

IRDG

Institut für das Recht
der digitalen Gesellschaft



UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES No. 22-13

DIGITAL CITADEL

Country Report on Russia

Elisabeth Saponchik

March 2022



Place of Publication

Institute for Law of the Digital Society, University of Passau

c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory

Innstraße 39, 94032 Passau

<https://www.jura.uni-passau.de/irdg/>

Author

Elisabeth Saponchik is a doctoral researcher at the University of Passau.

Abstract

This paper analyses current regulations in the field of information laws in Russia, whereas special attention is paid to provisions on data disclosure. The particular focus of the article is on the Federal Law on Information and Federal Law on Data Protection with its legally meaningful concept of data localisation, but also covers related recent legislation. The analysis shows that Russian information laws are very much centred at providing digital sovereignty and state control of Russian informational space. The article is supplemented by cultural and legal understanding of privacy in Russia.

Cite as

Saponchik, R. (2022). Digital Citadel – Country Report on Russia. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-12*. <https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/>.

Keywords

Russia, Privacy, Data Disclosure, Data Protection laws, Data localisation, Digital Sovereignty.

Contents

- A. Generalities* 1**
- I. Cultural Vectors of Data Disclosure 1**
 - II. Legal System and Lawmaking 3
- B. (General) Legal System of Information Law 4**
 - I. Structure of Information Law 4
 - II. Allocation of Informational Legal Positions 6
 - III. Institutions 7
 - IV. Procedural aspects 8
- C. Regulations Concerning Disclosure of Personal Data 9**
 - I. Legal Structure of Data Disclosure 9
 - II. Notions 11
 - 1. (Personal) Data as an Object of Protection 11
 - 2. Allocation of Data to a Person 11
 - 3. Reception and recipient 12
 - III. Relationship between Discloser and Recipient 13
 - 1. Provisions for Disclosure 13
 - a) Prohibited Disclosures 13
 - b) Disclosure Obligations 14
 - c) Voluntariness 14
 - 2. Recipient’s Obligations 15
 - a) Requirements for Personal Data Reception 15
 - b) (Procedural) Obligations Concerning Received Personal Data 15
 - 3. Control by Discloser 16
 - a) Transparency and Right to Request Information 16
 - b) Co-Determination and Co-Decision Concerning Data Use 16
 - c) Revocation 16
 - d) Procedural aspects 16
 - 4. Enforcement 17
 - a) Damages and Compensation 17
 - b) Procedural Aspects 17
 - IV. Objective Legal Obligations of the Recipient 17

1. Obligations Concerning Received Data	17
a) Dependence on Authorisation	17
b) Notification Obligations	17
c) Documentation	18
d) Processing Requirements	18
e) Prohibitions and Obligations	18
2. Monitoring	19
a) Recipient's Self-Monitoring	19
b) Regulated Self-Regulation	19
c) Supervisory Authorities	19
d) (Specific) Criminal Prosecution	20
e) Procedural Aspects	20
3. Enforcement	20
a) Interventions Concerning Data Processing	20
b) Interventions Concerning Business Models	21
c) Processor-related Sanctions	21
d) Sanctions for Individual Actors	21
e) Procedural Aspects	21
D. Sources and Literature	22
I. Related monographs	22
II. Related articles	22
III. Leading Cases	22
IV. Miscellaneous	22

A. Generalities*

I. Cultural Vectors of Data Disclosure

Identification of cultural [pre]conditions for individual data disclosure: cultural parameters that may the decision to disclose one's personal data; cultural practices and expectations regarding data disclosure [eg taboos]; data protection and privacy discourse, particularly articulated calls for reform); narratives and stories concerning data disclosure; synonyms for 'Data Protection' and 'Privacy' in the respective language.¹

With an extension of approximately 17 million square kilometres, Russia is one of the largest countries in the world. Russia lies partly in Eastern Europe and partly in Northern Asia. Russia's population is about 146 million, which makes Russia one of the 20 States with the largest population.

Russian language does not have a literal translation for the word '**Privatheit**'² or '**privacy**' in the sense of the physical sphere of an individual that belongs to him or her alone and is free from intrusion by third parties. In part, this is certainly due to the culture of living together in communal flats ('**kommunalka**') or in a house-commune ('**dom-kommuna**') during the Soviet era. The goal of the latter was the **collectivisation of private life**. In addition, there is also the Soviet ban on private property and its replacement by **personal property**³. Not least because of the elimination of the private during the Soviet era, people in Russian still refer to the 'personal life', 'personal thing' or 'personal space' (not to the

private one!).⁴ Despite the absence of the concept of privacy in the Russian language, the desire for it has always been strong. Historical experience points to curious linguistic creations: one example is the legal action of the resident of a communal flat who had to share a room with his ex-wife and for this reason asked for permission to install a shielding wall for 'domestic self-separation' ('**bytovoe samoograschdenije**').⁵ The personal thus lacked self-determination – an important element of privacy in the natural sense.

Another amusing example is provided by the Russian classic *M. Bulgakov's* story '**Heart of a dog**'. Representatives of the building management come to the flat of a professor of surgery with the demand to free part of his living space for workers. In response, the professor points to a legal document stating that his flat is officially exempt from 'densification' ('**uplotnenije**'). Since this does not help, he calls a high-ranking person and asks for a 'final' document so that neither the property management nor others are allowed to approach his door. Otherwise, he would leave it to the property management to carry out his operations. This example demonstrates that individual privacy could be **negotiable** if one possessed skills relevant to survival in any social order.

Today, Russian society is characterised by a culture of mistrust, which is certainly linked to the country's dramatic history. In addition,

*This report is part of an interdisciplinary research project on individual data disclosure: *Vectors of Data Disclosure – A comparative study on the disclosure of personal data from the perspectives of legal, cultural studies, and business information systems research*, supported by the Bavarian Research Institute for Digital Transformation (bidt). <<https://www.bidt.digital/en/vectors-data-disclosure/>>.

¹ These guideline texts are meant to facilitate an overview on the structure and content of all of the research project's country reports.

² German legal term.

³ Personal property rights in the Soviet Union were very limited and had a strict consumption character.

Personal property could not be used for profit-making. On this, see *Мантул, Собственность в Советском государстве, Философия права*, 2014, № 5 (66), стр.85/Grigorij Mantul, 'Property in the Soviet Union' [2014] 5(66), Philosophy of law 85 et seqq.

⁴ For example, Art 56 of one of the Soviet constitutions (1977) protects the fundamental right to **personal** life. In comparison, Article 23(1) of the current Russian Constitution (1993) protects the fundamental right to **private** life (or **privacy**).

⁵ Утехин, "Ничего личного", <arzamas.academy/courses/6/3> , дата последнего обращения 09.12.2021/Илья Utehin, 'Nothing personal', <arzamas.academy/courses/6/3> accessed 09 December 2021.

there is also ongoing political persecution by the State. Both mistrust towards fellow citizens and mistrust towards non-governmental organisations are characteristic. According to the Lewada Centre's 2020 survey, the following social institutions are trusted most: the army (66 %), the president (58 %), and the security services (53 %). All other institutions score rather poorly.⁶ At the same time, it is not possible to assume a high level of trust in the State as the Corona pandemic has shown: 54 % of Russian citizens are not willing to get vaccinated.⁷

One manifestation of the difficult establishment of private property and the culture of mistrust in Russia is **the problem of high fences**.⁸ Originally, Russian cities were built around a **fortress** (rather than a market) where the fence had an important function of internal and external **security**.⁹ If you travel to Russia from Europe today, the fencing of both private and urban spaces will be very noticeable.

Nowadays, the word **'privatnost'** is used more frequently in different contexts (from the IT sector to academic research). Privatnost already has a foreign origin from hearing it and

corresponds to the notion of privacy in German (or privacy in English).

Regarding data disclosure in Russia, there are already first survey results. The associations 'Big Data', WZIAM¹⁰, and Ipsos published a joint study in November 2021 according to which the majority of respondents are neutral towards data collection and think that it could be rather useful. The survey showed, among other things, that respondents are willing to disclose data if it improves service quality.¹¹ Overall, it can be said that technological development in Russia is very dynamic; nowadays, it is possible to buy tickets in the Moscow metro using a biometric payment system (Face Pay).

However, the willingness to disclose one's personal data is low in other contexts. For example, according to the recent Ipsos survey for the *World Economic Forum*, only 28 % of respondents in Russia are willing to disclose health data to the government. For disclosure to private companies, the willingness of respondents is much lower (25 %) although

⁶ *Левада-Центр*, Доверие институтам, <levada.ru/2020/09/21/doverie-institutam/>, дата последнего обращения 09.12.2021/Levada Centre, 'Survey on trust in social institutes' (*Levada Centre*, 21 September 2020) <levada.ru/2020/09/21/doverie-institutam/> accessed 09 December 2021.

⁷ *Левада-Центр*, Коронавирус, прививки и обязательная вакцинация, <levada.ru/2021/07/05/koronavirus-privivki-i-obyazatel'naya-vaktsinatsiya/>, дата последнего обращения 09.12.2021/Levada Centre, 'Surveys on coronavirus, vaccinations and compulsory vaccination' (*Levada Centre*, 05 July 2021) <levada.ru/2021/07/05/koronavirus-privivki-i-obyazatel'naya-vaktsinatsiya/> accessed 09 December 2021.

⁸ *Медведев*, "Феноменология забора", <hse.ru/video/120759974.html>, дата последнего обращения 07.12.2021/Sergei Medvedev, 'The Phenomenology of the Fence' <hse.ru/video/120759974.html> accessed 07 December 2021; Трудолюбков, Люди за забором: Частное пространство, власть и собственность в России

2015, New Publishing House/Maxim Trudolubov, *People Behind the Fence: Privacy, Power and Private Property in Russia* (New Publishing House, 2015).

