Cybersecurity in Russia

Olga Chislova · Marina Sokolova

Received: 6 April 2021 / Accepted: 21 June 2021 / Published online: 19 July 2021
© Springer Fachmedien Wiesbaden GmbH 2021

Abstract Cybersecurity in Russia is not a standalone concept but an integral part of national information security, which influences its legal status and applicable regulation, and determines its development trends. The purpose of this article is to outline the Russian approach to cybersecurity, describe the related legal framework, representative business cases and trends in legal development.

Keywords Information security · Information Security Doctrine (of the Russian Federation) · Sovereign Internet Law · Law on Security of Information Infrastructure · Law on Communications

1 General understanding

Unlike the EU, where *cybersecurity* is a common term, Russia tends not to use this idiom in its official legal documents. The difference lies not so much in the area of terminology as in the underlying concept. Under cybersecurity, the EU understands various activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats¹, while in Russia cybersecurity is an integral part of the *information security* concept. Information security is

¹ (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013.

Olga Chislova (✉) · Marina Sokolova
Freshfields Bruckhaus Deringer, Moscow, Russian Federation
E-Mail: olga.chislova@freshfields.com

Marina Sokolova
E-Mail: marina.sokolova@freshfields.com

quite broadly defined and understood as protection of an individual, society and/or the state against internal and external information threats, thereby maintaining the constitutional rights and freedoms, and quality and standard of living of citizens, as well as the sovereignty, territorial integrity and sustainable socio-economic development of the Russian Federation, and the defence and security of the state². Therefore, in Russia cybersecurity is understood as one of the elements of information security, i.e., cybersecurity requirements are implemented in the context of the information security policy. This difference is critical to understanding the Russian approach to cybersecurity matters: information security in Russia is governed and regulated by the state to a big extent in the interests of the state, which makes this area quite politically influenced. It is aimed at establishing independence from international cyberspace, Russia's sovereignty in the information field, and the development of domestic IT infrastructure.

In 2014, the Russian business community attempted to alter the country's approach to cybersecurity: a national cybersecurity strategy was proposed whereunder businesses and civil society would participate in the development of the cybersecurity standards and policy, international cooperation in cybersecurity would increase and other states' experience would be implemented. However, the strategy was criticised by the RF Federal Security Service (FSS) and was never adopted [1].

Instead the Information Security Doctrine of the Russian Federation was adopted two years later. It does not provide for the business community's participation in development of cybersecurity standards, but sets out broad principles, such as protection of constitutional rights, protection of Russia's critical information infrastructure, development of Russian science and IT, delivery of accurate information on Russian state policy and official positions to domestic society and internationally, assistance in the creation of an international information security system, and protection of Russian sovereignty in the information field. In other words, the Information Security Doctrine focuses on the information security concept and considers cybersecurity as one of the means ensuring such information security. This approach has influenced further development of the Russian legal framework in this field of law, including, but not limited to:

- Federal Law No. 126-Φ3 On Communications dated 7 July 2003, as amended (the **Law on Communications**);
- Federal Law No. 149-Φ3 On Information, Information Technologies and the Protection of Information dated 27 July 2006, as amended (the **Law on Information**);
- Strategy of National Security in the Russian Federation adopted by Decree of the President of the Russian Federation No. 683 On the National Security Strategy of the Russian Federation dated 31 December 2015;
- Decree of the President of the Russian Federation No. 646 On Adopting the Doctrine of Information Security of the Russian Federation dated 5 December 2016 (the **Information Security Doctrine**); and

² Decree of the President of the Russian Federation No. 646 On Adopting the Doctrine of Information Security of the Russian Federation dated 5 December 2016.

- Federal Law No. 187-ФЗ On the Security of Critical Information Infrastructure of the Russian Federation dated 26 July 2017, as amended (the **Law on Security of Information Infrastructure**).

2 General overview of legal requirements

Even though the term cybersecurity is not broadly used in Russian legal documents, here and further we will use this term when discussing the technical aspects of information security.

Russian legal regulations on cybersecurity apply to the following areas:

- specific information protection regimes that require the implementation of certain cybersecurity measures (for instance, protection of personal data or protection of state secrecy);
- restrictions applying to communications providers (for instance, the requirement to store data on communications for a certain period of time);
- cybersecurity requirements applicable to critical information infrastructure;
- a number of articles contained in the Russian Federation Criminal Code that de-facto introduce additional restrictions (e.g., a prohibition on the creation of computer viruses and cyberfraud); and
- individual cybersecurity systems created by private companies, subject to general restrictions provided for by law.

