismissed by court due to insufficient elements of the offense.

On the 31st of July 2016 Alexander Yakimov, Head of Christians of Evangelical Faith (pentecostals), delivered a speech at a celebration in Mari-Sholner (Mari El Republic).

---

90 https://ria.ru/incidents/20160815/1474387741.html
Nikolay Bakhtin, Prosecutor of Mari-Tureksk district, commented that on the 31st of July 2016 Alexander Yakimov was conducting a missionary activity "at the territory, which is not intended for religious meetings", namely "he was praying and praising the God at a public celebration, a social event". In accordance with Yakimov, he only congratulated the village chief and blessed its inhabitants. On the 1st of September 2016, the court found him guilty on and imposed on him a penalty amounting to RUB 5 000.

August 2016

August 2016, City of Noyabrsk (Yamalo-Nenets Autonomous Region). Alexey Teleus, Pastor of the Church of Evangelical Christians-Baptists, was charged with an administrative penalty amounting to RUB 5 000. He didn't appeal against that decision.

On the 27th of August 2016, Sergey Zhuravlev, Archbishop of the Christ the Saviour Orthodox Reformed Church (Kiev), was detained at the premises of the "New Hope" organisation, where he was conducting a sermon. A reason for the detention was a complaint for illegal missionary activities of Zhuravlev. He was accused of trying to convert the Jewish community into the Orthodox Christianity. In accordance with the religious leader, he was delivering a lecture for former drug and alcohol addicted persons, as well as for sex-workers about the history of Christianity and relations between the Orthodox Church and Israel, and did not try to convert anyone. He was imposed with a fine in the amount of RUB 5 000.

September 2016

September 14, 2016, City of Kemerovo (Region of Kemerovo). Irina Tischenko, Head of Women Allegiance of Ukrainian churches "New Generation" (a citizen of Ukraine) was imposed a penalty in the amount of RUB 30 000.

October 2016

October 5, 2016, City of Oryol (Region of Oryol). Donald Ossewaarde, a Baptist missionary from the USA, was fined RUB 40 000 by Zheleznodorozhny Court of the city of Oryol. Zheleznodorozhny District Court of the city of Oryol decided that, by inviting people to his home to study the Bible, Ossewaarde was conducting missionary activities on behalf of an unregistered religious group.

October 17, 2016, City of Kemerovo (Region of Kemerovo). Andrey Matyuzhov, Head of the church "New Generation", had not inform neither local authorities, nor the Russian Ministry of Justice for the region of Kemerovo regarding foundation of a new church, he neither registered it. He was holding church services and conducted sermons, visited by up to 200 people. The Court imposed a fine on him in the amount of RUB 40 000.

---

91 http://www.idelreal.org/a/27954187.html
93 http://baznica.info/article/noyabrsk-baptistov-oshtrofovali-za-missiyu-v-dome/
96 https://www.vedomosti.ru/politics/articles/2016/08/25/654414-zhertvami-zakona-yarovoi
November 2016

November 9, 2016, City of Astrakhan (Region of Astrakhan). Informal leader of local Scientologists in Astrakhan, Volgograd and Saratov was distributing information regarding L. Ron Hubbard’s works, and was fined for RUB 5 000.

In such a manner, "Yarovaya Package" provisions are designed not only for establishment of a total control over communications and calls by telephone or in the Internet, but also implement numerous minor amendments to the existing legal regulations, restricting the number of instruments available to the society to monitor the Government, while the Government, on the contrary, obtains unlimited control over all the aspects of life of its citizens, which, in the absence of effective and independent judiciary system and any guarantees for the right for privacy, virtually deprives people of any protection from the arbitrary intrusion of the Government.
Part 5. Security of communication services and Internet users are in the hands of the users. Risks and recommendations from NGO activists and civic activists

"Yarovaya Package" legalised and extended opportunities for the Government to control virtually any aspect of people's life. In a situation when the modern Government does not provide for effective instruments to challenge its illegal actions towards right for privacy of communications, civic activists shall take care themselves of their information security.

This problem emerged long before the adoption of "Yarovaya Package", while the latter demonstrated all the requirements and determination of the Government to control its citizens.

Risks for NGO and civil activists

It is necessary to understand that:

1. Information provided to the Government will be now made available for the law enforcement authorities and in the first place for FSS of Russia. No one knows how it is going to be stored or used: there are no mechanisms for its effective control. This is why civic activists should not be surprised that the information provided to social protection services was suddenly received by law enforcement authorities.

2. FSS of Russia will know long before your flight when and from which airport you are going to depart. Due to the fact that FSS of Russia exercises border control, you can be detained at the border or have problems with your departure.