⁹ Sergei Medvedev, 'The Phenomenology of the Fence' <hse.ru/video/120759974.html> accessed 07 December 2021. According to *Medvedev*, a weighty manifestation of Russian fence culture was the construction of the **Berlin Wall**, which not only separated the socialist and capitalist worlds, but rather had existential significance for Soviet regimes because the price of crossing behind the fence was one's life.

¹⁰ ВЦИОМ/WZIAM - All-Russian Centre of Public Opinion Research.

¹¹ Ассоциация больших данных, 'Россияне готовы делиться данными в обмен на лучший сервис' <rubda.ru/association_news/rossiyane-gotovy-delitsya-dannymi-v-obmen-na-luchshij-servis/>, дата последнего обращения 09.12.2021/Association 'Big Data', 'Russian citizens ready to give up data for better service quality' (*Association 'Big Data'*, 17 November 2021) <rubda.ru/association_news/rossiyane-gotovy-delitsya-dannymi-v-obmen-na-luchshij-servis/> accessed 09 December 2021.

67 % of respondents would disclose their health data to medical institutions.¹²

II. Legal System and Lawmaking

Central characteristics; sources of law and legal hierarchies; classification of legal systems; lawmakers and influential political and societal movements.

Characteristic of the Russian legal system are numerous historical upheavals that have influenced and sometimes disrupted the development of law in Russia. After the October Revolution in 1917, the pre-revolutionary legal system was largely abolished but some elements, in particular the police's position which was characterised by almost unlimited powers during the Russian monarchy, served as a foundation for the development of Soviet law.¹³ The role of law during the Soviet period is particularly evident in the fact that four constitutions were adopted between 1918 and 1978. Currently, the fifth constitution is in force which was adopted by referendum in 1993.

After the disintegration of the Soviet Union, economic reforms were carried out (known as **J Gaidar's** reforms or the '**government of the young reformers**') which at the same time led to the reform of the legal system. The result's result exceeded all possible expectations and brought freedom of the press, freedom of expression, political competition, and democratic elections into Russian life.¹⁴

¹² Ipsos, 'Global public backs COVID-19 vaccine passports for international travel' (Ipsos, 28 April 2021) <[ipsos.com/en/global-public-backs-covid-19-vaccine-passports-international-travel](https://www.ipsos.com/en/global-public-backs-covid-19-vaccine-passports-international-travel)> accessed 09 December 2021.

¹³ Мишина, Длинные тени советского прошлого 2014 Фонд "Либеральная миссия" стр. 18 /Ekaterina Mishina, *The Long Shadows of the Soviet Past* (The Liberal Mission Foundation, 2014) 18 et seqq.

¹⁴ *ibid* 54.

¹⁵ *ibid* 61; see also Краснов, Право: история и современность, 2017, №1, стр. (810)/Mikhail Krasnov, *Law: History and Modernity* (№1, 2017) 810.

¹⁶ This term refers to those federal laws that have already been provided for by constitutional norms. An example of this is Article 128(3) of the Constitution, according to which the powers and activities of the

Today, the communist social order does not exist any more, nor does the socialist legal system. The Russian legal system belongs to the Romano-Germanic legal system. The most important codifications took place between 1994 and 2006 when the Russian Civil Code, Criminal Code and procedural codes were adopted. A special feature of the Russian legal system is the **path dependence** when **applying the law** which is particularly evident in the judiciary.¹⁵

The sources of law are the Constitution, federal constitutional laws,¹⁶ federal laws, regional law, and sub-legal norms. In addition and according to Art 15(4) of the Russian Constitution, the Russian legal system includes generally recognised principles and norms of international law as well as international treaties adopted by Russia.¹⁷ In the event of a conflict between an international treaty and a domestic law, the rules of the international treaty apply.

In 2015, the Russian Constitutional Court took a turn regarding the relationship between international law and national law. According to the **Constitutional Court's ruling of 14 July 2015**, the European Court of Human Rights (ECtHR) judgements may not be followed if the ECtHR's interpretation of the European Convention on Human Rights (ECHR) contradicts the Russian Constitution.¹⁸ However, such a contradiction is rather

Constitutional Court, the Supreme Court of Russia and other federal courts are regulated by a federal constitutional law.

¹⁷ Art 15(4) of the Russian Constitution is applicable to all international treaties to which Russia has agreed. The Russian Constitution does not differentiate between ratified and non-ratified international treaties. According to Russian law, the State can consent to international treaties in various forms. For more information about different forms of consent the state can invoke see Art 6(1) of the Federal Law of 15 July 1995 № 101 'On International Treaties of the Russian Federation'/Федеральный закон от 15.07.1995 № 101 "О международных договорах Российской Федерации", <rg.ru/1995/07/21/mejdunarodnyedogovory-dok.html> accessed 09 December 2021.

¹⁸ The difficult relationship with the ECtHR is best understood through the speeches of the President of the

difficult to imagine as the ECHR and the Russian Constitution are based on the same principles. A special procedure has been established for the implementation of the Constitutional Court's ruling. Due to the aggression of the Russian Federation within the sovereign territory of Ukraine and therefore violations of the Statute of Council of Europe, the representation rights of Russia in the Council of Europe were suspended.¹⁹ This development was further followed by the exclusion of Russia from the Council of Europe.²⁰ Prior to the decision of the Council of Europe, Russia decided to leave the Council of Europe freely²¹ (presumably avoiding the kick-out initiated by CoE), which means another disruption of the legal system, comparable only to consequences of the October Revolution in 1917.

At the top of the **hierarchy of norms** is the Russian Constitution. It is followed by generally recognised principles and norms of international law and legally binding international treaties (see Art 15(4) of the Russian Constitution). This is followed by federal constitutional acts and federal laws. Sub-legislative acts and regional law follow thereafter.

At the federal level, the State Duma is responsible for **lawmaking**. Regional parliaments are responsible for legislation within the respective region (officially 'subject of the federation'). The traditional principle of federalism

applies according to which federal law overrides regional law. According to Art 104 (1) of the Russian Constitution, the legislative initiative belongs to the President, the Federation Council, the Senators of the Federation Council, the Deputies of the State Duma, regional legislative bodies, the Constitutional Court and the Supreme Court with regard to the issues that fall within their competencies. Another interesting peculiarity is attributable to the Russian Constitutional Court which has introduced **de facto amendments** to constitutional norms by way of its interpretative activity.²²

B. (General) Legal System of Information Law

I. Structure of Information Law

Constitutional and basic rights aspects; relevant regulations concerning intellectual property, secrecy, cybercrime [data privacy aut idem infra at C.]; Which regulations are based on international provisions [especially concerning intellectual property]?

The Russian Constitution does not contain an explicitly regulated fundamental right to data protection. Rather, such a right is derived from other fundamental rights, in particular from the fundamental right to a private life which is regulated in Article 23(1) of the Constitution. In addition, there is Article 24(1) of the Constitution, according to which the collection, storage, use, and dissemination of

Russian Constitutional Court: *Зорькин*, Диалог Конституционного Суда РФ и Европейского суда по правам человека в контексте конституционного правопорядка, <ksrf.ru/ru/news/speech/pages/ViewItem.aspx?ParamId=39>, дата последнего обращения 09.12.2021/Valery Zorkin, 'The Dialog of the ECtHR and Russian Constitutional Court in constitutional context' <ksrf.ru/ru/news/speech/pages/ViewItem.aspx?ParamId=39> accessed 09 December 2021; *Зорькин*, Россия и Страсбург, <rg.ru/2015/10/21/zorkin.html>, дата последнего обращения 09.12.2021/Valery Zorkin, 'Russia and Strasbourg' <rg.ru/2015/10/21/zorkin.html> accessed 09 December 2021.

¹⁹ Council of Europe, 'Council of Europe to discuss potential further measures against Russia', (CoE, 2022), <coe.int/en/web/portal/-/council-of-europe-to-discuss-further-measures-against-russia> accessed 15 March 2022.

to-discuss-further-measures-against-russia> accessed 15 March 2022.

²⁰ Council of Europe, 'The Russian Federation is excluded from the Council of Europe', (CoE, 2022), <coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe> accessed 03 April 2022.

²¹ Deutsche Welle, 'Russia formally departs Council of Europe', <dw.com/en/russia-formally-departs-council-of-europe/a-61136962> accessed 03 April 2022.

²² For an analysis of all 13 judgments of the Russian Constitutional Court on the interpretation of the Constitution: *Краснов*, Толкования как поправки, Сравнительное конституционное обозрение, 2014, №1 (110), стр. 77-91/Mikhail Krasnov, 'Interpretations as Amendments' [2014] 1(110) Comparative Constitutional Review 77, 77–91.

information about the private life²³ of individuals without their consent is prohibited. In the past, the Russian Constitutional Court has interpreted the concept of private life rather narrowly but this approach has currently changed and converged with the ECtHR's jurisprudence on Art 8 of the ECHR.²⁴ The Russian Constitutional Court defines private life as an aspect of human life that belongs only to the individual and is free from State or social control. Moreover, the Constitutional Court underlines that the fundamental right to private life includes an individual's possibility to control information about himself (and its dissemination).²⁵

The protection of privacy of correspondence, post, and telecommunications are regulated in Art 24(2) of the Constitution. Freedom of information rights are regulated in Art 29 of the Constitution.

The Federal Law **'On Information'**²⁶ (hereinafter Russian Law on Information) is the basic legal act of Russian information law. Current political and legislative activities in information law are centred around the concept of **digital sovereignty**.²⁷ All legal amendments implementing digital sovereignty are contained in the Russian Law on Information.

A distinction is made between **generally accessible information** as defined in Art 7 of the Russian Law on Information and **information with restricted access** as defined in Art 9 of the Russian Law on Information. Information with restricted access include personal data, commercial,²⁸ professional,²⁹ and state secrets.³⁰ Access to such information is regulated by specific federal laws.