2.1 Sovereign internet

One of the goals set out in the Information Security Doctrine is the introduction of Runet, i.e., an independent Russian internet.

In 2019, the so-called Sovereign Internet Law aimed at the independent functioning of the Russian segment of the internet was adopted³, which triggered creation of a national domain names system with top-level domain names .ru, .su, .pdf and the establishment of additional infrastructure for traffic maintenance and monitoring (including for DPI). The Federal Service for Supervision of Communications, Information Technology and Mass Media (**Roskommnadzor**) was provided with new powers to collect information from internet infrastructure owners, control connections to Internet Exchange Points and perform centralised management of the general communication networks, including by way of using special technical means for the prevention of threats and by giving binding instructions to communications operators and other persons in the event of a threat to the stability, security and integrity of the internet and other communications networks in Russia.

The Sovereign Internet Law laid down a legal basis for a Russian internet segment that can work independently from the global internet. Russian authorities, including

³ Federal Law No. 90-ФЗ On Introducing Amendments to the Federal Law on Communications and the Federal Law On Information, Information Technologies and Protection of Information dated 1 May 2019.

Roskomnadzor, have been entrusted with additional powers and technical abilities to monitor traffic and block access to certain resources.

The discussion of the Sovereign Internet Law received a significant public response: a meeting against the adoption of the bill, held in March 2019 in Moscow, according to journalists' reports gathered more than 15,000 [2].

The protest actions have not, however, changed Russia's approach to the matter. Although there have been delays in the implementation of the project, partially due to the COVID-19 pandemic [3] and partially due to a lack of clarity in the law itself [4], it is being implemented.

2.2 Security of critical information infrastructure

Another important legal development was the adoption, in 2017, of the Law on Security of Information Infrastructure, aimed at ensuring the safety and stable functioning of critical information infrastructure in Russia in case of cyberattacks. The law applies to authorities, state companies, private Russian companies and individual entrepreneurs that own, lease or otherwise legally possess various types of IT systems and networks used in twelve areas of activities, including healthcare, transportation, science, banking, the chemical industry and to Russian companies and individual entrepreneurs enabling the interaction of the above systems and networks (the law describes the above-listed as 'critical infrastructure subjects').

Under the Law on Security of Information Infrastructure, critical infrastructure subjects are required to transfer to 'primarily Russian' software and hardware. Specific requirements for such software and hardware are yet to be developed. Initially, such transfer was planned in May 2020, however, this proposal triggered objections of the business community mostly due to the insufficiency of the relevant Russian software and equipment [5] and the term has been moved to 2024 for the software and 2025 for the hardware [6].

2.3 The Yarovaya Law and the Telegram case

In 2016, the Law on Communications and some other federal laws were amended⁴ (unofficially this amendment is called the Yarovaya Law after one of the senators who proposed the amendment), in particular to extend Russian defence and law authorities' rights to access electronic information, oblige communications operators and the providers of information distribution via the internet (including messengers) to store certain information on the facts of communications and on the contents of communications for certain periods of time, and to provide such information to defence and legal authorities (including the FSS) in cases provided for by the legislation and to oblige the information distribution providers to disclose information to the FSS required to decode users' messages. The amendments introduced by the Yarovaya Law apply to all internet-based information distribution services providers,

⁴ Federal Law No 374-ФЗ On Introducing Amendments to the Federal Law On Counterterrorism and Some Other Legal Acts of the Russian Federation related to the Introduction of Additional Measures on Counterterrorism and Ensuring Public Safety dated 6 July 2016.

notwithstanding them being represented in Russia (e.g., Google and Facebook). The declared purpose of the amendments was to extend the authorities' powers to prevent terrorism in Russia, however, the amendments significantly restricted individuals' rights to privacy of correspondence, which triggered criticism by experts [7] and led to protests [8].

