Article

DOI: 10.17803/2713-0533.2024.2.28.246-267

Legal Challenges Surrounding Participation of Big Tech Companies in the Russian Social Networking Market

Vladimir A. Kanashevskiy

Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

Abstract: This article outlines the regulatory landscape surrounding the participation of global technological companies in the Russian social network market. These companies include Alphabet (Google), Meta/Facebook,[1] X (former Twitter),[2] Apple, Microsoft and Amazon. However, this article primarily concentrates on those that provide computing social network services, i.e., Google, Meta/Facebook and X/Twitter. The author considers a number of topics. Firstly, the Russian law requirements on the mandatory physical presence of foreign companies which provide social networking services in Russia. Secondly, the issues surrounding the storage of personal data in a foreign data base or cloud, particularly retention obligation and the cross-border transfer of personal data. Thirdly, obligations for Internet providers with regard to the blocking or deletion of information that violates Russian law. There are many obstacles for Big Tech companies to work in the Russian networking market, including lack of general regulation of these services, information security requirements, restrictions contained in Personal Data Law and Information Law. An analysis of the European and Russian regulation shows that both legal systems contain similar obligations. Furthermore, if relations between EU and Russia were better, it would be beneficial to accept EU rules (such as the Digital Services Act (DSA)) as binding.

[1] Note: Meta Platforms Inc. is recognized as extremist and banned in the Russian Federation.

[2] Note: X platform is banned in the Russian Federation.

This could be done by concluding an international agreement that would extend the sphere of application of some of the DSA rules, which are in the mutual interest of both parties. However, in the current political situation this goal is difficult to achieve.

Keywords: social networking services; retention obligation; personal data; information security; confidential information; cross-border transmission; data processing center; foreign cloud; database

Cite as: Kanashevskiy, V.A., (2024). Legal Challenges Surrounding Participation of Big Tech Companies in the Russian Social Networking Market. *Kutafin Law Review*, 11(2), pp. 246–267, doi: 10.17803/2713-0533.2024.2.28.246-267

Contents

I. Introduction

Until recently, many companies, especially large and medium sized ones, which provide social networking services were active in the Russian market, notably the major players such as Google, Meta/Facebook and X/Twitter. These companies, known as “large communication intermediaries” and “dominant platforms” (Moore and Tambini, 2022,

pp. 12, 18) have developed famous and effective social networking platforms. They are so powerful that there are even suggestions that these companies could be regulated as utilities or brought into public ownership (Moore and Tambini, 2022, p. 2). Many Russian companies have also developed competitive social network platforms, such as VKontakte (vk.com) or Odnoklassniki (odnoklassniki.ru), which are more popular among local users than Meta/Facebook and X/Twitter. Most of the major players (they are also named as Big Tech companies) are the US companies, whereas EU countries are represented primarily by small and medium enterprises (SMEs) (Hadebe, 2022, p. 4).

Because of the Special Military Operation (SMO), many foreign major players have closed their local offices in Russia and stopped providing social network services in Russia. They no longer advertise their services to Russian customers and do not localize their websites in order to be competitive in the Russian market. However, some Russian users continue to use foreign network social platforms via different virtual private networks (VPNs).

Foreign companies, including Big Tech companies, who are targeting their activities on Russian territory, must comply with the retention obligation. They are not allowed to transfer information to foreign databases or store it in data processing centers situated outside Russia without localization in Russia.

It should be noted that the activities of some Big Tech companies in the territory of the Russian Federation were prohibited because of their alleged non-compliance with Russian laws. Their apps and websites were blocked as they restricted access of Russian users to certain information. These and other issues surrounding the regulatory framework of the use of services of Big Tech companies in Russia will be addressed in detail below. We will start with an analysis of the requirements regarding mandatory physical presence that were recently introduced in Russia. Then, we will review the issues surrounding the storage of personal data in foreign clouds and databases that Big Tech companies own or use. In particular, we will discuss the retention obligation, sanctions applicable to its breach, its potential impact on cloud services, implementation of the retention obligations in Russian practice and the storage of Internet content in foreign clouds or databases. Finally, we will explore the issues

regarding the blocking or deletion of information that is distributed by the Big Tech companies in violation of Russian laws.

Roskomnadzor[3] maintains a list of foreign companies whose informational resources have been prohibited from advertising their services in Russia. As of February 2024, the list includes 26 companies, such as Google LLC, Twitter Inc., TikTok Pte Ltd., Zoom Video Communications Inc, and Viber Media S.à r.l. For example, Google LLC was prohibited from advertising its resources (google.ru; google.com; youtube.com; mail.google.com; gmail.com, etc.).[4] The same companies have been prohibited from placing advertisements on their resources in Russia.[5] Basically, this means that Big Tech companies, along with some other listed foreign entities, have been excluded from providing any Internet services in the Russian segment of the Internet. This happened because of various requirements that were introduced in Russian law in recent years. The first requirement, which appeared in 2021, is that foreign companies involved in the Internet industry must be physically present in the Russian territory. Another requirement, introduced in 2015, is that personal data of Russian citizens must be localized. Finally, there were some restrictions on the distributed information itself.