For example, in Russia, the federal law **'On Personal Data Protection'**³¹ (hereinafter Russian Law on Personal Data) applies which

²³ Art 23(1) and Art 24(1) of the Constitution use the word **'private life'**, which in Russian, however, consists of two words, such as **'private life' ('chastnaya zhizhn')**. The adjective **'chastnyiy'** is different from **'private'** and means **'separate', 'particular'** in Russian, see *Ожегов, Толковый словарь русского языка*, <ozhegov.slovaronline.com/38452-CHASTNYIY>, дата последнего обращения 16.12.2021/*Ozhegov online dictionary* <ozhegov.slovaronline.com/38452-CHASTNYIY> accessed 16 December 2021. If you make a noun out of the word **'chastnyiy'**, you get **'chastnost'**, which is a completely different word than **'privacy'**, as the meaning goes strongly in the direction of **'particularity'**, see on this *Ожегов, Толковый словарь русского языка*, <ozhegov.slovaronline.com/38451-CHASTNOST>, дата последнего обращения 16.12.2021/*Ozhegov online dictionary* <ozhegov.slovaronline.com/38451-CHASTNOST> accessed 16 December 2021.

²⁴ Проскурякова, Конституционно-правовые рамки защиты персональных данных в России, Вестник СПбГУ, 2016, № 14 (2), стр. 12 (15)/ Proskuryakova, 'Constitutional Framework of Data Protection in Russia' [2016] 14(2) Journal of Saint Petersburg University 12, 15.

²⁵ Определение Конституционного суда РФ от 09.06.2005, №-248-О/Decision of the Russian Constitutional Court, 09 June 2005, №-248-О.

²⁶ Федеральный закон от 14.07.2006 № 149 "Об информации"/Federal Law of 14 July 2006 № 149

'On Information' <rg.ru/2006/07/29/informaciadok.html> accessed 09 December 2021.

²⁷ см. п. 34(а) Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы/See e.g. point 34(a) of the Russian Information Development Strategy for 2017-2030 <kremlin.ru/acts/bank/41919> accessed 09 December 2021.

²⁸ Федеральный закон от 29.07.2004 №98 "О коммерческой тайне"/Federal Law of 29 July 2004 №98 'On Commercial Secrecy' <rg.ru/2004/08/05/taina-doc.html> accessed 09 December 2021.

²⁹ ст. 7 Федерального закона от 03.04.1995 "О Федеральной службе безопасности"/Art 7 of the Federal Law of 03 April 1995 № 40 'On State Security Service' <pravo.gov.ru/proxy/ips/?docbody=&nd=102034880&rdk=&intelsearch=> accessed 09 December 2021.

³⁰ Федеральный закон от 21.07.1993 №5485-1 "О государственной тайне"/Federal Law of 21 July 1993 №5485-1 'On State Secrecy' <pravo.gov.ru/proxy/ips/?docbody=&prev-Doc=102478068&backlink=1&nd=102025035> accessed 09 December 2021.

³¹ Федеральный закон от 14.07.2006 № 152 "О персональных данных"/Federal Law of 14 July 2006 № 152 'On personal data' <rg.ru/2006/07/29/personalnye-dannye-dok.html> accessed 09 December 2021.

is similar to the European Directive 95/46/EC ('Brussels effect').

The last significant development in Russian information law is the enactment of the law **'On the Activity of Foreign Persons in the Internet on the Territory of the Russian Federation'** (or ironically among lawyers law 'On Landing')³². At present, this law is only partially in force. It aims to ensure a level playing field for Russian and foreign companies.³³

According to the *World Intellectual Property Organization*, Russia is party to 79 international treaties in the field of intellectual property law.³⁴ Of particular importance for intellectual property law in Russia is the **Berne Convention for the Protection of Literary and Artistic Works**. In addition, there is also the **Universal Copyright Convention**. Intellectual property law is comprehensively regulated in Part V of the Russian Civil Code. In terms of regulation, the Russian Civil Code is a progressive and popular piece of legislation among Russian lawyers. However, individual intellectual property rights are not popular socially as they are often violated, especially in the internet. In June 2013, it was such a catastrophic situation with illegal film downloads that the State Duma passed an amendment legislation. One of the many amendments concerned the Russian Law on Information. Nowadays, the new Art 15.2 of the Russian Law on Information allows the blocking of websites that offer illegal media content for download. This problem affects not only films and music but also, for example, scientific works that can be acquired without the author's consent. The lack of appreciation of

intellectual property rights can probably also be seen as a manifestation of the path dependence from the Soviet era.

The amendment act on the Protection of Intellectual Property Rights also had a harmful spill-over effect. The practice of blocking has been extended to other areas of law where it significantly restricts the fundamental right to freedom of expression. Subjectively, this is a much bigger problem for Russian society than illegal downloading of music and films when at some point neither legal nor illegal media content may be distributed.

Chapter 28 of the Russian Criminal Code is completely dedicated to **cybercrimes**. Art 272 of the Criminal Code regulates, for example, the offence of unauthorised access to computer data.

II. Allocation of Informational Legal Positions

Commodity/commoditization, especially 'intellectual property'; collective goods; public goods.

According to Art 5 of the Russian Law on Information, information can become the subject of public law, civil law and other legal relationships. This makes information a universal legal object.³⁵ In the context of civil law, information becomes an **economic good** that can be used for profit unless Art 150 of the Civil Code is invoked.³⁶ Such exceptions include the protection of private life or secrecy which cannot be alienated.

At the same time, Art 128 of the Civil Code which governs objects of civil law does not

³² In Russian: "Закон о приземлении".

³³ Федеральный закон от 01.07.2021 № 236 "О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации"/Federal Law of 01 July 2021 № 236 'On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation' <rg.ru/2021/07/05/inet.html> accessed 10 December 2021.

³⁴ World Intellectual Property Organization, 'WIPO Lex – Russian Federation' (Wipolex, 2019) <wipolex.wipo.int/en/treaties/members/profile/RU> accessed 09 December 2021.

³⁵ Савельев, Комментарий к Федеральному закону от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и защите информации", 2015, Статут, ст. 5, стр. 31./ Alexander Savelyev, 'Art 5' in *Commentary on the Russian Law on Information* (Statut, 2015) 31.

³⁶ *ibid.*

apply to information or data.³⁷ Only Art 1225(1)(3) of the Civil Code classifies **databases** as intangible property. Art 1260(2) and Art 1333 et seqq of the Civil Code distinguish between two copyright protection regimes – one for the author of a database and for the creator (a person who organised the collection, processing, etc of the data). For example, the creator may make a database generally accessible (see Art 1333(2) of the Civil Code).

According to Art 2 of the Russian Law on Personal Data, the act regulates the guarantee of the fundamental right to privacy, personal, and family secrets when processing personal data. Reference has already been made to the basic legal distinction between generally accessible information and information with restricted access.

III. Institutions

Information supervisory authorities; private institutions/organisations [industry and sectoral associations], including international ones; public administration and cultivation/management of informational goods.

Roskomnadzor executes the function of the media and information supervisory authority. Roskomnadzor's powers are comprehensively regulated in the relevant regulations.³⁸ It is part of and subordinate to the Federal Ministry for Digital Development so that it does not correspond to the concept of an independent

data protection supervisory authority within the meaning of Art 51 of the GDPR. The lack of independence of Roskomnadzor is one of the factors why Russia is not considered as a third country with an adequate level of data protection pursuant to Art 45 GDPR.³⁹ In Russia's regions, Roskomnadzor has territorial representations.⁴⁰ Also, Roskomnadzor is mentioned in the context of the blocking of internet services. The legal basis for this can be found in Art 15.1-1 et seqq of the Russian Law on Information. Special attention should be paid to Art 15.5 of the Russian Law on Information which provides for restrictions for activities of internet services if they violate Russian data protection regulations. Roskomnadzor keeps a special register where such internet services are listed. Blocking is carried out at Roskomnadzor's request by hosting providers or telecommunications service providers. However, a prerequisite for blocking is a legally binding court decision. In this context, the blocking of **LinkedIn** should be noted which has not fulfilled the data localisation obligation according to Art 18(5) of the Russian Law on Personal Data.⁴¹

Rospatent is responsible for the protection of intellectual property rights. Likewise, Rospatent is not an independent body but part of the Federal Ministry of Economy. Rospatent's powers are regulated in a relevant regulation.⁴² According to point 5.8. of the

³⁷ Reference to legal amendment of 2019: **digital rights** were regulated as objects of civil law legal relationships within the meaning of Art 128 of the Civil Code.

³⁸ Постановление Правительства РФ от 16 марта 2009 г. N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"/Decree of the Government of the Russian Federation of 16 March 2009 № 228 'On Federal Service for Telecommunications, Information and Media Supervision', <digital.gov.ru/ru/documents/3226/> accessed 09 December 2021.

³⁹ See Oleg Blinov, 'Encrypt your data to make GDPR and Russian Data Localization Law compatible' <iapp.org/news/a/encrypt-your-data-in-order-to-make-gdpr-and-russian-data-localization-law-compatible/> accessed 04 August 2021.

⁴⁰ For the list of territorial representations of Roskomnadzor: <rkn.gov.ru/about/territorial/> accessed 09 December 2021.

⁴¹ Определение Московского городского суда от 10.11.2016 по делу 33-38783/2016/Moscow City Court, Judg. of 10 November 2016 - the case 33-38783/2016; to access the judgment see <mos-gor-sud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a> accessed 30 May 2021.

⁴² Постановление Правительства РФ от 21 марта 2012 г. № 218 "О Федеральной службе по интеллектуальной собственности"/Decree of the Government of the Russian Federation of 21 March 2012 № 218 'On Rospatent' <rospatent.gov.ru/ru/documents/218-postanovlenie-pravitelstva-rf-ot-21-marta-2012-g-218> accessed 09 December 2021.

