CHAPTER 6

Personal Data Protection in Russia

Alexander Gurkov

6.1 Introduction

Data protection is a recent area of law in Russia. The Russian State Duma enacted data protection laws only in 2006. Before that, the Russian Constitution's (1993) articles 23 and 24 laid the foundations for data protection. Starting in 2014, the Russian legislator introduced major amendments to data protection regulations, allowing for more control by governmental agencies over data flow.

The ideas of the Russian legislator are not unique in the global arena and were in some form implemented in other jurisdictions. This chapter uses EU conceptions of personal data protection as a point of reference. In 2018, the EU 2016 General Data Protection Regulation (GDPR) took effect and influenced the development of the data protection sphere around the globe. As one of the most comprehensive data protection legislations implemented in the world, the GDPR is a good point of comparison.

After the introduction (Sect. 6.1), the chapter provides an overview of the legal framework of data protection in Russia (Sect. 6.2). This lays the foundation for the next sections, which explain three important changes in Russian data protection legislation. These changes provided governmental agencies in Russia with more control over transferring information: introduction of a data localization requirement (Sect. 6.3), the Yarovaya law (Sect. 6.4), and regulations aimed at creating a sovereign internet (Sect. 6.5). The chapter ends with a section analyzing the influence of a political case on the understanding of personal data by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) and showing the

A. Gurkov (✉)
University of Helsinki, Helsinki, Finland
e-mail: alexander.gurkov@helsinki.fi

© The Author(s) 2021

D. Gritsenko et al. (eds.), *The Palgrave Handbook of Digital Russia Studies*, https://doi.org/10.1007/978-3-030-42855-6_6

vague nature of legislative definitions that gives public authorities vast freedoms in the application of regulations (Sect. 6.6).

Many Russian data protection legislative initiatives fall outside of world trends. Yet, some initiatives align Russian legislation with global trends, with the caveat that changes can be implemented when the government needs them to win a political case. This chapter shows the growing role and authority of Roskomnadzor, which will soon receive the potential to control the entirety of internet traffic in Russia and the ability to isolate the Russian internet. Some requirements of Russian data protection legislation are unprecedented in the world and are very costly for companies. Overall, the Russian legislator and various enforcement agencies act not with the aim of protecting individual rights in the sphere of personal data protection but with the aim of providing Russian authorities with more power to monitor and control the flow of data in Russia. This can be a legitimate aim given the fast development of personal data threats, but such an aim should be stated clearly and openly.

6.2 Ground Rules

6.2.1 Legal Framework

Articles 23 and 24 of the Russian Constitution (1993) already show that the main subjects to which data protection legislation is directed are data subjects and data operators. These same ideas were reflected in the legislation.

Article 23 provides that "Everyone is entitled to privacy of personal life, personal and family secrets, protection of one's honor and good name." Privacy is the right to control information about oneself. The right to privacy is a universal human right and is recognized as such by the Universal Declaration of Human Rights and the European Convention of Human Rights. It is the foundation for the right to data protection. The right to data protection originates from privacy but is not a universal human right. It is aimed toward operators of personal data to ensure its fair processing. Correspondingly, article 24 of the Russian Constitution addresses operators of personal data. It requires that the "collection, storage, usage, and distribution of information on private life are not permitted without the approval of a person." Before the enactment of specialized legislation, in December 2005 Russia ratified the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention). The Council of Europe Convention is a foundation on which several countries have built their data protection legislation.

In July 2007, the State Duma passed two laws dedicated to data protection: Federal Law No. 149-FZ "*Ob informacii, informacionnyh tehnologiâh i o zâsite informacii*" (On information, information technologies and data protection, Data Protection Act) and Federal Law No. 152-FZ "*O personal'nyh dannyh*" (Personal Data Law). The provisions of these acts were conventional and similar to those of the 1995 European Data Protection directive (Garrie and

Byhovsky 2017, 239). The Personal Data Law is the principal law regulating this sphere in Russia. It sets the purpose of personal data protection—securing the rights and freedoms of a person and a citizen in processing one's data (article 2).

Up until 2014, Russian data protection regulations did not stand out from the Council of Europe Convention. Following the terrorist acts in the city of Volgograd in 2013, the State Duma passed an anti-terrorist packet of legislation. A part of that package was the Federal Law of July 21, 2014, No. 242-FZ (Localization law), which introduced the localization requirement (more on that in Sect. 6.3). Apart from the Russian legislator, several authorities are competent to create data protection regulations. The Russian President, the Russian government, and Federal Services take active roles in this sphere (for more, see Chap. 3).

6.2.2 Enforcing Authorities

Among public authorities, Roskomnadzor plays the most active role. Dmitry Medvedev established Roskomnadzor in 2008 (Decree of the President No. 1715). Roskomnadzor reports to the Ministry of Digital Development, Communications and Mass Media (Ministry of Communications). It has many important competencies such as monitoring mass media and keeping the registries of data operators and prohibited websites (Resolution of the Government on Roskomnadzor). When it comes to specific powers of Roskomnadzor, the vector of activity of this Federal Service derogates from the direction in which personal data protection is aimed—securing individual rights and freedoms. Following article 23 of the Data Protection Act, Roskomnadzor can investigate and initiate control and supervision of data operators, without regard to violation of personal rights of individuals. It acts without regard to whether those individuals whose data is processed have any claims to data operators. As a result, the activity of Roskomnadzor is directed toward the protection of data as such and not toward the protection of individual rights affected by data processing (Tereshhenko 2018, 146).

Apart from Roskomnadzor, a few other authorities exercise their power in enforcing data protection policy in Russia. The Office of the Prosecutor is responsible for prosecuting criminal actions related to infringement of data protection. The Federal Service on Technical and Export Control is responsible for supervising the safety of personal data within the informational infrastructure of Russia.

