



Regulation of social media in Russia

IRIS *Extra*

A publication
of the European Audiovisual Observatory



IRIS Extra 2021

Regulation of social media in Russia

European Audiovisual Observatory, Strasbourg, 2021

ISSN 2079 - 1062

Director of publication – Susanne Nikoltchev, Executive Director

Editorial supervision – Maja Cappello, Head of Department for Legal Information

Editorial team – Francisco Javier Cabrera Blázquez, Sophie Valais, Legal analysts
European Audiovisual Observatory

Author

Andrei Richter

Translation

Erwin Rohwer, Nathalie Sturlèse

Proofreading

Anthony Mills, Udo Lücke, Aurélie Courtinat

Editorial assistant – Sabine Bouajaja

Press and Public Relations – Alison Hindhaugh, alison.hindhaugh@coe.int

European Audiovisual Observatory

Publisher

European Audiovisual Observatory

76, allée de la Robertsau, 67000 Strasbourg, France

Tel.: +33 (0)3 90 21 60 00

Fax: +33 (0)3 90 21 60 19

iris.obs@coe.int

www.obs.coe.int

Cover layout – ALTRAN, France

Please quote this publication as:

Richter A., *Regulation of social media in Russia*, IRIS Extra, European Audiovisual Observatory, Strasbourg, September 2021

© European Audiovisual Observatory (Council of Europe), Strasbourg, 2021

Opinions expressed in this publication are personal and do not necessarily represent the views of the Observatory, its members or the Council of Europe.

Regulation of social media in Russia

Andrei Richter, Comenius University in Bratislava



Foreword

In 2015, we published an IRIS *Extra* titled “Regulation of online content in the Russian Federation”, in which the authors analysed the most recent developments in this regard. Needless to say, much water has flowed under the Internet bridge since then, and especially social media have become one of the main forums for critical public debate in Russia. The present report looks into the pace of the intensifying response of public authorities, which has taken place mostly since the adoption of the 2017 Development Strategy of the Information Society, through legal regulation of social networks in the Russian Federation. Its aim, according to the Strategy, is to counteract “imposed patterns of behaviour” so as not to give an advantage to technologically more advanced organisations as they seek to achieve their perceived “political goals” in the information sphere.

This publication does not, however, examine certain issues related to regulation of social networks, such as copyright violations, defamation on social networks, privacy rights (including children’s privacy), competition and monopolisation, and issues related to anonymity or use of a false identity on social networks.

Author Andrei Richter, Professor Researcher of the School of Philosophy at the Comenius University, Bratislava, begins with essential background reading on the Russian Development Strategy of the Information Society, introduced in May 2017. **The first chapter** examines access to and penetration of social networks in Russia. This chapter also explores restrictions on the use of social media by certain actors. **The second chapter** details the legal grounds for sanctioning social networks in Russia. All social media platforms available in Russia must store the contact data of Russian users on servers geographically located in Russia. A second rule considers all social media operating from outside Russia as “foreign agents”. **The third chapter** examines how Russian legislation deals with illegal content published on social media platforms. The Russian “IT law” includes blacklisting and blocking mechanisms for sites publishing illegal content, on the one hand, and further dispositions which allow identification of the different categories of illegal information, on the other. **The fourth chapter** dives into more recent attempts in Russia to make social media platforms more responsible via self-regulation and **the fifth chapter** provides an overview of current Russian case law in this field. In **the sixth chapter** the author moves on to the most recent development, dating from July 2021: the law on “grounding foreign IT companies”.

Rounding up, the author concludes that regulation of social media platforms operating in Russia is a very recent phenomenon, its main aim being to ensure quick compliance with federal legislation and regulations, particularly concerning illegal content.

Strasbourg, September 2021

Maja Cappello

IRIS Coordinator

Head of the Department for Legal Information

European Audiovisual Observatory

Table of contents

1. Introduction	1
2. Access to, and penetration of, social networks	4
2.1. Popular social networks	4
2.2. “Socially meaningful” social media	5
2.3. Restrictions on the use of social media by certain actors	7
3. Legal grounds to sanction social networks	9
3.1. Improper storage of users' data	9
3.2. Lack of “foreign agent media” imprint	11
3.3. Sanctions over restrictions of freedom of the Russian media	12
4. Illegal content	15
4.1. Mechanisms to identify and block content	15
4.2. “Law on Fake News” and social media	16
4.3. Fines for a failure to delete prohibited materials	17
5. Law “on self-regulation of social media”	19
6. Case law of the Supreme Court of Russia	23
7. Law on “grounding foreign IT companies” as new compliance mechanism	25
8. Conclusion	27