Regulation Rospatent is responsible for the registration and sale of copyrights on works, databases, trademarks, etc. As mentioned above, Art 15.2 of the Russian Law on Information allows the blocking of websites that disseminate information and thereby violate copyrights. However, Roskomnadzor is responsible for the procedure.

At the international level, Russia is a member of the **OECD**, **WTO** and **WIPO**.

At the local level, there are NGOs like **Roskomsvoboda**⁴³ that fight for freedom of information and support unlawfully blocked internet services. Significant projects were the **Freedom of Information Foundation** and especially **'Komanda 29'**. The latter project consisted mainly of lawyers who worked cases related to Art 29 of the Russian Constitution (freedom of information, freedom of the press, ban on censorship) and won many of them prominently in Russia's highest courts. The activity of **'Komanda 29'** has been equated with the activity of the international non-governmental organisation **Společnost Svobody Informace** which has the status of an **'undesirable organisation'** in Russia.⁴⁴

⁴³ Website: <roskomsvoboda.org> accessed 09 December 2021.

⁴⁴ Undesirable organisation means foreign and international non-governmental organisations that endanger constitutional order, defence capability and security of the Russian state. См. ст. 3.1. Федерального закона от 28.12.2012 г. № 272 "О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации"/See more in Art 3.1. of the Federal Law of 26 December 2012 № 272 'On Intervention Measures in Connection with Human Rights Violations' <rg.ru/2012/12/29/zakondok.html> accessed 09 December 2021.

⁴⁵ Read more in German: Legal Tribune Online, 'Russische Anwaltsorganisation beendet Arbeit' (*Legal Tribune Online*, 19 July 2021) <https://www.lto.de/recht/nachrichten/n/komanda-29-russland-anwaltsorganisation-nawalny-buergerrechte-hochverrat-spionage/> accessed 09 December 2021.

⁴⁶ *Интерфакс*, РКН подтвердил блокировку сайта "Команды 29" из-за нежелательной НПО, <interfax.ru/russia/778315>, дата последнего обращения 09.12.2021/ *Interfax* 'Roskomnadzor confirms

'Komanda 29' has been dissolved in 2021.⁴⁵ Earlier archives of its advocacy activities were blocked by Roskomnadzor.⁴⁶

IV. Procedural aspects

Control and enforcement; individual; collective; through associations; by authorities [executive and judicial].

Russian data protection law provides in Art 17(1) of the Russian Law on Personal Data for an **administrative** and **judicial** remedy to bring an action against the activity or inactivity of the controller. Pursuant to Art 17(2) of the Russian Law on Personal Data, the data subject may claim **damages** (including non-material damages) (however, this is only possible in court proceedings). Roskomnadzor and its federal representations are responsible for an affected person's administrative legal action.⁴⁷ The respective procedure is regulated by federal law.⁴⁸

The judicial remedy is the least attractive. Commentaries point out that Roskomnadzor has much more legal leverage over responsible parties than courts.⁴⁹ Moreover, damages require pecuniary loss which is difficult to prove

blocking of "Komanda 29" (*Interfax*, 16 July 2021) <interfax.ru/russia/778315> accessed 09 December 2021.

⁴⁷ см. п. 5.11 Постановления Правительства РФ от 16.03.2009 № 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"/see point 5.11. of the Decree of the Government of the Russian Federation of 16 March 2009 № 228 'On Federal Service for Telecommunications, Information and Media Supervision' <rg.ru/2009/03/24/polozheniedok.html> accessed 09 December 2021.

⁴⁸ Федеральный закон от 02.05.2006 № 59 "О порядке рассмотрения обращений граждан Российской Федерации"/Federal Law of 26 April 2006 № 59 'On Civil Requests' <pravo.gov.ru/proxy/ips/? docbody=&nd=102106413> accessed 09 December 2021.

⁴⁹ *Савельев*, Научно-практический постатейный комментарий к Федеральному закону "О персональных данных", 2015, Статут, ст. 17, стр. 122/Alexander Savelyev, 'Art 17' in *Commentary on the Russian Data Protection Act* (Statut, 2015) 122.

in the cases of data protection rights' violations.⁵⁰ Furthermore, an action through the Human Rights Commissioner would be conceivable if the claimant disagrees with the outcome of the administrative or judicial proceedings.⁵¹ There is no federal data protection commissioner in Russia.

Copyright on databases means that it can be protected under Art 12 of the Civil Code. This provision enshrines the ways legal protection under civil law. However, not all legal protection channels are useful in the context of databases.

C. Regulations Concerning Disclosure of Personal Data

I. Legal Structure of Data Disclosure

Existence of 'Data Protection Law'; mandatory and nonmandatory regulation; differentiation between public and private sector; public or private sector as a role model for regulation; general or sectoral regulation; self-regulation [codes of conduct]; basic principles of regulation [preventive ban or freedom of processing]; risk-based approach [potential for misuse; protection of certain categories of data]; privileged areas [personal and family sphere; media; research].

There were already first signs of privacy protection in the Russian Empire. For example, the **Postal Regulations (1857)** and **Telegraph Regulations (1876)** guaranteed the right to privacy of correspondence, but this

was lost after the revolution.⁵² This development is not surprising since **after the revolution** people came to power who had had no (fundamental) rights for decades and who did not see themselves as holders of fundamental rights either. This logically led to the first Soviet Constitution (1918) guaranteeing a minimum of fundamental rights. In this constitution neither the fundamental right to private life nor the fundamental right to a personal sphere was regulated although this changed later (see the beginning of this country report).

The Russian Law on Personal Data has been in force in Russia since 2006. According to Art 1(1) of the Russian Law on Personal Data, it applies to both the public⁵³ and private sectors. It regulates both automated and non-automated data processing. The Russian Data Protection Act essentially corresponds to Directive 95/46/EC which is no longer in force. The private-family sphere, archives, and State secrets are excluded from its material scope of application. In addition, access to information on judicial activities containing personal data is regulated by a separate law.⁵⁴ In the event of a conflict between the Russian Law on Personal Data and an international treaty, the provisions of the latter apply.⁵⁵

The territorial scope of the Russian Law on Personal Data is determined by the **principle of effectiveness**. However, the principle of

⁵⁰ *ibid* 125.

⁵¹ ст. 16 п. 1 Федерального конституционного закона от 26.02.1997 №1 "Об Уполномоченном по правам человека в Российской Федерации"/see Art 16(1) of the Federal Constitutional Law of 26 February 1997 №1 'On the Human Rights Commissioner in Russia' <docs.cntd.ru/document/9038713> accessed 10 December 2021.

⁵² *Важорова, История возникновения и становления института персональных данных, Государство и право: теория и практика*, 2011, стр. 33 (34)/Mariya Wazhorowa, *The History of Data Protection in Russia, State and Law: Theory and Practice* (2011) 33 (34).

⁵³ However, according to Art 13 para. 1-2 of the Russian FDSG, state and municipal bodies have somewhat more regulatory freedom when processing personal data in their information systems (such as 'Gosuslugi.ru'), but this is limited to the handling of

the information system. In principle, the russFDSG applies.

⁵⁴ Федеральный закон от 22.12.2008 № 262 "Об обеспечении доступа к информации о деятельности судов в Российской Федерации"/Federal Law of 22 December 2008 № 262 'On Access to Information on Judicial Activity' <rg.ru/2008/12/26/sud-internet-dok.html> accessed 10 December 2021.

⁵⁵ See Art 4(4) of the Russian Federal Data Protection Act; worth of noting is also the landmark decision v. 15 July 2017 № 14-П of the Constitutional Court of Russia, according to which the Court created a mechanism for rejection of judgments of ECtHR when the interpretation of ECHR contradicts the Constitution of Russia, for detailed analysis see Lauri Mälksoo, 'Russia's Constitutional Court Defies the European Court of Human Rights' (2016) 12(2) *European Constitutional Law Review* 377, 377-395.

effectiveness is not regulated in the Russian Law on Personal Data. Its actual application is determined by the practice of legal application and the Ministry of Digital Development's declarations. The declarations are not legal acts and only have a recommendatory character. It should be noted that the Ministry of Digital Development's declarations are of considerable importance for the legal application practice by Roskomnadzor (which is part of the Ministry!). In the sense of a justification for the application of the principle of effectiveness, the declarations refer to European conflict of laws and Art 3(2) GDPR.⁵⁶ Such references to comparable regulations in European countries is a common practice of Russian State bodies.

Russian data protection law is designed as a **prohibition with the option of permission**. A possible permission is regulated in Art 6 of the Russian Data Protection Act. Traditional processing principles also apply, such as the **purpose limitation principle, legitimacy principle, data minimisation, accuracy**, and others.

In addition, the Russian FDSG regulates **data subjects' rights** (right to deletion, correction, right to information).

The Russian Law on Personal Data does not list a catalogue of risks. Nevertheless, there are signs of a risk-based approach. Art 19 of the Russian Law on Personal Data obliges the data controller to comply with **organisational and technical measures**. However, only the risk

of unauthorised or accidental access to the data is mentioned.

In connection with unauthorised access the obligation to **localise data** must be mentioned. The data localisation obligation came into force in 2015 and has proven to be a problem for domestic and foreign controllers. Many IT companies have already set up their servers for Russian' citizens data in Russia. Google, Twitter, and Facebook have not yet done so. For this, Google LLC was fined three million roubles (approx. 35,000 euros) based on Art 13.11(8) of the Code of Administrative Offences.⁵⁷

The highest sanction for violating the data localisation obligation is blocking. Neither Google, Twitter, nor Facebook have been blocked in Russia so far. Remarkably, Netflix, which also operates in Russia, was 'exempted' from the data localisation obligation by Roskomnadzor.⁵⁸ Netflix is not very popular in Russia, as there are country-owned streaming services. Also, the intellectual property law's state should not be forgotten which makes a lot of media content available on the Russian internet. Obviously, the data localisation obligation may be a matter of **negotiation** in individual cases. Ultimately, the aim is not to drive foreign companies out of the Russian market but to motivate them to comply with Russian laws.