In this article, we are going to address these and other related issues.

II. Mandatory Physical Presence of Foreign Companies that Provide Social Networking Services

Russian law does not contain any definition of social net-working services. The most relevant definition is one suggested by Nicole Ellison in 2007, who defined them as "web-based services that allow individuals

[3] Roskomnadzor is the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communication of the Russian Federation, which is the data protection supervisory authority in Russia. Available at: https://rkn.gov.ru/ (In Russ.). [Accessed 06.02.2024].

[4] List of Foreign Persons Conducting Their Activity on the Internet in the Territory of the Russian Federation. Available at: https://236-fz.rkn.gov.ru/agents/list (In Russ.). [Accessed 06.02.2024].

[5] List of Foreign Persons Conducting Their Activity on the Internet in the Territory of the Russian Federation.

to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and transverse their list of connections and those made by others within the system" (Daxton, 2017, p. ix).

Starting from the early 2010s, the Big Tech companies became very active in the Russian social networking market. The share of Meta/ Facebook and X/Twitter in the country was significant, around 40 %. Google's YouTube remains one of the main video hosting tools in Russia. However, these companies did not have a physical presence in the country, except Google, who had a small office in Moscow, which mostly performed marketing activities. The Russian authorities were interested in the legal presence of Big Tech companies for two main reasons:

A) Taxation of the sales which the Big Tech companies made in Russia, and

B) The enforcing of mandatory rules which prohibit distribution of certain information by the Big Tech companies or their involvement in political activities in Russia.

As a result, on 1 July 2021, Federal Law "On the Activities of Foreign Persons involved in the Internet industry in the territory of the Russian Federation (RF)" No. 236-FZ[6] was adopted and came into effect. This Law covers the activities of foreign individuals and entities who own Internet sites, software programs and informational resources and have more than 500,000 users who have access to those resources during the day. In addition, they render their services in the Russian language, process the data of Russian users, collect money from Russian customers, or place advertisements that are targeted at Russian users. In particular, Law No. 236-FZ covers the following three types of subjects:

a) Internet providers, whose users are located in the territory of the Russian Federation;

b) Information distributors who transmit electronic messages of Russian users; and

c) Distributors of advertisements targeted at Russian customers through the Internet.

[6] Available at: http://www.consultant.ru/document/cons_doc_LAW_388781/ (In Russ.). [Accessed 06.02.2024].

Under Law No. 236-FZ, the persons above must create a branch office or a representative office or an entity under Russian law, which would represent them in courts and be held liable to the full extent of their assets under the courts' judgements issued against foreign persons. They should interact with Russian customers and restrict public access to unauthorized information. If a foreign person does not comply with this Law, the regulators may take measures against it, such as prohibiting the placement advertisements, or restricting the transborder transfer of personal data, or blocking its websites. The obligation to create a branch or a representative office or entity has been in force since 1 January 2022.

There is no doubt that Law No. 236-FZ is aimed at regulating the activities of the IT giants, such as Google, Meta/Facebook, X/Twitter, Amazon and Apple. Furthermore, Roskomnadzor issued a list of companies which should create their local offices in Russia. Initially, 13 companies were included in this list: Apple, Discord, Meta/Facebook, Google, Likeme, Pinterest, Spotify, Telegram, TikTok, Twitch, X/Twitter, Viber and Zoom.[7] Many of these companies did not have offices in Russia which would represent them in their relations with customers, and basically were beyond the control of Russian regulators. Thus, it was almost impossible to enforce the judgements of Russian courts against these companies for breaches of Russian laws such as the Personal Data Law.[8] Because of the SMO, many of the big players in the market, such as Google, X/Twitter, Meta/Facebook have suspended their commercial activity in the Russian market. Those companies that had offices in Russia have closed them, or are in the process of liquidation (as in the case of Google LLC[9]). Nevertheless, some companies, such as Viber and Apple, have opened and maintained their offices in Russia.

[7] Roskomnadzor published the List of the Foreign Internet Companies that should open their local offices in Russia. Available at: https://rkn.gov.ru/news/rsoc/news73944.htm (In Russ.). [Accessed 06.02.2024].

[8] Federal Law "On Personal Data" No. 152-FZ dated 27 July 2006 (as amended on 6 February 2023). Available at: https://www.consultant.ru/document/cons_doc_LAW_61801/ (In Russ.). [Accessed 06.02.2024].

[9] *See* Extract for Google LLC (reg. number 1057749528100) from the Russian Unified Register of Legal Entities. Available at: https://pb.nalog.ru (In Russ.). [Accessed 10.02.2024].

How does the requirement of physical presence correspond to international practice? We can find a similar approach in some countries.