6.2.3 Main Categories of Data Protection Legislation

The main categories that define data protection legislation in Russia are data, personal data, data operators, data processing, and transfer of personal data. Article 2(1) of the Data Protection Act defines information as any data irrespective of its form of representation. Following article 3(1) of the Personal

Data Law, personal data is any information directly or indirectly related to a certain or identifiable individual (data subject). The law will not protect data that does not relate to an identifiable individual (anonymized data). Following this definition, it could be hard to differentiate between technical data and personal data, as almost any transaction made on the internet will constitute personal data (Bauer et al. 2015, 2).

When it comes to establishing the criteria of what counts as an identifiable individual, Roskomnadzor's practices may create some ambiguity. For example, in 2017 the Pension Fund of Russia leaked information containing full names and surnames of its clients, their taxpayer numbers, and information about their pension savings. As per the response of the Pension Fund, these do not constitute a data breach, as such data does not allow to identify a person (Tereshhenko 2018, 152). Roskomnadzor did not respond to this breach with any action. As much as the Pension Fund wanted to keep the breach harmless, information that contains names, surnames, and identity numbers is without a doubt personal data. Senior officials of Roskomnadzor stated in a 2015 commentary to the Personal Data Law that an individual taxpayer number allows to clearly identify a natural person (Gafurova et al. 2015, 16).

The Personal Data Law differentiates between categories of personal data. According to article 10 of the law, a special regulation applies to data relating to racial and national identity, political views, religious or philosophical beliefs, health conditions, and intimate life. The processing of such data can only be done in cases prescribed by the law, for example, if a data subject gives written consent to processing the data.

Following article 3(2) of the Personal Data Law, an operator is an authority, a company, or an individual that organizes and (or) performs processing of personal data. An operator also defines the purpose of personal data processing and composition of personal data to be processed, as well as actions toward personal data. Data protection legislation applies to all operators of data and third parties authorized by the operators. A general rule is that data operators need to notify Roskomnadzor of their intent to process data before engaging in data processing (article 22). There are certain cases where such notification is not necessary, for example, where data processing is done under labor legislation, if the data only includes a surname, name, and paternal name of the data subject, or if the data subject revealed the data in open access.

When collecting personal data, operators need to inform subjects about certain required aspects of data processing. For example, following article 18.1 (1) (2), operators need to publish a data processing policy. The law takes a reasonable approach by imposing this obligation on operators that are legal entities. In practice, this means that natural persons, as well as individual entrepreneurs, do not need to publish their processing policy.

Data operators need to set up security measures. According to article 18.1 of the law, data operators are free to choose measures that they need to take to comply with the law. The recommended measures under the law are

appointing a data protection officer, implementing certain organizational and technical measures aimed at securing the data, and performing internal control and audit.

What is interesting is that the list of such measures does not include an obligation to notify of a data breach, to either Roskomnadzor or data subjects. There was an attempt to amend the legislation and introduce the obligation to notify Roskomnadzor, Ministry of Internal Affairs, and even relevant data subjects of data breaches, but the draft law has not been passed by the State Duma since 2017 (Draft law No. 416052-6).

Data processing is any action or combination of actions associated with personal data (with or without the means of automation), including collection, recording, systematization, storing, extracting, and transferring. Processing should be adequate, relevant, and not excessive to the purpose for which the data is processed. Following article 5(7) of the Personal Data Law, one of the principles of data processing is that once the goal for which the information was processed is reached, the operator needs to anonymize or destroy the data unless there was any agreement to the contrary. At the moment, there are no detailed rules on how data should be destroyed. However, corresponding amendments authorizing Roskomnadzor to establish such detailed rules are being considered by the State Duma (Draft law "On termination of personal data").

The consent of data subjects is an essential part of processing personal data. Following article 9 of the Data Protection Law, an individual should give one's written consent for data processing. The consent should be specific, informed, and deliberate. It can be acquired in any form that can confirm that it was given, including filling online forms. The data subject can later change one's mind and revoke consent for data processing. Data operators bear the burden of providing proof that a data subject provided her consent.

Following article 9(4)(4) of the law, in certain cases, including when processing data related to political views, religious beliefs, health conditions, and intimate life, consent should be given in writing. The written form of consent should include the purpose of data processing. The law does not specifically require that the data processor ask a data subject to provide separate consent for each purpose of data processing. Data processors often construe this provision in such a way as to list different purposes of data processing in one form. Yet, since construing the law in the other direction is possible, there is a material risk that Roskomnadzor will require written consent from a data subject for every purpose of data processing. This was the case in a dispute between a limited liability company (LLC) Skartel and Roskomnadzor (*LLC Skartel v. Roskomnadzor Administration of the Central Federal Circuit*). The commercial court of the city of Moscow and then the appellate court confirmed the position of Roskomnadzor. The clients of Skartel signed terms and conditions that listed certain purposes of data processing. After doing that, some of the clients made additional agreements online. Such agreements included more purposes of data processing. The courts agreed with Roskomnadzor that consent for

such additional purposes of data processing, following verbatim reading of the law, should have also been given in paper-based writing form. To address this situation, the Ministry of Communications drafted amendments to the law on data protection that, among other measures, would allow receiving single consent of a person for multiple purposes of data processing (Draft law "On single consent form"). This is one of the examples where the aim of amendments is to ease the burden for data operators, as opposed to creating numerous new regulations introducing limitations and obligations in the sphere of data protection, as will be shown in further sections of this chapter.

Personal data can be processed without the data subject's consent in certain cases (article 6). For example, consent is not needed when data processing is necessary for a professional journalistic activity or when it is necessary for the enforcement of a court or a public authority decision.

6.2.4 Transfer Outside of Russia

Data operators can transfer personal data outside of Russia. Before making such transfer, the operator has to make sure that the rights of the personal data subject will receive adequate protection in the receiving country of the transfer. Article 12(1) of the Personal Data Law provides that all signatories to the Council of Europe Convention provide adequate protection to personal data. Apart from this, Roskomnadzor keeps a regularly updated list of countries that provide such protection (Order of Roskomnadzor on the list of countries with adequate personal data protection).