⁵⁶ Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Обработка и хранение персональных данных в РФ/Ministry of Digital Development and Mass Communications on Processing and Storage of Personal Data in Russia <digital.gov.ru/ru/personaldata/> accessed 10 December 2021.

⁵⁷ Meduza, Российский суд впервые оштрафовал Google за отказ локализовать данные россиян, <meduza.io/news/2021/07/29/rossiyskiy-sud-vpervye-oshtrafoval-google-za-otkaz-lokalizovat-dannye-rossiyan?fbclid=IwAR2ryPm6QPaX-UaV1Y3C5-qjllqP2szfyg6rDC1asm8li43WmH-0qs_inuJI>, дата последнего обращения 10.12.2021./Meduza, 'Russian court punishes Google

for data localisation breach' (Meduza, 29 July 2021) <meduza.io/news/2021/07/29/rossiyskiy-sud-vpervye-oshtrafoval-google-za-otkaz-lokalizovat-dannye-rossiyan?fbclid=IwAR2ryPm6QPaX-UaV1Y3C5-qjllqP2szfyg6rDC1asm8li43WmH-0qs_inuJI> accessed 10 December 2021.

⁵⁸ Роскомнадзор, RNS: Глава Роскомнадзора: вопросов к Netflix нет, 08.12.2016, <rkn.gov.ru/press/publications/news41975.htm>, дата последнего обращения 10.12.2021/Roskomnadzor, Official Statement on Netflix of 08 December 2016 (Roskomnadzor, 8 December 2016) <rkn.gov.ru/press/publications/news41975.htm> accessed 10 December 2021.

II. Notions

1. (Personal) Data as an Object of Protection

Situational [spoken words etc.]; local/spatial [at home]; logical [‘spheres’]; informational [datum, information]; treatment of public or publicized data; limitations and expansions of notions; categories.

Personal data within the meaning of Art 3(1) of the Russian Law on Personal Data is any information relating **directly** or **indirectly** to an **identified** or **identifiable** person. This definition is similar to Art 2(a) of Directive 95/46/EC. Personal data can be in textual, graphic, or spoken form.⁵⁹ It is irrelevant whether the data is collected by a person or by a device.⁶⁰

A legal innovation is the category of personal data released by the data subject for **further dissemination**. For consent to the processing of such data, higher data protection requirements apply.⁶¹ Onward dissemination is understood as the disclosure of data to an undefined group of persons.

Special rules also apply to the processing of special categories of data revealing **racial** and **ethnic** origin, **political**, **religious** and **philosophical** beliefs, health status and data concerning sex life. Separately, **biometric data** are regulated.⁶² The distinction between **meta-data** and **content data** is only provided for in the Russian Law on Information.

2. Allocation of Data to a Person

Creation; possession/control; personal connection; differentiation between domestic and foreign nationals;

⁵⁹ Савельев, Научно-практический постатейный комментарий к Федеральному закону “О персональных данных”, 2015, Статут, абз. 1 ст. 3, стр. 25/Alexander Savelyev, ‘Art 3 para. 1’ in *Commentary on the Russian Data Protection Act* (Statut, 2015) 25.

⁶⁰ Савельев, Научно-практический постатейный комментарий к Федеральному закону “О персональных данных”, 2015, Статут, абз. 1 ст. 3, стр. 25/ibid 25.

⁶¹ See Art 10.1.(6) of the russFDSG.

⁶² See Art 11 of the Russian Federal Data Protection Act.

treatment of multi-referential data; limitations and expansions of notions; categories.

According to Russian data protection law, data is assigned to a person by means of a **personal reference**. A person is indirectly identifiable if his or her identification is possible by reference to other data.

In principle, data protection law makes no distinction between nationals and foreigners. However, Art 18(5) of the Russian Data Protection Act provides for an exception. Only the data of Russian citizens are subject to data localisation. This means that the data of foreign citizens are excluded. The Russian Law on Personal Data does not regulate how the data subjects’ citizenship is to be determined. The Digital Ministry’s explanations indicate that if it is impossible to determine citizenship data localisation may be applied to all data without distinction.⁶³

The handling of **double-referenced data** is not regulated in data protection law. However, there are occasional provisions that regulate the domestic reference of the data for storage and release.⁶⁴ If a ‘genuine link’ to Russia can be established via this data, Russian law is applied to the storage and release of the data.

The data of deceased persons are still considered personal data. The processing of such data requires consent which can be given by the heirs, unless the data subject already consented to the processing of his or her data when he or she still lived.

If copyright in a database has been recognised under an international treaty of the Russian

⁶³ Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Обработка и хранение персональных данных в РФ/Ministry of Digital Development and Mass Communications on Processing and Storage of Personal Data in Russia <digital.gov.ru/ru/personaldata/> accessed on 13 December 2021.

⁶⁴ п. 13 Постановления Правительства Российской Федерации от 23.09.2020 № 1526 “О хранении данных”/P. 13 of the Decree of the Government of the Russian Federation of 23 September 2020 №1526 ‘On Data Retention’ <base.garant.ru/74691852/> accessed 13 December 2021.

Federation, the exercise of that copyright is governed by the rules of the Russian Civil Code irrespective of the law of the country from where the copyright originates. However, if the international treaty regulates the exercise of copyright differently from the Civil Code, the international treaty is applicable.

3. Reception and recipient

Special regulation for non-profit/non-commercial actors; the public as a [legal] recipient; use of public data; specialised/special obligations for small and medium-sized enterprises (SMEs); differentiation between recipients and third parties [especially within company groups]; differentiation between national and international actions; outsourcing options.

The term ‘recipient’ is not found in the provisions of the Russian Law on Personal Data. Instead, Art 3(2) of the Russian Law on Personal Data contains the term ‘data controller’. State and municipal bodies, legal entities, or natural persons who alone or jointly process personal data and decide on the **purposes and means** of such data processing are considered data **controllers**.

Another important term in Russian information law is **information distributor**. The legal definition of information distributor is broadly formulated.⁶⁵ The Regulation on Data Retention restricts this term to **Internet communication services**.⁶⁶ This means that information distributors can also be regarded as data controllers within the meaning of Art 3(2) of the Russian Data Protection Act. The information distributors have a number of important obligations.

⁶⁵ *Information distributor* - any person operating information systems and (or) computers intended for receiving, sending, delivering processing of electronic messages (cf. Art 10.1. para. 1 of the Russian Law on Information).

⁶⁶ п. 2 Постановления Правительства Российской Федерации от 23.09.2020 № 1526 “О хранении данных”/P. 2 of the Decree of the Government of the Russian Federation of 23 September 2020 №1526 ‘On Data Retention’ <base.garant.ru/74691852/> accessed 13 December 2021.

The public is not a recipient in the legal sense. At this point, however, norms come into play that regulate how the person responsible deals with **publicly accessible sources** (eg address books) that contain personal data. According to Art 8(1) of the Russian Federal Data Protection Act, a concerned person’s written consent is required for the entry of personal data in a publicly accessible source. The data subject alone decides on specific data that is published in such a publicly accessible source.

The handling of personal data from publicly accessible sources has been significantly restricted by the requirement of a separate consent for the further dissemination of the data.⁶⁷ A special case of this is probably Art 152.2. of the Civil Code. This norm explicitly allows the processing of data (including further dissemination) from a publicly accessible source in a civil law context.

Art 12 of the Russian Federal Data Protection Act regulates **cross-border data transfers**. The concept of an adequate level of data protection is used for this purpose. According to Art 12(1) of the Russian Law on Personal Data, countries that have ratified the **Convention for the Protection of Individuals with regard to Automated Processing of Personal Data** (hereinafter Agreement 108) have an adequate level of data protection. These include the Council of Europe’s member States.

Transfers outside of Agreement 108 are also possible. The prerequisite for this is that Roskomnadzor acknowledges that the State in question has an adequate level of data protection. Such States can be found in a decision.⁶⁸

⁶⁷ Art 10.1. of the russFDSG.

⁶⁸ Приказ Роскомнадзора от 14.09.2021 №183 “Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных”/Roskomnadzor Decision of 14 September 2021 № 183 ‘On the States ensuring an adequate level of data protection which are not parties to the Convention for the Protection of Individuals with regard to Automated

At present, this includes **Canada, Malaysia, Japan, Singapore, Korea, Tunisia, and South Africa.**

Art 6(3) of the Russian Federal Data Protection Act provides for the possibility of **commissioned processing**. The prerequisite for this is the consent of the data subject. This is different from Art 28 of the GDPR. Apart from that, Art 6(3) of the Russian Law on Personal Data and Art 28 of the GDPR follow a similar logic. Another special feature is that processors are not subject to the data localisation obligation as defined in Art 18(5) of the Russian Law on Personal Data. Legal practice also demonstrates that the application of the data localisation obligation to cloud services tends to fail.

III. Relationship between Discloser and Recipient

1. Provisions for Disclosure

Does regulation exist? personal data as intellectual property and commercial good; data law as a framework for action; ‘informational self-determination’

The requirements for disclosing data are not regulated in the Russian Law on Personal Data. The disclosure of data is based on the permissive elements of Art 6 of the Russian Law on Personal Data, on which also the processing of data can be based. The permissive elements are very similar to those in Art 6 of the GDPR. The data subject’s consent is of particular legal significance as it demonstrates the individual’s decision.

The data are no intangible property (unlike databases) or economic goods. However, Art 783.1. of the Civil Code provides for a contract on the provision of information. At the same time, Art 152.2. of the Civil Code protects the individual from unauthorised disclosure of information about his/her private

life that became known to a party as a result of the conclusion or execution of a contract.