Figure

Figure 1. Popularity of social networks in the Russian Federation..... 4

1. Introduction

Recommendation CM/Rec(2016)5 on Internet freedom,¹ adopted by the Committee of Ministers of the Council of Europe, recommended to member States of this organization that they be guided by, and promote specific Internet freedom indicators when participating in international dialogue and international policy-making on Internet freedom. Section 2.2 of the Internet freedom indicators, “Freedom of opinion and the right to receive and impart information”, reads, in particular:

2.2.1. Any measure taken by State authorities or private-sector actors to block or otherwise restrict access to an entire Internet platform (social media, social networks, blogs or any other website) or information and communication technologies (ICT) tools (instant messaging or other applications), or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

When adopting this recommendation, the Permanent Representative of the Russian Federation indicated that he reserved the right of his Government to comply or not with the recommendation, in so far as it referred to the methodology for its implementation at the national level.²

The Russian approach to regulating popular social networks is best exemplified in its Development Strategy of the Information Society, approved on 9 May 2017 by a Decree of the President of the Russian Federation Vladimir Putin (the “2017 Development Strategy”). Such strategies generally outline political aims for public authorities and means to achieve them, including legal instruments. Unlike its “predecessor,” the 2008 Development Strategy,³ the 2017 Development Strategy pays some – although still minor – attention to the place and role of social networks in Russia’s modern information society.⁴ The Strategy mentions that social networks have become part of the everyday life of Russians (para 7). The Strategy also refers to social networks when listing some 20

¹ Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers’ Deputies), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

² https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa#_ftn1.

³ Стратегия развития информационного общества в Российской Федерации (Development Strategy of Information Society in the Russian Federation), 7 February 2008, approved by an order of the President of the Russian Federation N Pr-212, <https://rg.ru/2008/02/16/informacia-strategia-dok.html>.

⁴ Указ Президента Российской Федерации “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” (Decree of the President of the Russian Federation “On Development Strategy of Information Society in the Russian Federation in 2017-2030”), 9 May 2017, N 203, <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102431687>.

instruments to facilitate the forthcoming “information society based on knowledge” (para 26). It calls for improvement to instruments of legal regulation for both the mass media, and “the means of access to information, which by many criteria could be attributed to the mass media, but are not those *per se* (Internet television, news aggregators, social networks, sites on the Internet, instant messengers)”.

Otherwise, the overall priority in the document is given to traditional Russian spiritual and moral values and the observance of norms of behaviour based on these values when employing information and communication technologies – these values can be found among the principles laid down in the Strategy. The pace of technology, explains the Strategy, “has significantly exceeded the possibilities of most people in learning and making use of knowledge”. The focus of Russians in the world outlook has thus been shifted from science, education and culture, to entertainment, characteristic of the “massive superficial perception of information”. This form of information consumption “contributes to the formation of imposed patterns of behaviour that gives an advantage in achieving economic and political goals to those States and organizations that own the technology for dissemination of information” (para 16).

In 2017, when the Strategy was adopted, according to the Yuri Levada Analytical Center, a Russian non-governmental research organization that conducts regular monitoring of public opinion, as many as 35% of Russians used social networks daily or almost every day. By 2021 their number had increased 1.5 times to 57 %. The number of those who do not use social networks at all in Russia dropped in approximately the same proportion – from 41% in 2017 to 26% in 2021. In 2021, those claiming that social networks provide the most often used source of news, took second place among all Russians (42%), while those mostly relying on television news still led with 64 %.⁵

Russian officials refer to even higher penetration figures⁶ of 124 million Internet users in the country with Internet penetration at 85% in January 2021. At the same time, there were 99 million social media users in Russia or 67.8 % of the total population. Between 2020 and 2021, the number of social media users in the country increased by 4.8 million, or 5.1%⁷ (while globally the increase was 13.2 %)⁸. These higher figures may be explained by the inclusion of messaging platforms in the category of social media.

Social media have become one of the main forums for critical public debate in Russia.⁹ This *IRIS Extra* report will look into the pace of the intensifying response of public authorities, which has taken place mostly since the adoption of the 2017 Development

⁵ Levada-Center, Social Networks in Russia, 25 February 2021, <https://www.levada.ru/en/2021/02/25/social-networks-in-russia/>.

⁶ Andrei Lipov, head of Roskomnadzor, in an interview with the Kommersant daily, “Владелец забора отвечает за то, что на нем написано” (“The owner of a fence is responsible for what is inscribed there”, 25 May 2021, p.10, <https://www.kommersant.ru/doc/4826455>).

⁷ Kemp S., *Digital 2021: The Russian Federation*, 11 February 2021, <https://datareportal.com/reports/digital-2021-russian-federation?rq=Russia>.

⁸ Kemp S., *Digital 2021: Global Overview Report*, 27 January 2021, <https://datareportal.com/reports/digital-2021-global-overview-report>.

⁹ “Russia: Social Media Pressured to Censor Posts,” Human Rights Watch, 5 February 2021, <https://www.hrw.org/news/2021/02/05/russia-social-media-pressured-censor-posts>.