6.2.5 Territorial Scope of Application

The internet spreads across national borders. Russian citizens can access websites of operators located all around the world (except for those blocked by Roskomnadzor). This does not mean that all of those operators need to comply with Russian localization requirements. The Data Protection Law does not specifically establish the territorial scope of its application. At the same time, when defining operators of personal data, the law does not limit operators to only companies registered in Russia. In view of Roskomnadzor, the Personal Data Law is binding upon foreign companies that process personal data in Russia (Roskomnadzor 2019a). The territorial scope is defined by data processing that (1) either takes place or is aimed at Russia or (2) concerns the data of Russian citizens. What is important is not where a company/person is based but the territory at which the actions of such a company or a person are directed. Companies incorporated outside of Russia may nevertheless be subject to Russian data protection regulations. In a similar fashion, article 3 of the GDPR establishes that its data protection requirements are binding not only for companies established in EU member states but also for companies located anywhere in the world if they process the data of EU citizens. The importance

of the territorial aspect of Russian data protection regulations is amplified with the adoption of the localization requirement for data operators.

6.3 Localization Requirement

The personal data localization requirement was a part of the 2014 anti-terrorist legislation package (Localization Law). Before the enactment of these amendments, there were no limitations on localization—processing and storing information of Russian citizens could be done on servers located anywhere in the world (Garrie and Byhovsky 2017, 242). The purpose of the localization requirements, according to the head of Roskomnadzor, is to "provide an extra protection for Russian citizens both from misuse of their personal data by foreign companies and from surveillance of foreign governments" (Savelyev 2016, 138; Zharov 2014).

From an economic standpoint, the introduction of the localization requirement is a self-imposed sanction that seriously weakens Russia's ability to attract investments (Bauer et al. 2015, 3). The localization rules affect many companies, including giants like Apple, Microsoft, Google, Facebook, and Twitter as well as big companies such as eBay, PayPal, Booking.com, and Reddit (Zhuravlev and Brazhnik 2014, 26). When enacted, these regulations disincentivized some companies from entering the Russian market. Such was the case with Spotify, which canceled its plans to launch services in Russia in 2015 due to the localization requirement (Garrie and Byhovsky 2017, 244).

The law imposes obligations for data operators and provides new competences to Roskomnadzor. When collecting and processing online data regarding Russian citizens, an operator must use databases (servers) that are located in Russia. Roskomnadzor received expanded competences while the entities that it supervises lost some guarantees. Following article 3 of the Localization Law, Roskomnadzor in its control and supervision over personal data protection no longer follows the guarantees provided to legal entities and sole entrepreneurs by the Federal Law "*O zaŝite prav ûridičeskih lic i individual'nyh predprinimatelej*" (On the protection of businesses). In practice, this means more freedom to Roskomnadzor and less control over its actions from other public authorities. For example, the Public Prosecution Office controls public authorities by approving their plans for inspections of businesses. Following Section II of the Roskomnadzor Inspection Rules, Roskomnadzor now plans its inspections without coordination with the Prosecution Office and has more freedom in making changes to inspection plans.

Roskomnadzor has defined priority spheres of interest where it most diligently monitors compliance with localization requirements. These spheres include, but are not limited to, recruiting agencies, credit companies, hotel businesses, and insurance companies (Roskomnadzor 2017). In these niches, by the very nature of business (recruiting agencies) or due to legislative requirements (insurance and credit companies), companies have to collect customers' personal data.

6.3.1 Subjects of the Obligation

Following article 18(5) of the Personal Data Law, when collecting personal data of Russian citizens, data operators should provide for recording, systematization, accumulation, and storage of data by using databases (servers) located in Russia. It is important to note that the localization requirement is limited to only some of the actions that constitute data processing—collecting the personal data of Russian citizens. Correspondingly, other actions of data processors, including usage, anonymization, erasure, and destruction, are not subject to this requirement.

Roskomnadzor has issued a clarification on when a data operator needs to comply with regulations. Such instances include using a domain name that is connected to Russia, like ru, рф, or su; having a Russian-language version of a website; and/or performance in Russia of a contract made on a website. In practice, this means that if an online store offers delivery to Russia, it needs to use a Russian server to process the data of Russian citizens.

6.3.2 Registry of Infringers

Roskomnadzor keeps a constantly updated Registry of Infringers of the Rights of Personal Data Subjects. In August 2016, it filed a claim to include the social network LinkedIn in the Registry of Infringers for failures to comply with the localization requirement and other data protection laws (*Roskomnadzor v. LinkedIn Corporation*). After winning the case in the court of first instance and the court of appeal, Roskomnadzor blocked LinkedIn. LinkedIn is not the only major internet service that received the attention of Roskomnadzor. According to the commentaries of Roskomnadzor representatives, Facebook and Twitter also did not comply with the regulations. However, a differentiated treatment was given to LinkedIn due to "repeated reports of data leaks from LinkedIn" (Bondarev et al. 2016). Perhaps the Russian government expected LinkedIn to comply given that LinkedIn located its servers in China to avoid the ban (Mozur and Goel 2014). Twitter and Facebook failed to comply with localization requirements in China and were banned there.

6.3.3 Amplification of Fines for Infringement

Article 13.11 of the Russian Code of Administrative Offences (CAO) establishes penalties for the infringement of Russian data protection regulations. Currently, it does not contain penalties for failing to comply with the localization requirement. Because of this, when Roskomnadzor was trying to pressure Twitter and Facebook into localizing their databases, the federal service had to fine the companies only for failing to provide information about the localization of their databases—an infringement provided in article 19.7 of the CAO. The maximum fine in this article is 5000 rubles (approximately 70

euros). Correspondingly, Twitter and Facebook were fined 3000 and 5000 rubles, respectively.