The European law operates with the concept of "very large online platforms,"[10] which have more than 45 million active monthly users in the EU. However, there is no requirement about the mandatory physical presence of these platforms in the territory of the EU or its member-states.

It should be noted that OECD[11] elaborated a special incentive (Pillar One), supported by more than 130 countries, which suggests that the multinational enterprises (MNEs) should be taxed regardless of their physical presence in the country.[12] Pillar One applies to approximately 100 of the biggest MNEs and distributes part of their profit to countries where they sell their products and services.[13] Big Tech companies are also among these companies.

It was envisaged that the local offices which should have been created by Big Tech companies in Russia would help the local authorities to tax Big Tech companies because their income would be mostly associated with the sales activities of their local offices. As a result, in 2016 "Google Tax" was introduced in Russia and came into effect in 2017. According to the law, if foreign companies sell digital services to Russian companies and entrepreneurs, these foreign companies must be registered with the Russian tax authorities and pay VAT themselves.[14] Prior to 2017, it was the obligation of the Russian counterparts who bought digital services

[10] *See* Digital Services Act (Art. 33). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065. [Accessed 05.02.2024].

[11] OECD is the Organization for Economic Cooperation and Development.

[12] OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris. Available at: https://doi.org/10.1787/beba0634-en. P. 10. [Accessed 06.02.2024].

[13] OECD. Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy Frequently asked questions. July 2022. Available at: https://www.oecd.org/tax/beps/faqs-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-july-2022.pdf. [Accessed 06.02.2024].

[14] The Russian Tax Code, Art. 174.2. Available at: https://www.consultant.ru/document/cons_doc_LAW_28165/ (In Russ.). [Accessed 06.02.2024].

from a foreign company to pay the VAT. They acted as tax agents in these cases. Now, Russian customers are released from this obligation since they are no longer considered to be VAT tax agents. However, the practical effect of this rule has been undermined by the fact that Big Tech companies have been prohibited from providing services in Russia and have suspended their activities here.

As of today (January 2024), the most popular internet resources in Russia are Yandex (82 % of the Russian population), Google (81 %), YouTube (78 %), WhatsApp[15] (78 %), VKontakte (74 %) and Telegram (68 %).[16]

III. Localization of Personal Data of Russian Citizens as Challenges for Big Tech Companies

III.1. Retention Obligation and Cross-Border Transfer Issues

Before Big Tech companies ceased their activity in Russia in 2022, one of the biggest obstacles for them was the requirements of Russian personal data protection laws. Under Personal Data Law, personal data is defined as any information related directly or indirectly to an identified or identifiable individual, i.e., a personal data subject. This definition is similar to the one under the European data protection legislation and typically includes the name, date and place of birth, address, job, education, income and other information based on which an individual can be identified.

According to Personal Data Law, *"at the time of the collection of personal data, inter alia over the Internet, the operator [i.e., the controller of personal data within the meaning of European data protection legislation] must ensure that the personal data of Russian citizens is recorded, systematized, accumulated, stored, specified (updated or modified) and retrieved in databases located in the Russian Federation."*

[15] Part of Meta that is recognized as extremist and banned in the Russian Federation.

[16] Mediascope. Available at: https://mediascope.net/data/ (In Russ.). [Accessed 20.02.2024].

Once this rule was introduced in Personal Data Law in 2015, there was a discussion as to whether the personal data of Russian citizens could be firstly recorded abroad and then reproduced in Russian databases. The Ministry of Digital Development issued clarifications[17] and explained that personal data should be *initially* recorded and stored in databases located in Russia.

However, this does not prevent the controller from making copies of such data and storing and further processing these copies elsewhere (i.e., the creation of backup copies). Nonetheless, the Russian database should be regarded as the primary storage location and the foreign databases only as secondary databases. Therefore, the same approach should be taken when updating personal data, i.e., the copies stored in Russian territory should be updated first and only then should the controller proceed with updating the foreign database.

Personal Data Law applies solely to the territory of the Russian Federation and/or to the personal data of Russian citizens. As the Ministry of Digital Development clarified, Personal Data Law does not have extraterritorial effect and any borderline cases should be evaluated on an individual basis.

The commentary on Personal Data Law which was placed on the Roskomnadzor website, states that *"parallel insertion of the collected personal data into a Russian information system and a system located on the territory of a foreign state does not comply with the requirements [of Personal Data Law] because the data may be transferred to a foreign information system only after their collection by way of a cross-border transfer."*[18]

However, many service providers (controllers) implement solutions involving parallel (simultaneous) storage of personal data in Russian and foreign databases. This conclusion can also be supported by the technical aspect — in today's technologies, it may, on occasion be

[17] The clarifications by the Russian Ministry of Digital Development, Communications and Mass Media were initially published on Roskomnadzor's site (https://digital.gov.ru/en/personaldata/). As of today, these clarifications are no longer available on Roskomnadzor's site but still play practical role.