In 2017, the FSS requested the Telegram messenger service (released in 2013 by Pavel Durov, the founder of the largest social network in Russia—Vkontakte) to disclose decryption keys for users' chats due to the investigation of acts of terrorism in Saint Petersburg. Although Telegram argued that the FSS failed to present evidence on the accused individuals' involvement in the terrorist activities and that it was technically impossible to provide the general decryption keys for point-to-point encrypted chats, a fine of 800,000 roubles (ca 12,000 euros based on the exchange rate at the time) was imposed on Telegram and a Russian court issued an order to cut access to Telegram in Russia. Roskomnadzor tried to block related IP-addresses (ca 20 mln IP addresses were affected) to enforce the court order. However, this resulted in user access to various resources being disrupted (including Google, Viber, ResearchGate and Science), while Telegram remained available.

In June 2020, Roskomnadzor announced the withdrawal of the blocking of Telegram [9]. According to the official information, this decision is based on Telegram's consent to cooperate in the prevention of extremism and terrorism. In November 2020, Roskomnadzor announced the opening of its own channel in Telegram.

2.4 Personal data

Under Russian law, personal data is a standalone category of information, the processing of which is protected by law, including when this information is processed using the internet. In 2014, the Information Law and the Federal Law On Personal Data⁵ were amended. Under the amendments, upon collection of Russian citizens' personal data the personal data operators must perform certain actions only using databases located in Russia (the Localisation Requirement) and a legal mechanism of stopping access to websites that violate the Localisation Requirement was introduced. The new rule applies to companies that are not represented in Russia provided that their business activities are targeting the Russian market, as well as to companies registered and represented in Russia.

Failure to comply with the Localisation Requirement resulted in access to LinkedIn being fully restricted in Russia since 2016 and in fines of around 4 million roubles (ca 44,400 euros) each for Facebook and Twitter even though none of the three companies are represented in Russia.

⁵ Federal Law No. 152-ФЗ On Personal Data dated 27 July 2006.

2.5 Restrictions on the use of anonymisers

In 2017, the Russian Federation restricted possibilities of accessing websites that are blocked in Russia [10]⁶. Internet-providers became obliged to identify owners of websites, programs or services that permit access to forbidden websites in Russia (this applies, *inter alia*, to VPN services, anonymisers and Tor) and provide this information to Roskomnadzor. Thereafter, the relevant service must either support Roskomnadzor in blocking the websites or access to such service will be limited in Russia.

3 Trends

These days, cybersecurity is a popular news topic and is a focus of legal development. There are a number of major amendments that have recently been implemented or are under discussion, in particular:

- the President of Russia has recently ordered a standalone Russian cybersecurity policy to be developed [11];
- at the end of 2020, the Russian Code of Administrative Offences was supplemented with a new article establishing liability for failure to comply with the requirements to restrict access to information that is considered illegal in Russia⁷. Several weeks later, Roskomnadzor ordered that Facebook, Instagram, Twitter, TikTok and some other platforms [12, 13] delete information relating to calls for unauthorised public protests and initiated investigations that triggered fines for some of the platforms' failures to delete this information (the maximum amount of a fine for this breach is 4 million roubles (ca 44,400 euro); failure to comply with Roskomnadzor's requirement may result in the blocking of access to the relevant platform in Russia or limiting the speed of the platform's loading time); and
- implementation of additional requirements for foreign IT-companies that operate in Russia but are not represented on its territory, such as the introduction of additional taxes for foreign IT companies [14], the implementation of a requirement for foreign IT companies to open representative offices or branches in Russia in order to be permitted to work in Russia [15], a requirement for foreign IT-companies to pay Russian individual income tax for Russia-based developers [16] and a demand to foreign IT-companies to comply with Russian legislation [17] are currently being discussed.

⁶ Federal Law No. 511-ФЗ On Introducing Amendments to the Russian Federation Code of Administrative Offences dated 30 December 2020.

⁷ Federal Law No. 511-ФЗ On Introducing Amendments to the Russian Federation Code of Administrative Offences dated 30 December 2020.