To influence this situation, the State Duma is considering the Draft Federal law "On amending the Code of Administrative Offences of Russia." The draft introduces special provisions for the violation of the data localization requirement and substantially increases fines—up to 18 million rubles (approximately 252,000 euros). Roskomnadzor will likely not attempt to block Twitter and Facebook for several reasons. First, Twitter and Facebook already demonstrated in the Chinese market that they are not willing to compromise under the risk of a ban. Second, blocking them will cause a bigger international response than that of LinkedIn. Third, Roskomnadzor does not have the technical means to properly implement a ban against such giants, as the futile attempt to block Telegram messenger demonstrated (discussed in Sect. 6.4).

6.4 Yarovaya Law

In 2016, the State Duma enacted two laws that are commonly referred to by the name of one of their authors—Irina Yarovaya—Federal Law 374-FZ and Federal Law 375-FZ (Yarovaya law). As per the Yarovaya law, organizers of data distribution are bound to store transferred information and provide Russian enforcement authorities with encryption keys (for more, see Chap. 5).

6.4.1 Storing Requirement

According to the newly introduced article 10.1 of the Data Protection Act, from July 2018, organizers of data distribution on the internet should, first, store text messages, voice communications, images, audio, video, and other messages of users in Russia for six months and, second, store all these messages' and users' metadata for one year. To top this off, in April 2018 the government of Russia issued a Resolution binding telecommunications providers to store all internet traffic data for 30 days (Resolution on Internet Traffic). As per the report of the Analytical Credit Rating Agency of October 2018, the aggregated cost for implementing these measures just for Russian mobile networks will exceed 250 billion rubles (approximately 3.5 billion euros) (Tishina 2018). The volume of stored data for 2019 is estimated at 60 exabytes (60 billion gigabytes), which is challenging to implement (Kolomychenko 2016).

A more controversial part of these amendments is the duty of the organizer of data distribution to provide state intelligence and surveillance authorities with access to the above-listed information. Data organizers will have to provide Russian enforcement authorities access to sensitive information without a court order. The aforementioned April 2018 Resolution of the Government, in clause 4, officially includes technical means of data accumulation into communications equipment of intelligence and surveillance operations. By this inclusion, the Resolution provides unmonitored access for enforcement

authorities to stored data of telecommunication providers. Communications equipment of enforcement authorities is constantly connected to data accumulation centers. Authorities do not need to ask for access to this information or even notify service providers. The GDPR does not provide for any comparable duty. Such obligation is clearly aimed at easing state control and not toward the protection of individual rights for personal data.

Similar regulation for internet organizers of data distribution was issued on October 29, 2018, by the Decree of the Ministry of Communications. Clause III(4) of the Decree sets up a upfront requirement for data distribution organizers—technical means should provide search, processing, and transfer of stored data to FSB (*Federal'naâ služba bezopasnosti*, Federal Security Service). Roskomnadzor keeps a Registry of Organizers of Data Distribution. As of October 2019, the registry contains 182 entries. Among the companies that are listed as organizers (and, correspondingly, bound to comply with the technological requirement of providing access to the Federal Security Service) are services like social network VKontakte, public email services Mail.ru and Mail.Yandex, cloud storage service Disk.Yandex, dating service Tinder, and classified advertisements website Avito. Being on that list and refusing to provide access to data can lead to blocking of the corresponding company's website.

Even before enactment of the Data Protection Act and Personal Data Law, regulations required Russian mobile operators to install devices providing access to Russian enforcement authorities to messages transmitted over mobile networks. These provisions were the subject of a dispute resolved by the European Court of Human Rights (ECtHR) in the case of *Roman Zakharov v. Russia*. Roman Zakharov (applicant), the editor-in-chief of a publishing company, filed a claim against Russian mobile telecom companies for violating his right to privacy of telephone communications. The mobile companies provided access for the FSB to install equipment intercepting all telephone communications. After losing this case in Russian courts, on October 20, 2006, Zakharov applied to the ECtHR.

In its judgment of December 4, 2015, the ECtHR noted that the legislation in question requires mobile operators to install equipment allowing the FSB to intercept communications of all users. The FSB does not need to notify users or telecom companies of such intrusion. The ECtHR indicated that the interception of telephone conversations can be justified by the aims of protection of national security, public safety, and prevention of crime. Such was the case in Russia. At the same time, legislation should provide adequate safeguards against abuses and guarantees that such a system will only be used when these measures are necessary. In view of the ECtHR, Russian legislation allowed such secret measures "in respect of a very wide range of offenses." Telephone conversation interceptions can be applied not only in regard to suspects but also toward persons that might possess information about an offense. The secrecy of interceptions was subject to court control. As a general rule, any interception needed a prior court order. Yet, some information, for example, about undercover agents or about the organization and tactics of conducting

operational-search measures, could not be submitted to a court. As a result, courts were not able to assess how reasonable the measures were. Courts could also order measures that were very wide in scope—like authorizing the interception of all conversations in the area where a crime was committed, without limiting it to specific persons. Enforcement authorities are not bound to notify telecom users that their conversations are intercepted. In light of the abovementioned argument, the ECtHR found that Russian legislation "did not provide adequate and effective guarantees against arbitrariness and the risk of abuse."

The very same day that the ECtHR made this ruling, the State Duma approved the draft law amending the Federal Constitutional Law "On the Constitutional Court of Russia." The amendments allow the Constitutional Court to consider whether enforcement of an ECtHR decision will be contrary to the Russian Constitution and allow refusal of performing such a decision.