Data law as a field of law does not yet exist in Russia. However, it is currently being developed. The German concept of ‘informational self-determination’ is known to Russian jurisprudence but it has not been adopted.

a) Prohibited Disclosures

Protections of secrecy; multi-referentiality; disclosure to actors abroad; public communications.

In principle, individuals are free to decide whether to disclose their data. Limits arise from the category of information with restricted access. According to Art 9(4) of the Russian Law on Information, this includes the **protection of secrets** (regulated in individual federal laws) and **confidential information**. Art 7 of the Russian Federal Data Protection Act states that personal data is classified as confidential information. The provision prohibits data controllers and other persons from disclosing the data to third parties. Furthermore, the further dissemination of data without data subject’s consent is prohibited.

Admittedly, the **data localisation obligation** of Art 18(5) of the Russian Law on Personal Data constitutes a prohibition of disclosure, because it restricts the data flows within a data controller. Data localisation obliges the controller to set up a server with personal data in Russia. The cross-border transfer of data from Russia to the foreign database of the same company would violate Art 12 in conjunction with Art 18(5) of the Russian Law on Personal Data because the data is not transferred to another person within the meaning of Art 12 of the Russian Law on Personal Data, but to oneself.⁶⁹ The consent of the data subject is not an exception for the application of data localisation. The correctness of this view is confirmed by *Zharov* (the former head of Roskomnadzor)

Processing of Personal Data’ <docs.cntd.ru/document/608935178?marker> accessed 09 February 2022.

⁶⁹ *Савельев*, Комментарий к Федеральному закону от 27 июля 2006 г. №149-ФЗ "Об информации,

информационных технологиях и защите информации", 2015, ст. 15.5, стр. 144/ Alexander Savelyev, ‘Art 15.5’ in *Commentary on the Russian Information Code* (Statut, 2015) 144.

who said in an interview that if the data was stored abroad its use would become uncontrollable.⁷⁰ Furthermore, as a user of internet services he felt safer if his data was stored in his own country. *Zharov* cites Booking.com as an example where it basically stores the data of Russian citizens on a server in Russia and transmits it to a foreign hotel only when such a hotel is booked. After the stay, Booking.com deletes the data.⁷¹

Further prohibitions result from the law ‘On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation’ which is only partially in force and which, according to Art 9(6) of the law, prohibits the collection of data and **the cross-border transfer of data** in the event of violations of the requirements, prohibitions, and restrictions under Russian law. Here, too, consent does not change anything.⁷²

b) Disclosure Obligations

Identification obligations and prohibition of anonymity; tax and other control.

Russian law imposes various disclosure obligations that are also common to European countries. For example, there is an **obligation to register** at the place of residence or stay in Russia.⁷³ In addition, there is a **duty of identification**.⁷⁴ The Tax Code provides for a number of **tax disclosure obligations** in

Art 23(1) of the Tax Code, such as filing a tax return or registering with State bodies responsible for taxes in Russia. There is no ban on anonymity.

A number of legal regulations make the use of public Wi-Fi subject to users disclosing their **mobile phone number** or **passport details**. This is to prevent terrorist threats. There have been several terrorist crimes in Russia notable the explosions in Moscow’s metro in 2010.

In connection with the data localisation obligation, a disclosure obligation arises for data controllers because according to Art 22(3) point 10.1. of the Russian Law on Personal Data **the location of the database** where the data of Russian citizens are stored must be disclosed to Roskomnadzor.

c) Voluntariness

Protection in dependency and hierarchy contexts; access to alternatives; prohibition of coupling; (voluntary) commercialization of personal data; incentives to data disclosure and protection therefrom [protection of adolescents; competition law; nudging]; prerequisites for consent; ‘privacy fatigue’; peer pressure [eg WhatsApp].

Consent is central to the assessment of the voluntary nature of data disclosure. According to Art 9(1) of the Russian Data Protection Act, consent must be **unambiguous, informed, and conscious**. In principle, the consent is free of form. It may be given in written,

⁷⁰ *Lenta.ru*: Здесь нет никаких проблем, <lenta.ru/articles/2015/09/01/personaldata/>, дата последнего обращения 13.12.2021/ Lenta.ru, ‘There are no problems here’ (*Lenta.ru*, 1 September 2015) <lenta.ru/articles/2015/09/01/personaldata/> accessed 13 December 2021; however, even domestic storage does not ensure complete control by domestic law, see § 2713 of the US CLOUD Act

⁷¹ *Lenta.ru*: Здесь нет никаких проблем, <lenta.ru/articles/2015/09/01/personaldata/>, дата последнего обращения 13.12.2021/Lenta.ru, ‘There are no problems here’ (*Lenta.ru*, 1 September 2015) <lenta.ru/articles/2015/09/01/personaldata/> accessed 13 December 2021.

⁷² см. абз. 6 ст. 9 Федерального закона “О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации”/see Art 9(6) of the Federal Law ‘On the

Activity of Foreign Persons on the Internet on the Territory of the Russian Federation’ <rg.ru/2021/07/05/inet.html> accessed 09 February 2022.

⁷³ см. абз. 1 ст. 6 или абз. 1 ст. 5 Федерального закона от 25.06.1993 N 5242-1 “О праве граждан Российской Федерации на свободу передвижения, выбор места пребывания и жительства в пределах Российской Федерации”/see Art 6 para. 1 or Art 5 para. 1 of the Federal Law of 25 June 1993 № 5242-1 ‘On the Right to Freedom of Movement and Choice of Place of Residence and Stay in Russia’ <pravo.gov.ru/proxy/ips/?docbody=&nd=102024464> accessed 13 December 2021.

⁷⁴ см. н. 3 абз. 1 ст. 13 Федерального закона от 07.02.2011 № 3 “О полиции”/see Art 13 para. 1 no. 3 of the Federal Law of 07 February 2011 № 1 ‘On the Police’ <rg.ru/2011/02/07/police-dok.html> accessed 13 December 2021.

oral, or electronic form. Implied consent is also possible. However, this requires that the implied act clearly expresses the will of the person concerned.

One exception is consent for the processing of sensitive categories of data which is given in writing. Another exception is consent for the publication of data in a publicly accessible source.

Art 10(1) of the Russian Law on Personal Data still provides for a type of consent that is only given for the further dissemination of the data to an unspecified group of persons. This consent must be given **directly and by means of a Roskomnadzor information system**. Implied consent is not sufficient for this purpose.

2. Recipient's Obligations

a) Requirements for Personal Data Reception

Information; requirements concerning content and formalities; warnings; notifications; assurances.

The term 'recipient' is not regulated in the Russian Law on Personal Data. The obligations under the Russian Data Protection Act are primarily addressed to the person responsible. The data may only be processed if a permissible circumstance exists (Art 6 of the Russian Data Protection Act).

Art 14(7) of the Russian Law on Personal Data obliges the controller to notify data subjects about the processing of data. According to Art 14 (7) of the Russian Law on Personal Data, such notification must contain information on the data controller, the purpose of the data processing, the categories of data, etc. There are some exceptions to the obligation to notify.

⁷⁵ см. абз. 4 ст. 5 Федерального закона от 14.07.2006 № 152 "О персональных данных"/Federal Law of 14 July 2006 № 152 'On personal data'

b) (Procedural) Obligations Concerning Received Personal Data

Purpose dedication/limitation; technological and organisational measures; data security; deletion and retention; further transmission and limitations thereto, also concerning transmission abroad.

Pursuant to Art 5(4) of the Russian Law on Personal Data, the **purpose limitation principle** applies in parallel to the processing principles already mentioned above.⁷⁵ A confidentiality obligation arises from Art 7 of the Russian Law on Personal Data which prohibits data controllers and other persons from disclosing and further disseminating data already collected to third parties without the data subject's consent.

The obligation to data localisation is particularly important. Pursuant to Article 18(5) of the Russian Federal Data Protection Act, when collecting personal data of Russian citizens, the data controller is obliged to **record, systematise, collect, store, update (improve, change), and extract the data** using databases located on Russian territory. There are some exceptions according to Art 6(1) points 2, 3, 4, 8 of the Russian Federal Data Protection Act. These include, for example, deviating provisions of an international treaty for the purpose of which the data are processed. With regard to internet communication services, the storage period on Russian servers is specified – 1 year for metadata and 6 months for content data (Art 10.1(3) of the Russian Law on Information). In addition, according to Art 10.1(3.1) of the Russian Law on Information, information society services are obliged to give access to give access to this data to law enforcement or security agencies upon request.⁷⁶

In addition, the controller is obliged to guarantee **technical and organisational measures** when processing the data. Furthermore, measures must be taken to prevent

<rg.ru/2006/07/29/personaljnnye-dannye-dok.html> accessed 09 February 2022.

⁷⁶ The storage and surrender claim relates to data with 'Russian' characteristics.

unauthorised access to data (Art 19(1) of the Russian Data Protection Act).

Cross-border data transfers are permitted if the receiving state has ratified **Convention 108** and thus has an adequate level of data protection. However, Roskomnadzor can also acknowledge an adequate **level of data protection** in other countries that have not ratified Convention 108 by way of verification and thus allow the transfer.

3. Control by Discloser

a) Transparency and Right to Request Information

The rights of data subjects are generally regulated in Chapter 3 of the Russian Law on Personal Data. In particular, individuals have the right to access their own data (this is similar to the right of information under Art 12 GDPR). The right of individuals to access their own personal data is not granted without restrictions. Restrictions arise, among other things, from processing of the data for the purpose of defence or security of the country. Another possible restriction is the processing of data in the context of a corruption investigation. In these cases, individuals are not granted access to data processing.

b) Co-Determination and Co-Decision Concerning Data Use

Restrictions for use; reservation of consent; revocation of consent; contestation and objection; special rules for international contexts; technical requirements for the act of permission/consent.

The individual has the right to have personal data **corrected, blocked, or deleted** (Art 16(1) of the Russian Law on Personal Data). The revocation of consent given is also permitted.