[18] Commentary on Federal Law No. 242-FZ dated 21 July 2014. Available at: https://pd.rkn.gov.ru/library/p195/ (In Russ.). [Accessed 06.02.2024].

difficult to distinguish between the primary and secondary databases and it may thus lead to the interpretation that simultaneous storage is acceptable even if, strictly speaking, it may be found not to fully adhere to Personal Data Law as interpreted by the regulators.

It should be noted that transfers abroad to a secondary database are permissible to countries that either are party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108,[19] or mentioned in the special list of the countries, approved by Roskomnadzor in 2022.[20] For the transfer of personal data to other countries, such as the United States, it is necessary to obtain permission from Roskomnadzor. These amendments were introduced in 2022.[21]

III.2. Sanctions for Breach of Retention Obligation and Their Impact on Big Tech Companies

Until recently, there were no specific monetary sanctions linked to the breach of the retention obligation. However, a company could be subject to a fine of EUR 50, if it breached the obligation to provide the supervisory authority with information relating to the implementation of the retention obligation.[22]

---

[19] Chart of signatures and ratifications of Treaty 108. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. [Accessed 06.02.2024].

[20] Roskomnadzor Order No. 128 dated 5 August 2022. Available at: https://www.consultant.ru/document/cons_doc_LAW_426970/ (In Russ.). [Accessed 04.02.2024].

The list currently includes 34 states: Australia, Gabon, Israel, Qatar, Canada, Kyrgyzstan, China, Thailand, Malaysia, Mongolia, Bangladesh, New Zealand, Angola, Belarus, Benin, Zambia, India, Kazakhstan, Costa Rica, Republic of Korea, Ivory Coast, Mali, Niger, Peru, Singapore, Tajikistan, Uzbekistan, Chad, Vietnam, Togolese Republic, Brazil, Niger, Republic of South Africa, Japan.

[21] Federal Law "On the Introduction of Amendments to Personal Data Law and Certain Legislative Acts..." No. 266-FZ dated 14 July 2022. Available at: https://www.consultant.ru/document/cons_doc_LAW_421898/3d0cac60971a511280cbba229d9b6329c07731f7/ (In Russ.). [Accessed 05.02.2024].

[22] Art. 19.7 of the Administrative Code of the Russian Federation. Available at: https://www.consultant.ru/document/cons_doc_LAW_34661/ (In Russ.). [Accessed 05.02.2024].

However, in December 2019, amendments were introduced to the Russian Administrative Code that prescribe that an administrative penalty should be imposed if the retention obligation is breached. Today, the monetary penalty for a legal entity for a breach of the retention obligation can range from EUR 9,500 to 56,500. In the case of a repeated violation, a fine ranging from EUR 56,500 to 170,000 may be imposed.[23] The supervisory authority may also apply to the court in order to request that the website of the breaching company should be blocked. Upon obtaining the court decision, the supervisory authority can block the relevant website by an order addressed to the relevant Internet service provider(s). This is, however, an extreme measure which can be applied only in specific circumstances as you can see from the reasoning below. If the breach is attributable to an officer of the breaching entity (i.e., a company director or the person who is responsible for the company's compliance with Personal Data Law requirements), the law stipulates fines that can amount to between EUR 1,000–2,000 for the breach of the retention obligation; and between EUR 4,700 and 7,500 for repeated violations.

Roskomnadzor has blocked the websites of some major players due to a prior breach of their retention obligation. On 10 November 2016 (case No. 33-38783/2016) the Moscow Court decided that the LinkedIn website and app should be blocked. This has effectively ended LinkedIn's operations in the Russian territory due to continuous violations of their retention obligation. Since then, LinkedIn has not been accessible from Russia.

Two other global social media companies have also been found to be in breach of their retention obligations — Meta/Facebook and X/Twitter. In December 2019, Roskomnadzor imposed a fine of EUR 50 on each of the companies for not providing information about the implementation of their retention obligations. The imposition of these relatively light sanctions, instead of blocking the companies' websites, happened presumably because of the significance of both companies in the Russian market and the regulator's connected fear of negative

[23] Art. 13.11(8) of the Administrative Code of the Russian Federation. Available at: https://www.consultant.ru/document/cons_doc_LAW_34661/ (In Russ.). [Accessed 05.02.2024].

publicity. For more than four years, the regulator has been seeking an amicable resolution to the problem, instead of blocking the Internet services of Meta/Facebook and X/Twitter. The amendments to the Administrative Code introduced in December 2019 were likely to serve as an incentive for both companies to comply with the retention obligation under Personal Data Law. As a result of these amendments, on 13 February 2020, the magistrate judge of the Moscow court imposed a fine of RUB 4 million (approximately EUR 40,000) on each company.[24] The decision against X/Twitter was upheld by the court of cassation in July 2020.[25]