6.4.2 Encryption Keys

Having access to stored information does not necessarily allow enforcement authorities to reach their goals. The majority of transferred data is encrypted. To get access, for example, to the messages of the users, the enforcement authorities will need to possess encryption keys. Following article 4.1 of the Data Protection Act, when organizers of data distribution use encoding, they have to provide the FSB with keys for decoding electronic messages. The most notorious case based on the implementation of this rule was the conflict between FSB and Telegram messenger. In July 2017 Roskomnadzor included Telegram into the registry of organizers of data distribution. FSB requested Telegram to provide it with encryption keys. Telegram refused and Roskomnadzor applied to the Taganskij district court of Moscow to fine and block Telegram (*Roskomnadzor v. Telegram Messenger Limited Liability Partnership*). The court ruled in favor of Roskomnadzor. The Supreme Court of Russia upheld the decision. For technical reasons, Roskomnadzor was not able to block Telegram. In its crusade against the messenger, Roskomnadzor blocked over 50 virtual private network (VPN) services and anonymizers (Tereshhenko 2018, 148). The services of Yandex, Viber, Google, and VKontakte had interruptions or were blocked for some time in the implementation of these measures (Suharevskaja 2018). Yet, these measures turned futile.

The FSB requested Yandex, Russia's largest technology company and fifth largest search engine worldwide, to provide it with encryption keys (Kolomychenko 2019). Yandex offers over 70 services in Russia that include public email, cloud storage, and online map services. At first, Yandex made a public refusal to provide FSB with the keys. Later, Yandex and the head of Roskomnadzor reported that Yandex and the FSB were able to find a solution to comply with the Yarovaya law but did not disclose the details of such solution (Kuznecova and Vyrodova 2019).

6.5 Sovereign Runet

6.5.1 Russian Informational Security

Since 2016, the protection of personal data is no longer a priority direction of Russian informational security doctrine. Personal data protection lost its place to countering the threats of informational security from foreign countries and actors. This conclusion can be made by analyzing the 2016 Presidential Decree of Vladimir Putin, which set up a new Doctrine of informational security in Russia (Doctrine). Following Clause III of the Doctrine, the President sees the main threats to Russian informational security coming from hostile geopolitical, military-political, terrorist, extremist, and criminal aims of unnamed foreign countries and actors. The Doctrine is predominantly focused on establishing protection and responses in the military sphere. The Doctrine replaced the 2000 Doctrine of Informational Security, which was also introduced by Putin. What is interesting is that the 2000 Doctrine set the protection of interests of a person as the first goal.

The 2016 Doctrine aims to protect the "critical informational infrastructure" of Russia. In 2019, in the implementation of the Doctrine, the State Duma has introduced amendments to the Data Protection Act and the Federal Law on Communications (Sovereign Runet law). The amendments introduce a set of measures aimed at ensuring the stable operation of the Russian internet (Runet). According to article 56.1(1) of the Law on Communications, the obligation to ensure safe, steady, and integral functioning of the Runet falls on the communications operators and owners of communications networks. Roskomnadzor will be carrying out primary state policies in this area (for more on Runet, see Chap. 16).

6.5.2 Runet Law

Internet providers need to install in their network the technical means (black boxes) for countering threats to stability, security, and integrity of the internet in Russia (article 46(5.1)). Roskomnadzor will provide the black boxes. The same article directly relieves internet providers from the obligation to limit access to prohibited websites. This is now the function of the black boxes.

Roskomnadzor receives centralized control over the entire Runet in cases of discovering a threat to the functioning of the networks (article 65.1). The government of Russia is yet to define what types of threats qualify for empowering Roskomnadzor with centralized control (article 65.1(5)). According to the head of Roskomnadzor, even a mere ban of a website already constitutes such a threat (Suharevskaja 2019). Thus, for now, it is not clear what should be the scale of the threat to transfer centralized control to Roskomnadzor. The legislator, by changing the heading of the encompassing chapter of the law, signals that a non-exceptional threat could be sufficient. The name changed from "Managing communication networks in cases of emergency and the state of emergency" to "Managing communication networks in certain cases." Thus,

the state of emergency was downgraded to "certain cases." Roskomnadzor will have centralized control over Runet beyond emergency cases.

Once the black boxes are installed, the Russian government will be able to control domestic traffic and, if needed, turn off incoming foreign traffic.

6.6 A New Interpretation of Personal Data

In December 2018, Roskomnadzor presented its new vision of personal data by including cookies in the scope of the term. Cookies collect certain data about the users to, for example, tailor advertisements to the user's location and browsing activity. The use of cookies on a website in terms of data protection is a controversial issue at the moment. The Russian legislation does not define the term "cookies." The legal analysis of cookies stems from the definition of personal data in Russian law. As discussed earlier, to be considered personal data, user data needs to allow a natural person to be identified. Roskomnadzor representatives themselves, in a 2015 commentary to the Personal Data Law, stated that the data should not be considered personal data if it does not allow identifying a natural person without the use of additional information (Gafurova et al. 2015, 15). It took a political case for Roskomnadzor to change the opinion.

The use of cookies was one of the subject matters in the dispute involving the "Smart voting system" of Russian political activist Alexei Navalny (*Roskomnadzor v. Gandi SAS*). Navalny's goal was to prevent the domination of United Russia party candidates in the regional and municipal elections of 2019. The system was built with the idea of uniting pro-opposition votes in each voting district for a single candidate that has the highest chance of winning the election against United Russia's representative. Voters could register on the website and on the day of elections would receive a text message with the name of an opposition candidate that has the highest winning chance. The website, https://2019.vote/, was registered to Gandi SAS. Roskomnadzor claimed a violation of data protection legislation by the website and applied to a court. Among the violations, Roskomnadzor stated that by using the services of Google Analytics and Yandex Metrica the website collected and processed personal data of its users.

Google Analytics and Yandex Metrica collect the data of users. Such data can include the location of the user, the device used to access a website, browser, and internet protocol (IP) address. This data itself, without the use of additional information, does not allow identifying a natural person. Nevertheless, in the eyes of Roskomnadzor and the court, using cookies through the services of Google Analytics and Yandex Metrica constituted data collection and processing. Navalny appealed the decision but with no success. In this understanding, Roskomnadzor goes against its commentaries on the scope of personal data. At the same time, if compared to the way other countries apply data protection legislation with regard to cookies, the measure is appropriate. For example, the GDPR specifically states that cookies may allow identifying a natural person (Recital 30).