3. The Law on prevention of delinquency allows for secret "preventive" monitoring of you, your placement on a "preventive" watch list, application of forced measures of educational influence towards you.

4. Now you can be 100% sure that secure Internet and telephone connection do not exist. If you don't take care of yourself and don't minimize the risks of monitoring of your communications by third parties, they may become available to those people, who were not supposed to receive them.

Taking into account that independent non-profit organizations and civic initiatives often become in the eyes of the Government its opponents (in our opinion, such position is fundamentally false, because in the most cases NGO and civic activists want to solve a specific issue, which is important for them, very often in collaboration with state authorities and local authorities), and activity of such activists is very often not supported by the State, all the information received may be used by the Government at its own discretion, while the Government may apply all the measures it considers feasible and necessary.

Creation of users’ profiles is being discussed by IT specialists for a long time. Such a profile will be based on your browser history, and will contain your political preferences, level of civil activity and other data.
Google collects a lot of information regarding its users to sell advertisement more effectively. The company is monitoring websites visited by users using DoubleClick network.

Until recently, such data were stored separately and basically were anonymous and attached to a specific browser and not to a person. However, in the end of October it was discovered that Google had amended its users’ policy. The company decided not to announce it publicly.

Now Google can create a full user’s profile, basing not only on the videos he or she watched, what emails he or she wrote, what he or she was searching in the Internet, but also on his or her browsing history, while all this information will be linked to a real name.68

Facebook Headquarters are located in New York, and the company is currently not providing information collected to the Russian law enforcement authorities.

In such a way, there are technical possibilities for creation of specific users’ profiles, due to the fact that law enforcement authorities were granted with virtually unlimited access to any information regarding any Russian citizen from the Government data bases. Thus, creation of a profile of a specific user becomes even easier, and it will allow to suppress civil activity with legal and illegal measures, "protecting" from NGOs and civic activists by loyal and indifferent citizens, which will provide for more pressure executed upon the civil society in Russia and civic initiatives.

**Five tips for NGOs and civic activists**

In order to minimize the risks of abuse of the right to privacy, civic activist should study information security measures and apply them in their practice.

**Firstly**, they should constantly update their knowledge regarding information security. Modern information technologies are developing rapidly and you need to stay abreast. You should visit seminars, read the articles in the Internet, consult with information security specialists.

**Secondly**, you should not use insecure communication tools for important messages. You should not use "Vkontakte" social network, mail.ru and yandex.ru mail services, Viber and Skype messengers, and all the Internet services provided by the companies with servers located in Russia. To ensure secure communication, you should use WhatsApp, secret chat Telegram, Signal. For correspondence, it is better to use gmail.com mail service.

**Thirdly**, you should not hold important conversations on the phone and send important information by SMS. Use Internet messengers, providing encryption (including voice encryption) for these purposes. The safest ones are WhatsApp and Signal.

**Fourthly**, in case your confidential correspondence is stored at your mobile phone or computer, protect it with passwords.

**Fifthly**, do not use flash drives to transmit information. It is better to use cloud services for these purposes.

These are 5 basic rules of information security, built upon the law, that will enhance your expertise in secure communication, and protect you privacy from intrusion of third parties.

---

68 https://meduza.io/cards/google-zapisyvaet-vse-chto-vy-delaete-v-internete-kak-emu-zapretit
In accordance with the Electronic Frontier Foundation\(^99\), the most secure messengers, providing encryption services and preventing third parties from accessing it (including messengers operators) are: Telegram (secret chats), Signal, WhatsApp.

Amnesty International in 2016 announced that in its opinion the most secure messengers are those using end-to-end encryption (encryption keys are stored at the end device, for example, at user’s smart phone). These are WhatsApp, iMessage and FaceTime by Apple, Duo by Google, messengers Line and Viber. Decryption keys for such conversations are stored with users only\(^100\).