Similarly, on 29 July 2021, the magistrate judge of the Moscow court imposed a fine of RUB 3 million (approximately EUR 28,500) on Google Corporation.[26] In June 2022, the magistrate judge of the Moscow court again considered the cases against the foreign companies for not complying with their retention obligations under Personal Data Law. Google LLC was fined RUB 15 million (approximately EUR 142,500) for their repeated refusal to localize the personal data of Russian users as required by Art. 13.11 of the Administrative Code.[27]

There were doubts whether the fines imposed by the Russian courts could be effectively enforced against Google, X/Twitter and Meta/ Facebook. Russia has never had an agreement with the United States on the recognition and enforcement of court judgements. Moreover,

[24] *See* Decision in case No. 05-0167/374/2020 dated 13 February 2020 issued against Twitter Inc. Available at: https://mos-sud.ru/search?formType=shortForm&uid=&caseNumber=05-0167%2F374%2F2020&participant= (In Russ.). [Accessed 06.02.2024]; Decision in case No. 05-0168/374/2020 dated 13 February 2020 issued against Facebook Inc. Available at: https://mos-sud.ru/search?formType=shortForm&uid=&caseNumber=05-0168%2F374%2F2020&participant= (In Russ.). [Accessed 07.10.2023].

[25] *See* Resolution of the 2nd Court of Cassation in case No. 16-3770/20 dated 7 July 2020. Available at: http://www.consultant.ru/ (In Russ.). [Accessed 06.02.2024].

[26] *See* Decision in case No. 05-2010/422/2021 dated 29 July 2021 issued against Google. Available at: https://mos-sud.ru/search?formType=shortForm&uid=&caseNumber=&participant=google (In Russ.). [Accessed 06.02.2024].

[27] Court Penalizes Foreign Companies for Their Refusal to Localize the Personal Data of Users in Russian Territory. Available at: https://rkn.gov.ru/news/rsoc/news74356.htm (In Russ.). [Accessed 05.02.2024].

the aforementioned companies did not have sufficient assets in Russia. There was a common understanding that the judgements would have not been enforced, unless the companies had paid the fines voluntarily. However, as we can see from the Federal Service of Bailiffs' website, there is no information about unpaid fines by Google, X/Twitter and Meta/Facebook. This means that these companies have all paid their billion-ruble fines (Mironenko, 2024).

In February and March 2022, X/Twitter, Meta/Facebook and Instagram were blocked from their activity on the Russian market under decisions of the Russian courts. The courts ruled that these companies had breached the principles of free distribution of information and had restricted access of Russian users to Russian mass media on their Internet platforms. X/Twitter was also blocked for the distribution of illegal content. Following this, the issue of the payment of fines for breach of retention obligations by these companies basically becomes irrelevant.

III.3. Implementation of the Retention Obligations in Russian Practice

As Russian practice shows us, many multinational corporations with operations in Russia ensure their compliance with Personal Data Law requirements by outsourcing the technical solution to third-party providers. Russian practice shows that many multinational corporations with operations in Russia ensure their compliance with Personal Data Law requirements by outsourcing the technical solution to third-party providers. Personal Data Law allows foreign Internet service providers to store the personal data of Russian citizens simultaneously in Russian and foreign databases. However, according to the official interpretation of this law by regulators, there should be an initial recording of all personal data in a Russian database (the "initial database") and then the subsequent transfer and recording of the same data in a foreign database (the "secondary database"). In other words, there should be a time lapse between the recording and storage of the data in Russia and its subsequent export abroad.

This requirement of Personal Data Law can make it difficult to implement international informational solutions that are based on blockchain technology. These solutions provide the simultaneous updating of information contained in different databases in all nodes of such systems (Saveliev, 2021).

According to Personal Data Law, a personal data operator (a data controller in the European sense of this word), who is also acting as an Internet service provider, should undertake all technical and organizational measures to protect the confidentiality of the information, such as data encryption and data anonymization.[28] However, it is difficult to implement these measures in practice since foreign data controllers cannot be bound by Russian technical requirements. The national law of the country where foreign providers have their domicile sets forth its own rules and technical requirements regarding the protection of information. However, in view of the provisions of Russian law, foreign personal data controllers should advise their Russian clients (personal data owners) to choose a convenient data center where the respective personal data is to be stored. Specifically, such a data center should be located in a country that provides adequate protection of personal data from the point of view of Personal Data Law.

It should be noted that notion of a data localization rule is also known to some other national legal systems. Thus, in the European Union (EU), there is a general rule, established by GDPR,[29] which provides that any transfer of personal data is permissible if the adequate level of protection is guaranteed (Art. 44). According to the EU Data Retention Directive Retention of 2006, all EU member states must store electronic communications for at least six months. These rules have been further developed in subsequent legislation of EU countries (FRA, 2017). This can be regarded as the EU response to the expansion of the US Big Tech companies, such as Amazon, Microsoft and Google whose

[28] *See* Roskomnadzor Order "On the Requirements and Methods of Personal Data Anonymization" No. 996 dated 5 September 2013; Guidelines on the Application of Roskomnadzor Order No. 996 (approved by the Roskomnadzor on 13 December 2013). Available at: http://www.consultant.ru/ (In Russ.). [Accessed 06.02.2024].