Strategy through legal regulation of social networks in the Russian Federation. Its aim, according to the Strategy, is to counteract “imposed patterns of behaviour” so as not to give an advantage to the technologically more advanced organizations in achieving their perceived “political goals” in the information sphere.

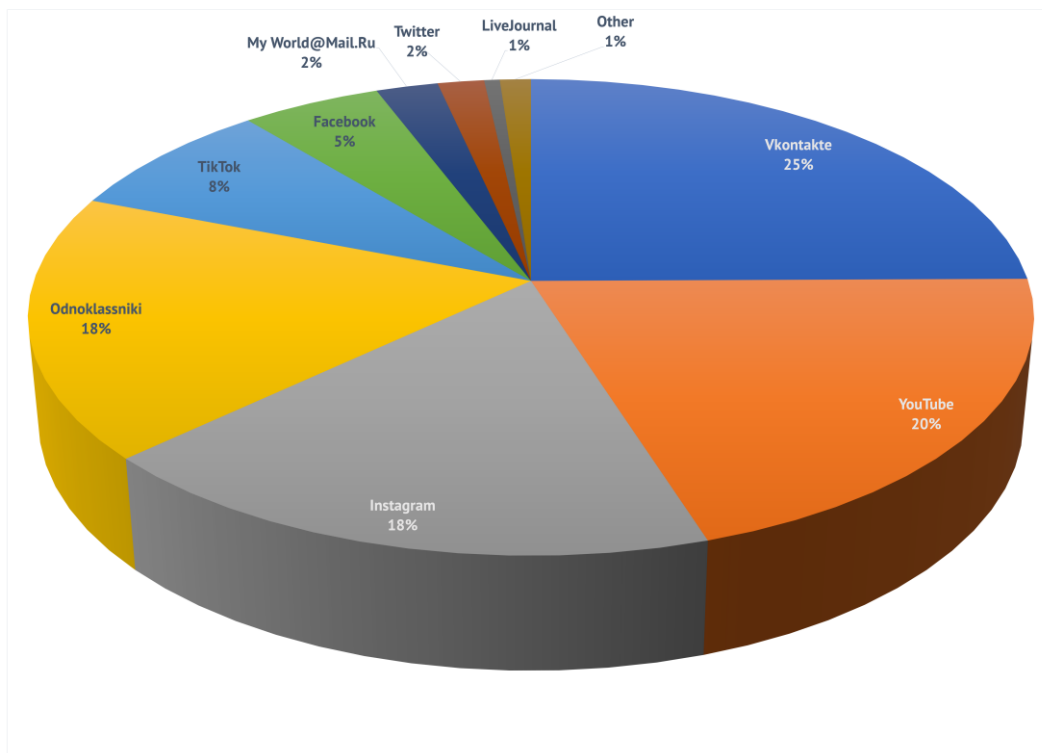
This publication does not look into certain issues of regulation of social networks such as copyright violations, defamation on social networks, privacy rights (including children’s privacy), competition and monopolization, issues related to anonymity or use of a false identity on social networks.

2. Access to, and penetration of, social networks

2.1. Popular social networks

Due to historic and linguistic reasons, Russian social media still occupy a leading position in the country (as well as, for that matter, in many other post-Soviet countries). The Levada Center provides the following popularity ratings for social networks:

Figure 1. Popularity of social networks in the Russian Federation



Source: Levada Center

The popularity trends show a steady increase of the share of Vkontakte, YouTube and Instagram, a big jump for TikTok at the expense of Odnoklassniki, and a stagnation for Facebook.¹⁰

¹⁰ Levada-Center, op.cit. The report by Simon Kemp lists largely the same 'most popular' networks, although in his list the leader is YouTube, see Kemp S., *Digital 2021: The Russian Federation*, op.cit.

Three of the four Russian social networks from the top 10 list – Vkontakte, Odnoklassniki and My World@Mail.Ru – fully belong to one company, Mail.ru Group Limited, registered in Limassol, Cyprus.¹¹

The fourth, LiveJournal (or, in Russian, Zhivoi Zhurnal – ZhZh), “willfully blurring the lines between blogging and social networking”,¹² belongs to the Rambler Group. Since 2020, Rambler has been fully owned by Sberbank, controlled by the Government of Russia.¹³

2.2. “Socially meaningful” social media

These four major Russian social networks entered a special list of national “socially meaningful” online media resources that was compiled by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (henceforth referred to as Ministry of Communications) following the 2020 Address of the President of the Russian Federation to the Federal Assembly.¹⁴ The list originally appeared to illustrate the voluntary initiative of the five major telecoms in providing non-billed traffic¹⁵ to private citizens when certain online services and websites are accessed (with the exception of satellite service access), including governmental ones. The “big five” provide Internet service to some 70 percent of all Russian households.