Of particular interest is Art 16(1) of the Russian Law on Personal Data which prohibits

legally relevant decisions solely on the basis of data processing. Such cases include, for instance, so-called *people analytics*, which plays an important role in the decision making about hiring and laying off employees, analysing their effectiveness and work performance, as well as deciding on job promotions.⁷⁷ However, there is also an exception to this if the individual has consented.

There are no special rules for cross-border situations and no technical requirements for co-determination.

c) Revocation

Data portability; deletion; 'right to be forgotten / to forget'.

There is no right to data portability in the Russian Law on Personal Data. A right to deletion arises from Art 17(1) of the Russian Law on Personal Data.

The right to be forgotten was introduced in 2015 in Art 10.3. of the Russian Law on Information. There is already initial court practice on this. The right to be forgotten can only be invoked against search engines. Then, the individual is entitled to the deletion of corresponding links from the search results where the information is published. However, there is no claim against search engines for the deletion of specific content.⁷⁸

d) Procedural aspects

Costs for and effectivity of the rights of the affected persons [information, etc]; consumer appropriateness.

The exercise of data subjects' rights is free of charge. Within the framework of the right of action pursuant to Art 17(1) of the Data Protection Act, **administrative** or **judicial** recourse is open to the individual.

However, the individual may be required to pay the sum of money resulting from

⁷⁷ Савельев, Научно-практический постатейный комментарий к Федеральному закону "О персональных данных", 2015, Статут, ст. 16 (1), стр. 121/ Alexander Savelyev, 'Art 16(1)' in *Commentary on the Russian Data Protection Law* (Statut, 2015) 121.

⁷⁸ Савельев, Электронная коммерция в России и за рубежом: правовое регулирование, 2016, Статут, стр. 598./Alexander Savelyev, 'E-commerce in Russia and Abroad' (Statut, 2016) 598.

Roskomnadzor's administrative expenses within the framework of the administrative legal process. However, this only happens if the individual has intentionally provided false information in his or her application. A court decision is necessary for the recovery of the monetary sum.

Within the scope of the judicial remedy, legal costs are susceptible according to the provisions of the procedural codes (eg Art 88 of the Code of Civil Procedure).

4. Enforcement

a) Damages and Compensation

[Material and immaterial] damages; reparations; disgorgement of profits; punitive damages.

The individual has the right to (im-)material damages within the framework of the judicial remedy. It has already been explained that it is difficult to prove material damage in the case of data protection violations.⁷⁹ The approximate amount of immaterial damages is between 3 euros (eg for transfer of personal data to debt collection companies) and 6 euros (for SMS advertising), which in Russian currency amounts to approximately 300–500 roubles.⁸⁰ By now, the courts prefer to black out the amount of non-material damages (even for non-personal data!) as they themselves understand how little this corresponds to the criteria of reasonable and fair damages.⁸¹

There are no punitive damages.

b) Procedural Aspects

'Threshold' for legal protection; right to initiation; burden of proof and evidentiary privileges; dispute value; 'small claims'; alternative dispute resolution; rights to bring/press charges; 'rational apathy'.

Roskomnadzor is explicitly designated as a State body responsible for protecting the rights of individuals in connection with data processing (see Art 23(1) of the Russian Law on Personal Data). Apart from deciding on

administrative complaints by data subjects, it has a number of other powers.

Russian data protection law does not provide for a special judicial procedure for the enforcement of claims under the Russian Data Protection Act. A lawsuit is filed within the framework of the already existing administrative and judicial legal protection channels.

IV. Objective Legal Obligations of the Recipient

1. Obligations Concerning Received Data

a) Dependence on Authorisation

Of business models, processing variants, terms and conditions.

There are no rules on authorisation requirements in the Russian Law on Personal Data. For example, there are no codes of conduct as regulated in Art 40 GDPR. Despite this, some companies issue codes of conduct. Mostly, this is true for foreign companies which is possibly connected to the requirements of foreign law. However, this is legally irrelevant for compliance with the Russian Law on Personal Data. The processing procedure is based on the rule of prohibition with the option of permission.

b) Notification Obligations

Regarding business models and business activities; regarding processing activities.

However, some notification obligations are present in Russian data protection law. According to Art 22(1) of the Russian Data Protection Act, the controller is obliged to notify Roskomnadzor of the start of data processing. Another obligation to notify arises from Art 22(3) point 10.1 of the Russian Data Protection Act because the **location of the database** in Russia must also be disclosed to Roskomnadzor.

⁷⁹ Савельев, Научно-практический постатейный комментарий к Федеральному закону "О персональных данных", 2015, Статут, ст. 17, стр.

127./Alexander Savelyev, 'Art 17' in *Commentary on the Russian Data Protection Law* (Statut, 2015) 127.

⁸⁰ In Russia it's only enough for a coffee! *ibid* 128.

⁸¹ *ibid*.

c) Documentation

Accountability.

Art 18 of the Russian Law on Personal Data which regulates the controller's obligations is silent on accountability. Among other things, there is no accountability for compliance with the processing principles comparable to Art 5(2) GDPR. An equivalence to accountability is the generally formulated liability of the controller for compliance with the Russian Law on Personal Data before Roskomnadzor (Art 23.1(2) of the Russian Law on Personal Data). Roskomnadzor is authorised to conduct **state data protection audits** of companies.⁸² Processors are also subject to the state data protection audit.⁸³

d) Processing Requirements

Prohibition subject to permission; balancing of interests; restrictions for terms and conditions; business practices; APIs/interfaces for third parties.

The basic requirement for data processing is the **prohibition with the option of permission** (Art 6 of the Russian Law on Personal Data). The **balancing of interests** as an element of permission is also provided for in Art 6(1)(7) of the Russian Data Protection Act.

Against the background of the common reservations of permission, the processing of

personal data should be noted where the use of a certain procedure makes it no longer possible to establish a reference to a person. Such data may be used for the improvement of State and municipal administration. Furthermore, the processing of such data is possible due to the requirements of the laws 'On Experimental Use of Artificial Intelligence in Moscow'⁸⁴ and 'On Experimental Legal Regimes in the Field of Digital Innovations'⁸⁵.

For contracts concluded on the Internet, rules on general terms and conditions apply.

The Russian Law on Personal Data does not contain any specifications for technical interfaces. However, Art 19(2)(2) of the Russian Law on Personal Data contains references to sub-legal acts that regulate technical requirements.⁸⁶

e) Prohibitions and Obligations

Prohibition of processing variants [eg profiling]; criminal prohibitions; restrictions under competition regulations; prohibition of abuses [of power/market power]; further transmission to third parties, especially governmental bodies; elicitation from abroad.

The data protection law's focus lies on the prohibition with the option of permission (see Art 6 of the Russian Law on Personal Data). Article 16(1) of the Russian Law on Personal Data regulates the prohibition of automated

⁸² Постановление Правительства РФ от 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных"/Decree of the Government of the Russian Federation of 29 July 2021 № 0146 'On State Control over Processing of Personal Data', <consultant.ru/document/cons_doc_LAW_388756/> accessed 14 December 2021.

⁸³ *ibid* 7.

⁸⁴ Федеральный закон от 24.04.2020 № 123 "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"/Federal Law of 24 April 2020 №123 'On experimental use of artificial intelligence in Moscow' <publication.pravo.gov.ru/Document/View/0001202004240030> accessed 14 December 2021.

⁸⁵ Федеральный закон от 31.07.2020 № 258 "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации"/Federal Law of 31 July 2020 № 258 'On experimental legal regimes in the field of digital innovations' <pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102801499> accessed 14 December 2021.

⁸⁶ Приказ ФСТЭК России от 18 февраля 2013 г. № 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"/Decision of the Federal Service for Technical and Export Control of 18 February 2013 № 21 'On substantive determination of technical and organisational measures for processing of personal data' <fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> accessed 14 December 2021.

individual decisions. However, a data subject can consent to automated data processing which then renders the data processing legal.

The data localisation obligation (Art 18(5) of the Russian Law on Personal Data) can also be considered in conjunction with the provisions on cross-border data transfer (Art 12 of the Russian Law on Personal Data).

A number of prohibitions arise for foreign companies as a result of violation of Russian law from the ‘On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation’. An example of this are the ban on advertising in Russia, the ban on displaying search results, and the ban on collecting and transferring personal data across borders or restricting users’ access to Internet services.⁸⁷

2. Monitoring

a) Recipient’s Self-Monitoring

Self-restrictions; compliance mechanisms; internal responsibilities [company privacy officers; ombudspersons.

The Data Protection Act has a wide range of addressees and they are obliged to comply with the Act’s provisions. The processing principles enshrined in Art 5 of the Russian Data Protection Act serve the controller’s self-control.

The Russian Data Protection Act does not entail a company data protection officer. However, there is nothing to prevent data controllers from appointing someone as a

company data protection officer if necessary without a special legal provision.

b) Regulated Self-Regulation

Sectoral and industry associations.

The Russian Data Protection Act does not contain any regulations on regulated self-regulation. However, this is envisaged as a goal of the **strategy for the development of data protection in Russia** which was prepared by Roskomnadzor. At the moment, regulated self-regulation is under development. Progress can be seen in individual areas; there are, for example, many initiatives in the banking sector.⁸⁸

c) Supervisory Authorities

Data protection authorities; competition authorities; economic oversight authorities.

The system of independent data protection authorities within the meaning of Art 51 of the GDPR is not known to Russian data protection law. Pursuant to Art 23 of the Russian Data Protection Act, compliance with data protection regulations is the responsibility of the Roskomnadzor and its territorial bodies. Roskomnadzor is part of the Federal Ministry for Digital Development.

The competition authority is the Federal Antimonopoly Service of the Russian Federation. Conflicts of competence with Roskomnadzor are not known. Both authorities have a practice of concluding cooperation agreements with each other.⁸⁹

⁸⁷ см. ст. 9 Федерального закона “О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации”/see Article 9 of the Federal Law ‘On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation’.