[29] General Data Protection Regulation. Available at: https://gdpr-info.eu/. [Accessed 18.02.2024].

share in the market of cloud computing services as high as 92 %. As a result (Hadebe, 2022, p. 12). Such countries as "Bulgaria, France, Germany, Luxembourg, Poland and Sweden have already sanctioned 'data localisation' measures that prevent certain types of data from being held abroad" (Hadebe, 2022, p. 13).

In Russia, data center services are required to store specific information on Russian territory, notwithstanding economic sanctions, any increase in equipment cost, and lack of qualified employees. Since 24 February 2022, the situation has deteriorated because of many of the Big Tech companies as well as small and medium sized Internet service providers have left the country. Today, there is a common understanding that the problem of the lack of facilities for storing data can be resolved by building data centers in Russia rather than using foreign databases. Russia should not rely exclusively on foreign facilities, even though their use is commercially profitable. The use of US data centers was convenient for Russian providers because of the time difference between the US and Russa: the US facilities were free and easily accessible during the night.

Russia has obvious competitive advantages in building data centers in its territory. These are relatively cheap energy and cold climate. The new data centers are to be built in regions with low-cost energy and low temperature, since the storage and processing of data requires a lot of energy and low temperatures (Ivanov, 2023).

III.4. Requirements for Information Distributors as to the Distributed Content: Restriction of Public Access to Unauthorized Information

In the years 2021–2023, Russian courts issued numerous judgements against Big Tech companies for not taking appropriate measures with regard to the restriction of public access to unauthorized information. For example, Google was obliged to pay RUB 26 million (EUR 245,000), Meta/Facebook RUB 66 million (EUR 625,000), and X/Twitter RUB 38 million (EUR 360,000) in administrative penalties as stipulated in the Administrative Code (Trushina, 2021). The companies actually paid these fines (Kommersant, 2021). The penalties were imposed for breach

of Information Law,[30] which prohibits the dissemination of information that violates Russian laws, such as information that promotes extremist activity, child pornography, drug production and drug dealing. For example, on 27 May 2021, the magistrate judge of the Moscow court penalized Google corporation (1600 Amphitheatre Parkway Mountain View, CA 94043, USA) for not disabling access to certain resources containing information the dissemination of which is prohibited in the Russian Federation. Access to these resources had been restricted by the Russian authorities, but were still available for Google users.[31]

Recently, Google and Meta/Facebook were brought to more strict liability. According to Art. 13.41 of the Administrative Code, the penalties for repeated violation should amount to between one twentieth (1/20) and one tenth (1/10) of the company's annual turnover. For example, on 24 December 2021, the magistrate judge of the Moscow court fined Google and Meta/Facebook RUB 7,2 billion (EUR 85,6 million) and RUB 2 billion (EUR 23,8 million) respectively for repeatedly failing to remove unauthorized information. These penalties were calculated based on Google and Meta/Facebook's turnover for the year 2020. For example, Google LLC's turnover in 2020 was approximately RUR 85 billion (EUR 1 billion) (Stepanova, 2021).

The aforementioned measures adopted by the Russian authorities are not unique and can be found in the U.S. practice. For example, US federal investigators issued a subpoena to X/Twitter for personal information of users suspected of collaborating with WikiLeaks to publish confidential U.S. documents (Daxton, 2017, p. viii). However, it is worth noting that in the U.S. to date social network sites have been treated as private spaces rather than public ones, and they are allowed to make their own rules, even if those rules are more restrictive than is allowed under U.S. law (Henderson, 2017, p. 23). This is also largely true in respect of most European countries.

[30] Federal Law "On Information, Information Technology and Protection of Information" No. 149-FZ dated 27 July 2006, as amended on 12 December 2023. Available at: https://www.consultant.ru/document/cons_doc_LAW_61798/ (In Russ.). [Accessed 06.02.2024].

[31] *See* Decision in case No. 05-1584/422/2021 dated 27 May 2021 issued against Google. Available at: https://mos-sud.ru/search?formType=shortForm&uid=&caseNumber=05-1584%2F422%2F2021&participant= (In Russ.). [Accessed 06.02.2024].

Similar instruments can be found in EU law, specifically in the Digital Services Act (DSA) and the Digital Markets Act (DMA), which changed the way of providing digital services in the EU. Both documents were adopted in 2022 and now are in force in EU countries.[32] The DSA contains rules on how platforms such as Meta/Facebook and YouTube should handle content that has been signaled to them as illegal, and the DMA intends to empower European authorities to prevent anticompetitive behavior from digital companies (Penfrat, 2020). A new regulatory regime established by the DSA and the DMA is a reaction to years of harmful practices on Big Tech online platforms, ranging from terrorist activities to widespread sharing of child sexual abuse and anti-competitive practices on global platforms (Goujard and Stolton, 2021).