**The full rating of messengers by Amnesty International**\(^101\)

<table>
<thead>
<tr>
<th>Company</th>
<th>Service</th>
<th>Number of active users</th>
<th>Number of points out of 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>FacebookMessenger, What’sApp</td>
<td>1 billion for each messenger</td>
<td>73</td>
</tr>
<tr>
<td>Apple</td>
<td>iMessage, FaceTime</td>
<td>Data is concealed. 1 billion of iPhone smartphones have been sold in the world</td>
<td>67</td>
</tr>
<tr>
<td>Telegram</td>
<td>Telegram Messenger</td>
<td>100 million</td>
<td>67</td>
</tr>
<tr>
<td>Google</td>
<td>Allo, Duo, Hangouts</td>
<td>Data is concealed, total number of Google users is more than 2 billion</td>
<td>53</td>
</tr>
<tr>
<td>Line</td>
<td>Line</td>
<td>218 million</td>
<td>47</td>
</tr>
<tr>
<td>Viber Media</td>
<td>Viber</td>
<td>250 million</td>
<td>47</td>
</tr>
<tr>
<td>Kakao Inc</td>
<td>KakaoTalk</td>
<td>49 million</td>
<td>40</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Skype</td>
<td>300 million</td>
<td>40</td>
</tr>
<tr>
<td>Snapchat</td>
<td>Snapchat</td>
<td>200 million</td>
<td>26</td>
</tr>
<tr>
<td>Blackberry</td>
<td>Blackberry Messenger</td>
<td>100 million</td>
<td>20</td>
</tr>
<tr>
<td>Tencent</td>
<td>QQ, WeChat</td>
<td>853 million, 697 million</td>
<td>0</td>
</tr>
</tbody>
</table>

Your information security is in your hands. Remember it, if you don’t want strangers to know everything about you.

\(^99\) [https://www.eff.org/node/82654](https://www.eff.org/node/82654)  
\(^100\) [http://www.rbc.ru/technology_and_media/21/10/2016/5808f07e9a79471023e8b713?from=newsfeed](http://www.rbc.ru/technology_and_media/21/10/2016/5808f07e9a79471023e8b713?from=newsfeed)  
\(^101\) [http://www.rbc.ru/technology_and_media/21/10/2016/5808f07e9a79471023e8b713?from=newsfeed](http://www.rbc.ru/technology_and_media/21/10/2016/5808f07e9a79471023e8b713?from=newsfeed)
"Yarovaya Package" introduces a system of extrajudicial control over the secrecy of communication of the citizens. At the same time, all the expenses, related to strengthening of the Government control over correspondence of citizens, will be incurred by commercial enterprises providing communication services, while the Government gets a virtually unlimited access to the content of communications of its citizens.

For failure to comply with these requirements administrative penalties up to 1 million RUB are imposed. Penalties for individuals and legal entities are also increased. The above mentioned measures are designed for granting a total control over the Internet and the secrecy of communication to the Government, as well as for increasing pressure on the opposition and the civic initiatives, which is not compliant with the fundamentals of a legal and democratic state.

From July 20, 2016 FSS of Russia was enabled to monitor private life of everyone living in Russia, regardless of the provisions of the Constitution of the Russian Federation, which guarantee a right to privacy of communication, telephone conversations, postal, telegraph and other communications, while this right may be restricted following a court decision only. It looks like the Russian Constitution does not work again. The Government already has access to the information regarding all the telephone connections of the Russian citizens, fixed-line and mobile, content of all the messages sent by SMS service or forums (including closed ones) in Russian social networks. In accordance with the Law such information shall be stored for 3 years, but it is not clear who will control the compliance with this provision and how effective such control will be.

From July 01, 2018 FSS of Russia will get access to the content of all correspondence and telephone conversations. Such information may be stored for 6 months.

"Yarovaya Package", adopted without any references to expert opinions or due public discussions, provides for unlimited access for the Government to control secrecy of communication of the citizens, monitor their movements, secretly monitor information transmitted by them, as well as abolish the services of anonymous data transmission, which constitutes an abuse of civil rights and freedoms of citizens, results in abuse of the right to respect for private and family life, freedom of expression, right for free information distribution, reduces the guarantees from arbitrary intrusion of the Government in privacy of citizens, demonstrates the absence of fundamentals of a democratic state in regulating legal relations in this area, and results in the total governmental control over an individual.

In the absence of guarantees against that state authorities will not abuse its power to the detriment of public interests, civic activists have to take care of their information security themselves.

NGOs and civic activists shall implement the latest technologies of secure communication, which do not require any specific skills and will enable them to independently control the provision of information to third parties and make sure that
they are the only ones empowered to control the distribution of information required for organization of socially useful activities.
NGO Lawyers Club is an expert initiative group of lawyers of NGOs and attorneys, collaborating with us.

Club’s mission is to promote philanthropy and develop the non-commercial sector by supporting vocational education of lawyers, protection of the right to freedom of association, as well as provision of legal support to civic initiatives and third sector organisations around Russia.

We are confident that legal professionals can and must contribute to creation and development of NGOs in order to develop the civil society in Russia. We are united by the human rights values and understanding that social and other problems cannot be solved without full participation of non-governmental organisations based on the initiative of the Russian citizens.

Media partner is NGO TV

https://www.youtube.com/user/NGOTVRussia
https://www.facebook.com/NGO-TV-1573681462853762/?fref=ts