Aside from the need to implement tasks set by the President in his annual address, it was presented as a three-month “experiment” necessary, under the tough economic conditions of the COVID-19 pandemic, to provide “information support” to the citizens.¹⁶ Later in 2020, the list was expanded to 371 online media, and this “accessible Internet” initiative was supported by other ISPs and twice extended by the Ministry of Communications. Reportedly, the experiment was found successful, as 1.8 million users became customers of the free service in 2020 alone.¹⁷

¹¹ “Mail.ru Group Limited: Interim Condensed Consolidated Financial Statements for the Three Months Ending March 31, 2021”, <https://corp.imgsmail.ru/media/files/mail.rugroupifrsq12021.pdf>.

¹² About LiveJournal, <https://www.livejournal.com/about/>.

¹³ Sberbank, “Sber increases its share in Rambler Group to 100 percent” (Сбер увеличивает долю в Rambler Group до 100%), Press release, 29 October 2020, https://www.sberbank.ru/ru/press_center/all/article?newsID=25343e79-febb-4c32-aba7-25018563eaa1&blockID=1303®ionID=77&lang=ru&type=NEWS.

¹⁴ Address of the President to the Federal Assembly (Послание Президента Федеральному Собранию), 15 January 2020, <http://kremlin.ru/events/president/news/62582>.

¹⁵ Non-billed traffic is traffic that goes beyond fixed-fare plans for Internet access according to pre-defined thresholds of MB.

¹⁶ Roskomnadzor, “List of socially meaningful information resources in the IT network Internet” (Перечень социально значимых информационных ресурсов в информационно-телекоммуникационной сети «Интернет»), <https://digital.gov.ru/ru/documents/7146/>, as approved by the Ordinance of the Ministry of Digital Development, Communications and Mass Communications N148 of 31 March 2020, <https://digital.gov.ru/uploaded/files/prikaz-148-gv.pdf>.

¹⁷ Interfax news agency, “Experiment on ‘accessible Internet’, extended for half-year (Эксперимент по “доступному интернету” продлили на полгода), 30 December 2020, <https://www.interfax.ru/russia/743675>.

The Government has not explained yet how and if it will offset the cost of the project to the private telecoms.¹⁸ Moreover, it introduced an amendment to the Statute “On Communications”, which – for the above-mentioned reasons – makes this “voluntary initiative” part of federal law (Article 46, part 5-3).¹⁹ In the summer of 2021 the amendment was adopted by the State Duma and enforced by the President.²⁰

The Government conducted another “successful experiment”, which lasted from 10 March to 15 May 2021. Twitter was chosen by the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Communications (henceforth referred to as Roskomnadzor), the governmental watchdog in the sphere of media and telecoms, to test its new “technical means of counteracting threats”²¹ (TSPU). The TSPU were applied to slow down Twitter’s traffic for a failure to comply with demands on the removal of user content prohibited in Russia. It affected access to Twitter on fixed networks, and on related Wi-Fi networks, as well as access from mobile devices. Its start was marred by a massive slow-down, by mistake, of numerous other websites, including those of governmental agencies.

According to Roskomnadzor,²² by the time the slow-down ended, Twitter removed all but 563 of some 5 900 tweets with information banned in Russia, i.e. “with child pornography, narcotic and suicidal content, calls for minors to participate in unauthorised mass events.” Therefore, in appreciation of the efforts to comply, the slow-down was partly removed, leaving it in place only on mobile devices. This announcement ended with a warning to Facebook and YouTube that they might be next to fall under similar sanctions.²³

The developments with regard to freedom of access to foreign social networks in Russia should be understood in the context of the “Sovereign Internet Law” which entered into force in November 2019.²⁴ It is formally aimed at ensuring that the Russian portion of the Internet, the so-called *Runet*, can function independently of the global Internet in the event of certain threats, while providing to the public authorities technical possibilities necessary to effectively restrict access to certain online services and content.²⁵

Such threats are defined by the Government and include “a threat of providing access to online information or information resources, access to which must be restricted

¹⁸ Interfax news agency, “Ministry of Communications will not compensate operators’ losses from ‘accessible Internet’ (Минцифры не возместит операторам потери от “доступного интернета”), 21 September 2020, <https://www.interfax.ru/russia/727895>.

¹⁹ On amendments to the Federal Statute “On Communication” (О внесении изменений в Федеральный закон «О связи»), draft bill N 1087071-7 of 29 December 2020, <https://sozd.duma.gov.ru/bill/1087071-7>.

²⁰ Federal Statute “On amendments to the Federal Statute “On Communication”” (О внесении изменений в Федеральный закон «О связи»), N 319-FZ of 2 July 2021, <http://publication.pravo.gov.ru/Document/View/0001202107020019>.

²¹ Andrei Lipov, op.cit.