Like Russian law, the DSA established the key principle of the moderation of social medium platforms — "delete first, think later" (Penfrat, 2021). According to the DSA, a service provider should immediately remove illegal content or restrict access to it.[33] National authorities may also order providers to act accordingly once they discover any illegal content.[34] These obligations are similar to those that exist in Russian law. If relations between EU and Russia were better, it would be beneficial to accept the DSA rules as binding. This could be done by the conclusion of an international agreement which would extend the sphere of application of the DSA. According to Art. 2(1) of the DSA, this Regulation applies if the recipients of intermediary services have their place of establishment in the EU, whereas the place of establishment of the providers of those services is not relevant. Therefore, the conclusion of an international agreement would be necessary to extend the application of the DSA outside the EU. As it is rightly noted by S. Hadebe, the significance of the DMA is that it represents the "rules that target few companies — the digital environment is in the hands of powerful companies. It may be easier to regulate the behavior of a few

[32] The Digital Service Act package. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [Accessed 06.02.2024].

[33] Para. 22 of the Preamble to the DSA. *See* also: Art. 18 of the DSA.

[34] Para. 31 of the Preamble to the DSA. *See* also: Art. 9 ("Orders to act against illegal content") of the DSA.

players, especially when there is concentration in the economy […].” (Hadebe, 2022, p. 21).

Apart from political considerations that are not analyzed here, it is obvious that the main obstacle to the conclusion of such an international agreement is the different views as to the information which could be qualified as “illegal” between the countries. As a starting point, one recommendation would be to include in the list of illegal information the most obvious actions and crimes, such as those mentioned in the DSA: crimes against children, hate speech, sale of prohibited goods, and other obviously illegal activities).[35] As regards other information, such as extremist actions, political and religious activities, this should be left for later discussion and possible future negotiations. In this context, the appropriate self-regulatory codes, such as codes of hate speech, disinformation, and terrorism (Moore and Tambini, 2022, p. 6) would also play a key role.

IV. Storing Internet Content in Foreign Clouds and Databases belonging to Big Tech Companies

Information Law provides that organizers of information distribution via the Internet (the “Information Distributor”) must:

a) store meta-data (i.e., information about the details of receiving, transmitting, delivering and/or processing voice information, written texts, images, voices, video and other electronic messages of Internet user) on Russian territory for a period of one year, and

b) store the content of the data itself (i.e., texts, images, voices, video, etc.) in the Russian databases for a period of six months, and

c) provide such information to the law enforcement authorities on their demand.[36]

The Information Distributors must design the equipment and software used in their information systems in such a manner that

[35] *See* Paras 17–20 of the Preamble to the DSA.

[36] Art. 10.1 of Federal Law “On Information, Information Technology and Protection of Information” No. 149-FZ dated 27 July 2006, as amended on 12 December 2023. Available at: https://www.consultant.ru/document/cons_doc_LAW_61798/ (In Russ.). [Accessed 06.02.2024].

would allow the law enforcement authorities to exercise their statutory competencies (i.e., the equipment and software must be designed in a way that allows for easy access by the police and the FSB[37] to the stored content).

The Information Distributor is defined as a party that *ensures the functioning of information systems and/or computer programs designed and/or used for receiving, transmitting, delivering and// or processing of the Internet users' electronic messages*. In European law, the closest equivalent to Informational Distributor is the term "provider of intermediary services."[38] The Information Law defines "electronic messages" as *any information transmitted or received by users of information-telecommunication network*. Such electronic messages include *"voice information, written texts, images, voices and other electronic messages of the Internet users."* These all-embracing definitions support the conclusion that, for the purposes of the Information Law, electronic messages are any messages transmitted over the Internet, such as e-mail messages, instant messages, and chats. Under the current prevailing view, this definition is purposefully broad to cover any user-generated content, and providers would qualify as Information Distributors. Earlier, before ceasing their activity in Russia, such players as Google (email service Gmail, social networking service Google+), Microsoft (instant messages Outlook, and voice-over-IP services Microsoft Lync), Meta/Facebook (private messages, discussion boards), and X/Twitter (social network) were qualified as Information Distributors.

One can conclude that the idea of these provisions of Information Law is to ensure that the relevant information is kept in the territory of the Russian Federation in order to allow the Russian law enforcement agencies to gain access to this data within a certain period of time. This is necessary for the investigation of different types of crimes, specifically related to cyberspace, terrorist activities, illegal trafficking of human organs and child abuse.

[37] FSB is the Federal Security Service of the Russian Federation.

[38] *See* e.g.: Digital Services Act.

The Information Law does not prohibit the transmission of electronic messages outside Russia, including the use of foreign clouds to proceed with the relevant services (email services, instant massages, social networks, etc.). However, the law imposes a retention obligation so that electronic messages remain available and accessible in Russia after being transferred. It also requires the Information Distributor's equipment and software to be designed in such a way as to allow an easy access by the law enforcement and security authorities, namely the FSB.