⁸⁸ *RSpectr.com*, В России саморегулирование в области защиты персональных данных развивается за счет отраслевых инициатив, <rspectr.com/novosti/52237/v-rossii-samoregulirovanie-v-oblasti-zashity-personalnyh-dannyh-razvivaetsya-za-schet-otraslevykh-iniciativ>, дата последнего обращения

14.12.2021/*RSpectr.com*, ‘Regulated self-regulation in data protection develops in individual areas’ (*RSpectr.com*, 9 November 2017)<rspectr.com/novosti/52237/v-rossii-samoregulirovanie-v-oblasti-zashity-personalnyh-dannyh-razvivaetsya-za-schet-otraslevykh-iniciativ> accessed 14 December 2021.

⁸⁹ См. ФАС, ФАС России и Роскомнадзор подписали соглашение о взаимодействии, <fas.gov.ru/news/7402>, дата последнего обращения 14.12.2021/See: The Federal Service for Control of Competition and Roskomnadzor conclude a cooperation agreement <fas.gov.ru/news/7402> accessed 14 February 2021.

d) (Specific) Criminal Prosecution

(Focus) prosecution units for informational offences; [situational/special] investigators.

Currently, there are no focus prosecution units or special investigators for offences related to personal data. However, Roskomnadzor fulfils a small special role in this regard. According to Article 23(3)(7) of the Russian Federal Data Protection Act, Roskomnadzor can provide the prosecutor's office and other law enforcement bodies with information that is relevant for deciding whether to initiate criminal proceedings.

e) Procedural Aspects

Investigation powers; resources of monitoring institutions.

Roskomnadzor and its territorial bodies are authorised to conduct governmental data protection audits. This applies to both controllers and processors. The procedure is regulated in the relevant regulation.⁹⁰ The processing activity is assigned to one of the four risk categories.⁹¹ How often such a data protection audit is carried out depends on the corresponding risk category. According to point 37 of the Regulation, a data protection audit can be both scheduled and unscheduled. In the context of data localisation, legal practice has shown that Roskomnadzor has always extended the implementation period for large IT companies before the data protection audit was carried out.

A specific feature of Russian information law is the obligation of **Internet communication services** to ensure compliance with the

technical requirements specified for information systems of such services by law enforcement and security authorities pursuant to Art 10.1(4) of the Russian Information Act. This compliance serves to enable the law enforcement and security authorities to fulfil their tasks.

The same obligation is found in the Russian **Telecommunications Law** (see Art 64(1)(2) of the Russian Law on Telecommunications).

3. Enforcement

a) Interventions Concerning Data Processing

Restriction and prohibition of data processing.

Roskomnadzor's powers of intervention are regulated by Art 15.1-1 to Art 15.6-1 of the Russian Law on Information and are extensive. Roskomnadzor is known in Russia mainly for **blocking** various content on the internet. Art 15.5 of the Russian Law on Information is important for data protection. According to Art 15.5 of the Russian Law on Information, Roskomnadzor can, for example, block an internet service if data protection regulations are violated. *LinkedIn*, for example, was blocked in Russia.⁹² A prerequisite for this is a court ruling. Another case is *Telegram* whose blocking, however, failed due to technological peculiarities of the service. Despite this, the Russian order to block Telegram was repealed last year after *Telegram* has made a deal with the Russian State.⁹³ According to media reports, Telegram's founder is said to have concluded a deal with Russian authorities.⁹⁴ However, the situation regarding this is

⁹⁰ Decree 'On State Control over Processing of Personal Data' (n 82).

⁹¹ See Annex to Decree 'On State Control over Processing of Personal Data' (n 82).

⁹² Определение Московского городского суда от 10.11.2016 по делу 33-38783/2016/Moscow City Court, Judg. of 10 November 2016 - the case 33-38783/2016; to access the judgment see <mos-gor-sud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adb19fe32a> accessed 30 May 2021.

⁹³ Роскомнадзор, О мессенджере Телеграм, <rkn.gov.ru/news/rsoc/news73050.htm>, дата обращения 09.02.2022/Roskomnadzor, 'Über Telegram' (*Roskomnadzor*, 18 June 2020) <rkn.gov.ru/news/rsoc/news73050.htm> accessed 09 February 2022.

⁹⁴ RBC: Разблокировка Телеграм в России и провал TON, <rbc.ru/crypto/news/5eecb41b9a7947d19b4df7a2>, дата последнего обращения 14.12.2021./RBC, 'Unblocking Telegram in Russia and the failure of block-chain project TON' (*RBC*, 2020)

rather opaque. It sometimes seems justified to assume that the Russian data protection law's restrictive regulations are primarily aimed at starting a dialogue with transnational companies. For example, *Google*, *Facebook*, and *Twitter* have not yet localised data in Russia and have also not been blocked, although this has long been legally possible. Blocking is probably a means of last resort.

Unblocking is possible according to Art 15.5(11) as soon as the data controller has fulfilled the data protection requirements.

Recently, Roskomnadzor blocked the *Tor* network but probably on a different legal basis of the Russian Law on Information than a violation of regulations on personal data.⁹⁵

The data localisation obligation can also be understood as a process-related interference since it requires Russian citizens' data to be stored exclusively within the country.

b) Interventions Concerning Business Models

Competition and economic supervision; government/public monopolies.

In comparison to competition law, there are no powers of intervention related to business models in data protection law. Something similar may result from the new law 'On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation' as its Art 2 declares the creation of 'equal conditions of activity for Russian and foreign legal entities' as a regulatory goal. According to Art 5(3) of this law, foreign companies that direct their activities to the Russian market must register a branch office, representative office, or other form of organisation in accordance with Russian law.

<rbc.ru/crypto/news/5eecb41b9a7947d19b4df7a2> accessed 14 December 2021.

⁹⁵ RBC: Роскомнадзор разблокировал сайт Tor, <rbc.ru/technology_and_media/08/12/2021/61b06ec79a7947326c020dc5>, дата

c) Processor-related Sanctions

Prohibition orders concerning business activities; corporate sanctions; revenue-based sanctions.

Processor-related sanctions can be found sporadically in different legal acts. The Russian Federal Data Protection Act refers to the Code of Administrative Offences in Art 24(1) of the Russian Federal Data Protection Act.

Art 13.11. of the Code of Administrative Offences regulates the sanctions for data protection law violations. For example, it introduces the fine for violations of data localisation obligations. The fine ranges from 1,000,000 roubles (approx. 12,000 euros) to 6,000,000 roubles (approx. 70,000 euros). For repeated violations of the data localisation obligation, the fine increases to a range of 6,000,000 to 18,000,000 roubles (approx. 200,000 euros).

Blocking has already been mentioned. However, it can be lifted.

A number of sanctions result from Art 9 of the Law 'On the Activity of Foreign Persons on the Internet on the Territory of the Russian Federation' which, among other things, introduces a restriction on money transfers in favour of the foreign service (but also prohibits data collection and cross-border data transfer).

d) Sanctions for Individual Actors

[Managing] directors' liability; individual criminal sanctions.

Data protection law does not provide for any special liability of managing directors. However, such liability (under civil, administrative, or criminal law) is conceivable under general provisions.

e) Procedural Aspects

Priority of data regulation enforcement; resources of enforcers; shaming impact/pillorying effect of breaches/violations.

последнего обращения 14.12.2021/RBC, 'Roskomnadzor locks Tor' (RBC, 2020) <rbc.ru/technology_and_media/08/12/2021/61b06ec79a7947326c020dc5> accessed 14 December 2021.

There is no prioritisation of data offences. There is little or no information on the enforcement bodies' equipment. The technical failure to block Telegram shows that Roskomnadzor does not have all the technical means at hand to effectively enforce Russian law.

The concept of pillorying as a legal term does not exist in Russian law. However, one could say that a data offence influences the social perception of the person concerned. This need, however, not always be only negative. One example is the refusal of Telegram's founder to comply with the data localisation obligation and data disclosure obligation. This had rather a positive social resonance in Russian society as it was a sign against restrictive data regulation in Russia. Yet, the subsequent non-transparent negotiations with Russian State bodies cast a bad light on this.

D. Sources and Literature

I. Related monographs

Федотов М.А., Информационное право, 2019, Издательство "Юрайт"/Mikhail Fedotov, *Information Law* (Jurajt, 2019) (available only in Russian).

Савельев А.И., Электронная коммерция в России и за рубежом: правовое регулирование, 2016, Статут/А. Savelyev, *E-commerce in Russia and Abroad* (Statut, 2016) (available only in Russian).

II. Related articles

L. Mälksoo, 'Russia's Constitutional Court Defies the European Court of Human Rights'

(2016) 12(2) *Constitutional Law Review* 377–395 (available only in English).

Zhuravlev M and Brazhnik T, 'Russian data retention requirements: Obligation to store the content of communications' (2018) 32 *Computer Law & Security Review* 128–145 (available only in English).

A. Savelyev, 'Russia's new personal data localisation regulations: A step forward or a self-imposed sanction?' (2016) 34 (3) *Computer Law & Security Review* 496–507 (available only in English).

III. Leading Cases

Определение Московского городского суда от 10.11.2016 по делу 33-38783/2016/Moscow City Court, Judg. of 10 November 2016 – Case 33-38783/2016 (LinkedIn case) (available only in Russian).

IV. Miscellaneous

Савельев, Научно-практический постатейный комментарий к Федеральному закону "О персональных данных", "Статут" 2015/А. Savelyev, *Commentary on the Russian Data Protection Law* (Statut, 2015) (available only in Russian).

Савельев, Комментарий к Федеральному закону от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и защите информации", 2015, Verlag "Статут"/А. Savelyev, *Commentary on the Russian Information Law* (Statut, 2015) (available only in Russian).