²² Roskomnadzor, “On partial removal of measures to slow down traffic of Twitter” (О частичном снятии мер по замедлению трафика Twitter), Press release, 17 May 2021, <https://rkn.gov.ru/news/rsoc/news73632.htm>.

²³ Ibid.

²⁴ <http://merlin.obs.coe.int/article/8603>.

²⁵ Freedom House, “Freedom on the Net”, 2020, Russia, https://freedomhouse.org/country/russia/freedom-net/2020#footnote12_g9flt86.

in accordance with the legislation of the Russian Federation,” and “a threat of countering (making difficult) efforts to restrict access” to such information.²⁶

The Russian sovereign Internet infrastructure relies on hardware called “Red Boxes”, installed at ISPs, Internet exchange points, and operators throughout the country. The boxes connect to the Control Command Centre in Moscow and allow those in command to remotely slow down traffic, block access, or redirect online information flows in any region of Russia.²⁷

2.3. Restrictions on the use of social media by certain actors

Recent regulations introduced by the Russian authorities point to concerns that information of a sensitive nature to them was willingly shared in the social networks by civil and military servants.

In 2016, the State Duma adopted amendments to the federal statutes “On the state civil service of the Russian Federation” and “On municipal service in the Russian Federation,” which relate to the use by state and municipal servants of social media and other websites and/or webpages that may identify them.²⁸

The new norms demand from civil (municipal) servants and applicants to the positions of such servants that they provide their employers with information on the addresses of the websites and webpages where they post information that is publicly accessible, and data that enables their identification.

Such information is provided by the servants annually, while applicants submit it for a three-year period prior to the year of their applications. By a decision of the employer, certain staff members may be authorized to verify the data submitted, as well as to “process” the information on the websites and webpages posted by the civil/municipal servants and/or applicants.²⁹

The Russian Ministry of Labour has published guidelines and a standard form for filing information as required by the above norms. The guidelines explain, in particular, that the sites and/or webpages to be included in the self-reports are personal pages of social

²⁶ On approval of the Rules of centralized command of the communication network of general use (Об утверждении Правил централизованного управления сетью связи общего пользования), Ordinance of the Government of the Russian Federation of 12 February 2020 N 127,

<http://publication.pravo.gov.ru/Document/View/0001202002170013?index=0&rangeSize=1>.

²⁷ Irina Borogan, “Russia’s ‘Red Boxes’ Menace the Internet”, Center for European Policy Analysis, 4 June 2021, <https://cepa.org/russias-red-boxes-menace-the-internet/?fbclid=IwAR1FW9s92B5XfllF6s1doSjXPuEln7muuSuXdqLqV90nnD9sTtAmuyUcRDo>

²⁸ <http://merlin.obs.coe.int/article/7706>.

²⁹ “On amendments to the Federal Statute ‘On the state civil service of the Russian Federation’ and to the Federal Statute ‘On municipal service in the Russian Federation’ (О внесении изменений в Федеральный закон “О государственной гражданской службе Российской Федерации” и Федеральный закон “О муниципальной службе в Российской Федерации”), 30 June 2016 N 224-FZ, <https://rg.ru/2016/07/04/municipal-dok.html>.

networks, as well as blogs, microblogs, and personal sites.³⁰ Actually, a sample form for such a self-reporting process report, published on the official website of the Supreme Court of Russia, referred to sample accounts on social media only: Odnoklassniki, Vkontakte and Instagram.³¹

In 2017 similar rules were approved for the civil servants in the court system.³²

In 2019 even broader restrictions were promulgated for military servicemen and civilians on army reserve duty. They were prohibited from disseminating – in mass media and online – not just state, but any other protected secrets, as well as various other types of information related to military matters, such as information on their daily activities. They were also barred to be in the possession of electronic devices that allow to store, disseminate or provide access to audio-, video- or photo information, as well as to their geo-location.³³

³⁰ Ministry of Labour of the Russian Federation, “Guidelines on filling out the form for submitting information about site addresses and/or pages of sites in the information and telecommunication network ‘Internet’, wherein publicly available information was posted by a state civil servant or municipal employee, a citizen of the Russian Federation, applying to a position of the state civil service of the Russian Federation or municipal service, as well as data allowing them to be identified (Методические рекомендации по заполнению формы представления сведений об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых государственным гражданским служащим или муниципальным служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации или муниципальной службы, размещались общедоступная информация, а также данные, позволяющие его идентифицировать), undated 2017), <https://docs.cntd.ru/document/456045861>.

³¹ <http://www.supcourt.ru/files/15866/>.