6.7 Conclusion

The law gives a vague definition of personal data. It allows Roskomnadzor to include in personal data new types of data without ever needing to amend legislation. The inclusion of cookies into the scope of personal data is one such example. This step, although following the understanding of personal data in the GDPR, differs from Roskomnadzor's former understanding of the term. The duty of data distributors to store users' data substantially eases monitoring of data for Russian enforcement authorities. This duty is not an invention of the Russian legislation. The 2006 EU Data Retention Directive introduced similar measures. The major difference from Russia was that the EU Directive required data operators to store the metadata (e.g., telephone numbers and IP addresses), not the data itself. Russian legislation, apart from that, creates convenient conditions for the enforcement authorities to obtain access to data. In 2014, the Court of Justice of the European Union invalidated the Directive for violating fundamental rights (*Digital Rights Ireland v. Minister for Communications*).

Fines for breaches of data protection legislation will be increased to provide Roskomnadzor with an additional instrument of pressure. Blocking websites can be an effective measure, but blocking giants like Google will be noticeably harmful to the Russian economy itself, as many Russian companies use Google cloud services. Trying to ban Twitter and Facebook might prove futile since Roskomnadzor was not able to block a much smaller messaging application, Telegram. Once the black boxes are fully implemented, Roskomnadzor will have much more capabilities in blocking services and websites with great precision. At the same time, the law "On the Sovereign Runet," despite being enacted, still needs substantial time before it can be properly implemented.

Among the expected novelties of Russian legislation is the introduction of the Big Data concept. Big Data allows re-identifying a person from a data set that seems to have no direct link, as well as extracting personal data that an individual did not provide, through the analysis of vast amounts of information (Gruschka et al. 2019, 5027). An example of such re-identification is the 2006 release by Netflix of a data set including a user ID and movie ratings connected to such ID. By itself, this data does not allow identifying a person. When combined with other information however, such as user movie ratings of the Internet Movie Database, the data allowed identifying a Netflix customer (Narayanan and Shmatikov 2008, 121–124). Currently, Big Data does not fall within the scope of personal data in Russia. At the same time, the definition of personal data in article 4 of the GDPR allows including Big Data in the scope of personal data (Bonatti and Kirrane 2019, 7).

The Russian legislator is very active in the sphere of data protection. Almost all novelties grant new powers to controlling authorities and increase the burden of compliance even for companies located outside of Russia if their activity is aimed at Russia. Roskomnadzor plays a central role in this sphere. Roskomnadzor does not need to comply with the rules and limitations for

conducting inspections that are obligatory for other public authorities. Instead, the Federal Service follows a set of rules especially established for its activities. In the nearest future, Roskomnadzor will strengthen its position by receiving the power to exercise centralized control over Runet. Legislative grounds for the state monitoring over the data flows grow alongside the technical capabilities of Russian government to exercise such control.

References

Bauer, Matthias, Lee-Makiyama Hosuk, Erik van der Marel, and Bert Verschelde. 2015. *Data Localisation in Russia: a Self-Imposed Sanction*. Brussels: European Centre for International Political Economy (ECIPE).

Bonatti, Piero A, and Sabrina Kirrane. 2019. Big Data and Analytics in the Age of the GDPR. In *2019 IEEE International Congress on Big Data (BigDataCongress)*, 7–16. https://doi.org/10.1109/BigDataCongress.2019.00015.

Bondarev, Denis, Dmitrij Nosonov, and Anna Balashova. 2016. Roskomnadzor načal blokirovku LinkedIn [Roskomnadzor Started Blocking LinkedIn]. *RBC*, November 17. https://www.rbc.ru/technology_and_media/17/11/2016/5829cb809a7947c578b9cfcd.

Gafurova, Alfija Nasibullovna, Elena Vladimirovna Dorotenko, and Jurij Evgenevich Kantemirov. 2015. *Federal'nyj zakon "O personal'nyh dannyh."* Antonina Arkadevna Priezževa, ed. Moscow: Redakciâ "Rossijskoj gazety."

Garrie, D., and Irene Byhovsky. 2017. Privacy and Data Protection in Russia. *Journal of Law Cyber Warfare* 5: 235–255. https://doi.org/10.1136/bmjopen-2019-EMS.28.

Gruschka, Nils, Vasileios Mavroeidis, Kamer Vishi, and Meiko Jensen. 2019. Privacy Issues and Data Protection in Big Data: a Case Study Analysis Under GDPR. In *2018 IEEE International Conference on Big Data (Big Data)*, 5027–5033. https://doi.org/10.1109/BigData.2018.8622621.

Kolomychenko, Marija. 2016. Operatoram vystavili sčët [Operators Were Issued an Invoice]. *Kommersant*, December 26.

———. 2019. FSB potrebovala klûči šifrovaniâ perepiski pol'zovatelej u 'Yandex' [FSB Requested Encryption Keys for Users' Messages from Yandex]. *RBC*, June 4. https://www.rbc.ru/technology_and_media/04/06/2019/5cf50e139a79474f8ab5494b.

Kuznecova, Evgenija, and Julija Vyrodova. 2019. Yandex podtverdil naličie rešeniâ po klûčam šifrovaniâ dlâ FSB [Yandex Confirmed the Existence of a Decision on the Encryptions Keys for FSB]. *RBC*, June 7. https://www.rbc.ru/society/07/06/2019/5cfa2a169a7947affada5b1a?from=from_main.

Mozur, Paul and Vindu Goel. 2014. To Reach China, LinkedIn Plays by Local Rules. *The New York Times*, October 5. https://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html.