References

1. Federation Council of the Federal Assembly of the Russian Federation's official website (2013) Transcript of Parliament hearings on the topic of Legislative Procurement of National Cybersecurity in the Russian Federation held on 29 November 2013. <http://council.gov.ru/media/files/41d4c80ace277857ad9c.pdf>. Accessed 31 Mar 2021
2. Kommersant (2019) People who do not know how to use Email are attempting to regulate the Internet. <https://www.kommersant.ru/doc/3907444> (Created 10 Mar 2019). Accessed 31 Mar 2021
3. Interfax (2021) Runet stability trainings delayed until the end of the pandemic. <https://www.interfax.ru/russia/746893> (Created 26 Jan 2021). Accessed 30 Mar 2021
4. Kommersant (2020) Operators pumped up with 'sovereign Internet'. <https://www.kommersant.ru/doc/4494156?query> (Created 18 Sept 2020). Accessed 30 Mar 2021 (No. 170, p. 7)
5. Kommersant (2020) Three-year phase-out for imports. <https://www.kommersant.ru/doc/4557385> (Created 2 Nov 2020). Accessed 30 Mar 2021 (No. 201/II, p. 7)
6. Draft decree of the President of the Russian Federation On Measures to Ensure Economic Area Information Security upon use of Software and Hardware at Critical Information Infrastructure Facilities. <https://regulation.gov.ru/projects#npa=109874> (Created 21 May 2020). Accessed 31 Mar 2021 (project ID: 02/06/10-20/00109874)
7. Zasursky I (2018) The triumph of Cheka officials or why is the Yarovaya Law not working? In: Snob. <https://snob.ru/entry/166484/> (Created 3 Oct 2018). Accessed 31 Mar 2021
8. RBC (2016) A few thousand people gathered to a protest against the Yarovaya Law in Moscow. <https://www.rbc.ru/politics/09/08/2016/57aa0a259a79470ed51332fd> (Created 9 Aug 2016). Accessed 31 Mar 2021
9. The Federal Service for Supervision of Communications, Information Technologies and Mass Media's official website, news (2020) On Telegram messenger. The Federal Service for Supervision of Communications, Information Technologies and Mass Media. <https://rkn.gov.ru/news/rsoc/news73050.htm> (Created 18 June 2020). Accessed 30 Mar 2021
10. Federal law No. 276-Φ3 On Introducing Amendments to the Federal Law On Information, Information Technologies and Protection of Information dated 29 July 2017. The amendments came into force on 1 November 2017
11. Parlamentskaya Gazeta (2021) President calls for a strategy on preventing cybercrimes. <https://www.pnp.ru/politics/prezident-prizval-sozdat-strategiyu-po-borbe-s-kiberprestupnostyu.html> (Created 24 Feb 2021). Accessed 30 Mar 2021
12. The Federal Service for Supervision of Communications, Information Technology and Mass Media official website, news (2021) Roskomnadzor will hold Internet-platforms liable for engaging teenagers in illegal activities. <https://rkn.gov.ru/news/rsoc/news73302.htm> (Created 21 Jan 2021). Accessed 30 Mar 2021
13. The Federal Service for Supervision of Communications, Information Technology and Mass Media's official website, news (2021) Social networks will be held liable for engaging teenagers in illegal activities. <https://rkn.gov.ru/news/rsoc/news73328.htm> (Created 27 Jan 2021). Accessed 30 Mar 2021
14. Parlamentskaya Gazeta (2021) Roskomnadzor will consider a digital tax as a requirement for foreign IT-companies. <https://www.pnp.ru/politics/v-roskomnadzore-dopustili-vvedenie-cifrovogo-naloga-dlya-zarubezhnykh-it-kompaniy.html> (Created 12 Feb 2021). Accessed 30 Mar 2021
15. (2021) A draft bill obliging IT-companies to have representative offices in Russia will be submitted to the State Duma. <https://www.pnp.ru/economics/v-gosdumu-vnesut-proekt-obyazyvayushhiy-it-kompanii-imet-predstavitelstva-v-rossii.html> (Created 8 Feb 2021). Accessed 30 Mar 2021
16. Parlamentskaya Gazeta (2021) Foreign IT-companies can be obliged to pay individual income tax in Russia. <https://www.pnp.ru/politics/v-rossii-mogut-obyazat-inostrannye-it-kompanii-platit-ndfl.html> (Created 5 Mar 2021). Accessed 31 Mar 2021
17. Parlamentskaya Gazeta (2021) A State Duma committee will address a call to comply with Russian laws to IT-companies. <https://www.pnp.ru/politics/komissiya-gosdumy-obratitsya-k-it-kompaniyam-s-prizyvom-ispolnyat-rossiyskie-zakony.html> (Created 16 Mar 2021). Accessed 31 Mar 2021

Olga Chislova Counsel

Marina Sokolova Consultant