³² Judicial Department at the Supreme Court of the Russian Federation, “On approval of the Regulations on the procedure for submission by citizens applying for positions of the federal state civil service in the Judicial Department at the Supreme Court of the Russian Federation, and by federal state civil servants filling the positions of the federal state civil service in the Judicial Department under the Supreme Court of the Russian Federation, of information on the placement of information in the information and telecommunication network “Internet”, processing of the specified information and verification of its reliability and completeness (Об утверждении Положения о порядке представления гражданами, претендующими на замещение должностей федеральной государственной гражданской службы в Судебном департаменте при Верховном Суде Российской Федерации, и федеральными государственными гражданскими служащими, замещающими должности федеральной государственной гражданской службы в Судебном департаменте при Верховном Суде Российской Федерации, сведений о размещении информации в информационно-телекоммуникационной сети “Интернет”, обработке указанных сведений и проверке их достоверности и полноты). Order of 18 July 2017 N 133 (as amended on 31 July 2019), https://sudact.ru/law/prikaz-sudebnogo-departamenta-pri-verkhovnom-sude-rf_330/.

³³ Federal Statute On the status of military servicemen (О статусе военнослужащих), 27 May 1998 N 76-FZ, Art. 7, <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102053139>.

3. Legal grounds to sanction social networks

There are certain grounds to sanction social networks in Russia that are not related to their content.

3.1. Improper storage of users' data

In 2014, President Vladimir Putin signed into law a federal statute that amended, in particular, Article 18 of the Federal Statute “On Personal Data”.³⁴ The focus of the change was the demand that all Internet service providers be responsible for collecting, processing, and storing personal data of the citizens of the Russian Federation in databases (servers) which are located on the territory of Russia.

This rule affected foreign social networks, once Roskomnadzor, with its staff of some 8,000 including 100 software experts,³⁵ started to monitor if the location of the processing of personal data of the Russians indeed fell under its jurisdiction. A violation of this rule became yet another instance when Roskomnadzor, which is in addition authorised to control protection of the rights of subjects of personal data, shall block access to online resources.

This amendment entered into force on 1 September 2016. Prior to that, all major global professional social networks were approached by Roskomnadzor with demands to follow the new provision of the law. Some started to negotiate and collaborate, while LinkedIn apparently refused to enter such negotiations. Its ban happened after the Moscow City Court upheld an earlier court decision taken upon a claim by Roskomnadzor which accused LinkedIn of failing to comply with the legal requirement on data storage of some six million of its users in Russia.³⁶ The court of first instance granted Roskomnadzor permission to effectively block online access to the LinkedIn websites and services at linkedin.com.

The court of second instance found no reasons to uphold the appeal of LinkedIn Corp. It confirmed that the plaintiff violated “the rights and legitimate interests of the citizens of the Russian Federation as subjects of personal data by collecting information on the users of the website as well as on other citizens of the Russian Federation who are not its users, by processing these data and by their dissemination, including via the website in question, without necessary permissions as well as in violation of the law of the Russian

³⁴ Federal Statute On personal data (О персональных данных), 27 July 2006 N 152-FZ, <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261>, see <http://merlin.obs.coe.int/article/7020>.

³⁵ Andrei Lipov, op.cit.

³⁶ Elena Gorelova, “After blocking LinkedIn, the prestige of the social networks in the eyes of employers has only risen” (После блокировки LinkedIn престиж соцсети в глазах работодателей вырос), Vedomosti daily, 22 November 2016, <https://www.vedomosti.ru/management/articles/2016/11/23/666511-linkedin-prestizh>

Federation in the field of personal data”.³⁷ Despite the blocking that followed, LinkedIn still claims to have seven million users in Russia today.³⁸

Other major foreign social networks failed to comply as well: Facebook and Twitter were given repeated deadlines to localize the personal data.³⁹ In 2019 (the most recent year for which data are available) Roskomnadzor reported 9,159 complaints it had received regarding all sorts of abuses of personal data by “owners of Internet resources, including owners of social networks”, up from 999 complaints in 2018.⁴⁰

Recently, Russian authorities appear to have chosen the policy of imposing financial penalties instead of blocking social networks. One reason could be the repeated failed attempts by Roskomnadzor in 2018-2020 to block access in Russia to Telegram, a popular messaging platform, as well as the public protests that followed these attempts. Telegram was launched by the Russian-born entrepreneur Pavel Durov after the social network Vkontakte, created and once led by him, became the subject of a hostile takeover, while he fled Russia.⁴¹ The shift in policy to avoid blocking was also likely encouraged by a chain of judgments in 2020 by the European Court of Human Rights, wherein such measures were found to be in violation of Article 10 of the Convention on Human Rights.⁴² But as early as 2019, the then head of Roskomnadzor called for rather “eating the elephant one bite at a time”.⁴³ Soon thereafter the State Duma amended the Code on Administrative Offences to establish significant fines for violations of the personal data regulation, as set out by above-referenced Article 18 of the Federal Statute “On Personal Data”. The fines now range from RUB 1 to 6 million⁴⁴ for legal entities which commit a first offence, and from RUB 6 to 18 million for repeated offences. Moreover, those who commit the offences without establishing a legal entity (in Russia) face the same penalty.⁴⁵

³⁷ Decision by the Tagansky District Court on case 02-3491/2016, 4 August 2016 <http://docs.pravo.ru/document/view/87232058/>; Appeals Decision by the Judicial Collegium on Civil Cases of the Moscow City Court on case 33-38783/16, 10 November 2016, <http://www.mos-gorsud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a>. <http://merlin.obs.coe.int/article/7805>.