Narayanan, Arvind, and Vitaly Shmatikov. 2008. Robust De-Anonymization of Large Sparse Datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, 111–125. IEEE. https://doi.org/10.1109/SP.2008.33.

Roskomnadzor. 2017. Podvedeny itogi realizacii federal'nogo zakona o lokalizacii baz personal'nyh dannyh rossijskih graždan na territorii Rossii [Summed Up the Results of Implementation of the Federal Law on Localization of Databases of Personal Data

of Russian Citizens on the Territory of Russia]. https://rkn.gov.ru/news/rsoc/news49466.htm.

———. 2018. Analitičeskij obzor meždunarodnogo opyta po lokalizacii baz dannyh, soderžaŝih personal'nye dannye graždan [Analytical Review of International Practices of Localising Databases Containing Personal Data of Citizens]. https://pd.rkn.gov.ru/docs/Obzor_po_lokalizacii.docx.

———. 2019a. Otvety na voprosy v sfere zaŝity prav sub'ektov personal'nyh dannyh [Answers for Questions in the Sphere of Protection of Personal Data Subjects' Rights]. https://rkn.gov.ru/treatments/p459/p468/.

———. 2019b. Reestr narušitelej prav sub'ektov personal'nyh dannyh [Registry of Infringers of the Rights of Data Subjects]. https://pd.rkn.gov.ru/registerOffenders/.

———. 2019c. Reestr organizatorov rasprostraneniâ informacii [Registry of Organizers of Data Distribution]. https://reestr.rublacklist.net/distributors_main/.

Savelyev, Alexander. 2016. Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction? *Computer Law & Security Review: the International Journal of Technology Law and Practice* 32 (1): 128–145. https://doi.org/10.1016/j.clsr.2015.12.003.

Suharevskaja, Alena. 2018. Ot blokirovki Telegram v Rossii postradali 400 internet-resursov [400 Internet Resources Suffered from Blocking the Telegram]. *Vedomosti*, May 7. https://www.vedomosti.ru/technology/articles/2018/05/07/768819-ot-popitok-zablokirovat-telegram-postradali-400.

———. 2019. Gosduma prinâla zakon o suverennom runete [State Duma Passed the Law on Sovereign Runet]. *Vedomosti*, April 16. https://www.vedomosti.ru/technology/articles/2019/04/16/799258-gosduma-zakon.

Tereshhenko, Ljudmila Konstantinovna. 2018. Gosudarstvennyj kontrol' v sfere zaŝity personal'nyh dannyh [State Control in the Sphere of Personal Data Protection]. *Pravo* 4: 141–161. https://doi.org/10.17323/2072-8166.2018.4.142.161.

Tishina, Julija. 2018. Zakon Yarovoi soberet dividendy [Yarovaya Law will collect dividends]. *Kommersant, October* 12: 2018.

Zharov, Aleksandr. 2014. Kontrol' za informacionnoj sredoj—èto absolûtno normal'no [Control Over the Infosphere is Normal]. https://82.rkn.gov.ru/news/news70654.htm.

Zhuravlev, Mikhail, and Tatiana Brazhnik. 2014. Problems for Internet Business and Users Caused by New Russian Legislation. *Information Law Journal* 5 (4): 25–32.

Legal Sources

Decree of the President of Russia N 1715. 2008. O nekotoryh voprosah gosudarstvennogo upravleniâ v sfere svâzi, informacionnyh tehnologij i massovyh kommunikacij [On Certain Questions of State Governance in the Sphere of Communication, Informational Technologies and Mass Communications], 3 December. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=125069213307289911155398059&cacheid=05820B83A55F59EE0E94998C14648BF4&mode=splus&base=LAW&n=129958&rnd=0.21288845240581#1p3rvlx5azg.

Decree of the President of Russia N 646. 2016. Ob utverždenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii [On Establishing the Doctrine of

Informational Security of Russian Federation], 5 December. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=3011D334331B32E8AC7532B1E6A41400&mode=splus&base=LAW&n=208191&rnd=C93498B21CA171595106BE62A5A5A7AF#2cicpk6ophu.

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kigital Landesregierung and Others. 2014. Court of Justice of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

Draft Federal law N 01/05/08-19/00093621. O vnesenii izmeneniâ v Federal'nyj zakon 'O personal'nyh dannyh' v časti utočneniâ trebovanij k uničtoženiû personal'nyh dannyh [On Amending the Federal Law 'On Personal Data' in Clarifying the Duty to Confirm the Termination of Personal Data] (Draft law On Termination of Personal Data). https://regulation.gov.ru/projects#npa=93621.

Draft Federal law N 729516-7. O vnesenii izmenenij v Kodeks Rossijskoj Federacii ob administrativnyh pravonarušeniâh [On Amending the Code of Administrative Offences of Russia]. https://sozd.duma.gov.ru/bill/729516-7.

Draft law N416052-6. O vnesenii izmenenij v Federal'nyj zakon 'O personal'nyh dannyh' i stat'û 28.3 Kodeksa Rossijskoj Federacii ob administrativnyh pravonarušeniâh [On Amending the Federal Law 'On Personal Data' and Article February 28 of the Code of Administrative Offences of Russia]. http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=416052-6.

EU Regulation N 2016/679. 2016. On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 27 April (GDPR).

European Parliament and Council Directive N 2006/24/EC. 2006. On the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 15 March (EU Data Retention Directive).

Federal Constitutional Law N 1-FKZ. 1994. O Konstitucionnom Sude Rossijskoj Federacii [On the Constitutional Court of Russian Federation], 21 July. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=59026883909335713102225273&cacheid=EBB9123F2F2DE437A09152E8759719BB&mode=splus&base=LAW&n=303524&rnd=75A319AFD029A32757FF30715DAF729C#1rcvv770we5.