V. Conclusion

Currently, there are certain restrictions and difficulties for the Big Tech companies in providing their social networking services in Russia. The first one is the lack of statutory regulation in this sphere and this circumstance does not allow players in this market to effectively predict all legal consequences of using their social platforms. The second impediment is the strict Personal Data Law rules that are not designed to regulate social networking services. This obstacle also restricts the use of public cloud solutions provided by Big Tech companies. The Russian Government needs to enact and implement some general guidance regarding the use of public social platforms. Such guidance could be created based on the respective foreign practice. Specifically, it would be beneficial if the DSA rules were accepted as binding in cross-border relations between the EU and Russia.

Based on the analysis of the current regulation of the Internet industry, we can conclude that foreign providers, including Big Tech companies, may provide Russian customers and users with social networking services, provided that certain conditions are met. Firstly, they must abide by Russian law and delete or restrict access to information that contains illegal content, such as child pornography and extremist activity. Secondly, they should take measures to protect sensitive information, such as the personal data of Russian citizens. Finally, it is much more beneficial to cooperate with local regulators rather than arguing with them.

References

FRA, (2017). Data retention across the EU. *FRA*, 13 July 2017. Available at: https://fra.europa.eu/en/publication/2017/data-retention-across-eu#publication-tab-0 [Accessed 18.02.2024].

Daxton, R., (2017). "Chip" Stewart. In: Srewart, D., (2017). *Social Media and the Law. A Guidebook for Communication Students and Professionals*. New York: Routledge.

Goujard, C. and Stolton, S., (2021). Europe reins in Big Tech: What you need to know. *Politico*, 25 November 2021. Available at: https://www.politico.eu/article/europe-digital-markets-act-dma-digital-services-act-dsa-regulation-platforms-google-amazon-facebook-apple-microsoft/ [Accessed 10.01.2022].

Hadebe, S., (2022). Digital Sovereignty and Tight Regulation in the EU: Analysing the motivation behind the Digital Markets Act. 30 April 2022. Available at: https://ssrn.com/abstract=4785054 [Accessed 14.06.2022].

Henderson, J., (2017). New Boundaries of Free Speech in Social Media. In: Srewart, D., (2017). *Social Media and the Law. A Guidebook for Communication Students and Professionals*. New York: Routledge.

Ivanov, E., (2023). Data Building: Who and How to Build Data Processing Centers. Stroimprosto, 26 April 2023. Available at: https://stroimprosto-msk.ru/publications/data_stroitelstvo-kto-i-kak-stroit-centry-obrabotki-dannyh/ [Accessed 18.02.2024]. (In Russ.).

Kommersant, (2021). Google Pays Fine of RUB 8,5 Million. *Kommersant*, 30 December 2021. Available at: https://www.kommersant.ru/doc/5155054 [Accessed 06.02.2024]. (In Russ.).

Mironenko, V., (2024). Google and Meta Have Paid in Full Their Multibillion Fines to the Russian Budget. *3DNews*, 2 January 2024. Available at: https://3dnews.ru/1098251/google-i-meta-polnostyu-vi-platili-mnogomilliardnie-oborotnie-shtrafi-v-rossiyskuyu-kaznu [Accessed 10.02.2024]. (In Russ.).

Moore, M. and Tambini, D., (2022). *Regulating Big Tech: Policy Responses to Digital Dominance*. New York: Oxford University Press.

Penfrat, J., (2020). The EU's attempt to regulate Big Tech: What it brings and what is missing. *European Digital Rights (EDRi)*,

18 December 2020. Available at: https://edri.org/our-work/eu-attempt-to-regulate-big-tech/ [Accessed 06.02.2024].

Penfrat, J., (2021). Delete first, think later. *European Digital Rights (EDRi)*, 24 March 2021. Available at: https://edri.org/our-work/delete-first-think-later-dsa/ [Accessed 05.02.2024].

Stepanova, J., (2021). Content has Took a New Turn. *Kommersant*, 24 December 2021. Available at: https://www.kommersant.ru/doc/5152095 [Accessed 06.02.2024]. (In Russ.).

Saveliev, A., (2021). *Scientific and Practical Commentary on the Personal Data Law*. 2nd edition. Moscow: Statut Publ. (In Russ.).

Trushina, N., (2021). Google Might Leave Russia After Imposition of Multibillion Fines. *MK.RU,* 24 December 2021. Available at: https://www.mk.ru/economics/2021/12/24/posle-milliardnogo-shtrafa-google-zagovorili-o-ego-ukhode-iz-Rossii.html [Accessed 06.02.2024]. (In Russ.).

Information about the Author

Vladimir A. Kanashevskiy, Dr. Sci. (Law), Professor, Head of the Department of Private International Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

vakanashevskij@msal.ru

ORCID: 0009-0009-9369-5158