³⁸ Kemp S., *Digital 2021: The Russian Federation*, op.cit.

³⁹ Interfax news agency, “Roskomnadzor will demand from Facebook and Twitter that they localize data of users from RF (Роскомнадзор потребует от Facebook и Twitter за 9 месяцев локализовать данные пользователей РФ)”, 12 February 2019, <https://www.interfax.ru/russia/650240>.

⁴⁰ Roskomnadzor, Activity Report of the Authority on Protection of the Rights of Subjects of Personal Data in 2019 (Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2019 год), Moscow, 2020, p. 8, https://rkn.gov.ru/docs/Otchet_UO-2019_new.pdf.

⁴¹ Myles-Primakoff D. and Sherman J., “Russia Can’t Afford to Block Twitter - Yet, Foreign Policy”, 30 April 2021, <https://foreignpolicy.com/2021/04/30/russia-block-twitter-telegram-online-censorship/>.

⁴² *Engels v. Russia* op.cit.; *OOO Flavus and Others v. Russia* (Applications nos. 12468/15 and 2 others), 23 June 2020, <http://hudoc.echr.coe.int/eng?i=001-203178>; *Vladimir Kharitonov v. Russia* (Application no. 10795/14), 23 June 2020, <http://hudoc.echr.coe.int/eng?i=001-203177>.

⁴³ RBK news portal, “Head of Roskomnadzor, in reply to a question on possible blocking of Facebook, suggested ‘eating the elephant one bite at a time’” (Глава Роскомнадзора в ответ на вопрос о возможной блокировке Facebook предложил «есть слона по частям»), 16 April 2019, https://www.rbc.ru/technology_and_media/16/04/2019/5cb5b4659a79471da70386bc.

⁴⁴ At the time of writing, 1 Euro equals 87 RUB.

⁴⁵ Paras 8 and 9 of Article 13.11 of the Code on Administrative Offences of the Russian Federation (introduced on 2 December 2019 by Federal Statute N 405-FZ). Earlier, social media were fined for the “failure to provide

They have been implemented in practice. In February 2020 Facebook and Twitter were fined RUB 4 million each, and after failed appeals, Facebook paid the fine in November 2020; at the time of writing, Twitter has not yet paid the fine. The latest “ultimatum” by Roskomnadzor handed to these and other foreign social networks has been in regard to localisation of the personal data by 1 July 2021, or the threat of fines for repeat offences.⁴⁶ Indeed, in August 2021, WhatsApp was fined RUB 4 million, while “repeated violators” Facebook and Twitter – RUB 15 and 17 million.⁴⁷ It appears that Roskomnadzor intends to add to the current regulation of personal data location a measure that would force online media companies to store in Russia copies of their “software libraries” to facilitate effective control of them.⁴⁸

3.2. Lack of “foreign agent media” imprint

Social media fall, at least in part, under the regulation of the “foreign agent” legislation in Russia.⁴⁹ Under requirements adopted in 2019, all foreign media that perform the functions of a foreign agent as well as registered media outlets founded with participation of a Russian legal entity, which perform the functions of a foreign agent, shall contain an imprint when disseminated in Russian territory. The imprint, approved by Roskomnadzor, says (in Russian):

The following story (material) is produced and/or distributed by the foreign mass media outlet that performs the functions of a foreign agent, and/or by the Russian legal entity that performs the functions of a foreign agent.

In social media (including Twitter!), this imprint must always be in text form. The size of the font used for the imprint must be twice the size of the font used for the post/message or the story itself; the colour of the font must be in sharp contrast to the background; and the imprint must immediately follow the headline of the post or story, or – if there is no

information” (on transfer of personal data to Russia) to the public authorities, and the fine amounted to a mere 3 000-5 000 RUB for legal entities (Article 19.7 of the Code on Administrative Offences).

⁴⁶ Interfax news agency, “Facebook and Twitter are to localize the data of users in RF by 1 July” (Facebook и Twitter обязаны локализовать до 1 июля базы данных пользователей в РФ), 26 May 2021, <https://www.interfax-russia.ru/main/facebook-i-twitter-obyazany-lokalizovat-do-1-iyulya-bazy-dannyh-polzovateley-v-rf>.