Federal Law N 126-FZ. 2003. "O svâzi [On Communications], July 7. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=8145F3B2B11EC4A6313C8BB2FA35483B&mode=splus&base=LAW&n=323999&rnd=C93498B21CA171595106BE62A5A5A7AF#2joroiejcjy.

Federal Law N 242-FZ. 2014. O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii v časti utočneniâ porâdka obrabotki personal'nyh dannyh v informacionno-telekommunikacionnyh setâh [On Amending Certain Legislative Acts of the Russian Federation in Clarifying the Order for Processing Personal Data in the Informational-Telecommunications Networks], 21 July (Localization law). http://www.consultant.ru/document/cons_doc_LAW_165838/

Federal law N 294-FZ. 2008. O zaŝite prav ûridičeskih lic i individual'nyh predprinimatelej pri osuŝestvlenii gosudarstvennogo kontrolâ (nadzora) i municipal'nogo

kontrolâ [On Protection of Rights of Legal Entities and Individual Entrepreneurs Subject to State Control (Supervision) and Municipal Control], 26 December (Federal Law on the Protection of Businesses). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=CA7B5A15556F739CC816E000C5CB51A6&mode=splus&base=LAW&n=330806&rnd=C93498B21CA171595106BE62A5A5A7AF#2gxvycneh54.

Federal Law N 90-FZ. 2019. O vnesenii izmenenij v Federal'nyj zakon 'O svâzi' i Federal'nyj zakon 'Ob informacii, informacionnyh tehnologiâh i o zaŝite informacii' [On Amending the Federal Law 'On Communications' and Federal Law 'On Information, Information Technologies and Protection of Information'], May 1 (Sovereign Runet law). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=F80E7209AB399E0609FB56D046A80279&mode=splus&base=LAW&n=323815&rnd=C93498B21CA171595106BE62A5A5A7AF#1xj47cvtt2e.

Draft Federal law N 04/13/09-19/00095069. O vnesenii izmenenij v Federal'nyj zakon 'O personal'nyh dannyh' [On Amending the Federal Law 'on Personal Data'] (Draft Law on Single Consent Form). http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=187549#043229329098463776.

LLC Skartel v. Roskomnadzor Administration of the Central Federal Circuit. 2016. Commercial court of the city of Moscow. http://kad.arbitr.ru.

Order of the Federal Service for Supervision of Communications, Information Technologies and Mass Media N274. 2013. Ob utverždenii perečnâ inostrannyh gosudarstv, ne âvlâûŝihsâ storonami Konvencii Soveta Evropy o zaŝite fizičeskih lic pri avtomatizirovannoj obrabotke personal'nyh dannyh i obespečivaûŝih adekvatnuû zaŝitu prav sub'ektov personal'nyh dannyh [On Approving the List of Foreign States Non-Members of the Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data and Providing Adequate Protection of Rights of Personal Data Subjects], 15 March (Order of Roskomnadzor on the List of Countries with Adequate Personal Data Protection). http://base.garant.ru/70368490/53f89421bbdaf741eb2d1ecc4ddb4c33/#ixzz61mGs68jR.

Resolution of the Government of Russia N 146. 2019. Ob utverždenii Pravil organizacii i osuŝestvleniâ gosudarstvennogo kontrolâ i nadzora za obrabotkoj personal'nyh dannyh [On Adoption of the Rules of Organisation and Execution of State Control and Supervision Over Processing of Personal Data], 13 February (Roskomnadzor Inspection Rules). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=8567EB662DD7CB0DB503A0C9C925737B&mode=splus&base=LAW&n=318256&rnd=C93498B21CA171595106BE62A5A5A7AF#2axuel56aqm.

Resolution of the Government of Russia N 228. 2009. O Federal'noj službe po nadzoru v sfere svâzi, informacionnyh tehnologij i massovyh kommunikacij [On a Federal Service for Supervision of Communications, Information Technologies and Mass Media], 16 March (Resolution of the Government On Roskomnadzor). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=463319870561769819592886&cacheid=F5E2970579ED033F234F23220E4E794F&mode=splus&base=LAW&n=334166&rnd=C93498B21CA171595106BE62A5A5A7AF#94nspi112vc.

Resolution of the Government of Russia N 445. 2018. Ob utverždenii Pravil hraneniâ operatorami svâzi tekstovyh soobŝenij pol'zovatelej uslugami svâzi, golosovoj informacii, izobraženij, zvukov, video- i inyh soobŝenij pol'zovatelej uslugami svâzi [On

Adoption of the Rules of Storing by Communications Providers of Text Messages of Communications' Users, Voice Information, Images, Sounds, Video and Other Messages of the Users of Communication], 12 April (Resolution on Internet Traffic). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=502388752092438570703657 25&cacheid=EFC0F91BA6AC6AE25FAB42585CF0556F&mode=splus&base=LAW&n=325767&rnd=C93498B21CA171595106BE62A5A5A7AF#rljff75k49.

Roman Zakharov v. Russia. 2015. European Court of Human Rights. https://hudoc.echr.coe.int/eng#{"itemid":["001-159324"]}.

Roskomnadzor v. Gandi SAS. 2018. Taganskij district court of Moscow. https://www.mos-gorsud.ru/rs/taganskij/cases/docs/content/3a5e78f7-cb95-414d-985a-8ab2347bec9a.

———. 2019. City of Moscow court. https://www.mos-gorsud.ru/mgs/cases/docs/content/368d1a9a-0d98-43da-8b49-a1001f08c126.

Roskomnadzor v. LinkedIn Corporation. 2016. City of Moscow court. https://www.mos-gorsud.ru/mgs/cases/docs/content/c364d1d9-e30c-4ffa-aabb-327c8977adab.

Roskomnadzor v. Telegram Messenger Limited Liability Partnership. 2018. Taganskij district court of Moscow. https://mos-gorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa?caseFinalRangeDateFrom=13.04.2018&caseFinalRangeDateTo=13.04.2018&formType=fullForm.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.