⁴⁷ Roskomnadzor, “Court fined Facebook, `Twitter and ~WhatsApp RUB 36 million for non-localization of databases of Russian users in the territory of the RF” (Суд оштрафовал Facebook, Twitter и WhatsApp на 36 млн рублей за нелокализацию баз данных российских пользователей на территории РФ), Press release, 26 August 2021, <https://rkn.gov.ru/news/rsoc/news73828.htm>.

⁴⁸ Ibid.

⁴⁹ See Richter A., “Foreign agents” in Russian media law, IRIS Extra, European Audiovisual Observatory, Strasbourg, December 2020, <https://rm.coe.int/iris-extra-2020en-foreign-agents-in-russian-media-law/1680a0cd08>.

headline –must precede the story. Such a warning must accompany every story by the “foreign agent” media outlet.⁵⁰

Currently there are 20 legal and physical entities in the list of “media performing as foreign agents” operated by the Ministry of Justice of the Russian Federation.⁵¹ They are themselves responsible for labeling their official accounts in the social networks, while posting the reference to the “foreign agent” origin of materials of “foreign agent” NGOs, individuals – “foreign agents,” or public associations. “Foreign agents” that have not registered a legal entity remain the responsibility of the individuals who post or repost their materials in the social networks.

3.3. Sanctions over restrictions of freedom of the Russian media

At the very end of 2020, a set of amendments expanded the scope of the Federal Statute “On measures to influence persons involved in violations of fundamental human rights and freedoms, the rights and freedoms of citizens of the Russian Federation” (or “Dima Yakovlev Statute”).⁵² They allow the blocking of access to online resources owned by entities officially designated as being involved in such violations. Such a designation comes from the Prosecutor General (or his deputies) upon consent from the Ministry of Foreign Affairs. The violations recognised by the adopted amendments include “limitations” to the online dissemination of information in Russian or in other languages of the Russian Federation which is “essential for the public,” including materials of the Russian mass media, if such limitations discriminate on the basis of, for example, their property status, or are the result of sanctions imposed by foreign governments upon the Russian Federation, Russian citizens or Russian companies.⁵³ The nature of the “limitations” has not been defined in the law, but the administrative practice of Roskomnadzor points to the instances of marking the source

⁵⁰ Roskomnadzor, “On approval of the form indicating that messages and materials of a foreign mass media performing the functions of a foreign agent, and (or) a Russian legal entity performing the functions of a foreign agent, distributed on the territory of the Russian Federation, created and (or) distributed by the specified persons, as well as the requirements and procedure for placing such instructions” (Об утверждении формы указания на то, что сообщения и материалы иностранного средства массовой информации, выполняющего функции иностранного агента, и (или) российского юридического лица, выполняющего функции иностранного агента, распространяемые на территории Российской Федерации, созданы и (или) распространены указанными лицами, а также требований и порядка размещения такого указания), Order of the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Communications of 23 September 2020 No. 124, <https://rg.ru/2020/10/20/roskomnadzor-prikaz124-site-dok.html>.

⁵¹ Ministry of Justice of the Russian Federation, “Register of the foreign media that perform the functions of a foreign agent” (Реестр иностранных средств массовой информации, выполняющих функции иностранного агента), <https://minjust.ru/ru/documents/7755/>.

⁵² Federal Statute “On amendments to the Federal Statute ‘On measures to influence persons involved in violations of fundamental human rights and freedoms, the rights and freedoms of citizens of the Russian Federation’” (О внесении изменений в Федеральный закон ‘О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации’), <http://publication.pravo.gov.ru/Document/View/0001202012300002>. See Richter A., *op.cit.*, p. 10.

⁵³ <http://merlin.obs.coe.int/article/9068>.

as “governmental media” or the content as “violent” or the intentional removal of the account from ‘most popular’ lists.

Once the entity is designated as having violated the freedom of information rights of Russians, the office of the Prosecutor-General sends a relevant ruling to Roskomnadzor. The latter begins by placing the resource on a special new “blacklist” type Register that is still to be made available on its official website. So far, Roskomnadzor has adopted a procedure on establishing and using such a blacklist,⁵⁴ but it has not yet entered into force. The Register will include, in particular, information on communications with Roskomnadzor, such as the date and time of its notices to cease causing “limitations” to Russian media.

Thereafter, within a day, Roskomnadzor will send a warning to the owner of the online resource demanding that a stop be put to these limitations. If this does not happen, Roskomnadzor will block, “entirely or partially”, access to the online resource. The Russian authorities’ decisions may be retracted once the violations have ceased.

Typically, the Prosecutor-General’s office issues its rulings in response to petitions from concerned individuals or entities; but it may also conduct investigations on its own initiative. Such rulings can be appealed in court. If the appeal is successful, the online resource will be excluded from the Register and unblocked.⁵⁵

Critics point to certain flaws in the amendments. Because the list of grounds is not exhaustive, additional types of discriminatory restrictions appear to be subject to interpretation by the authorities. The law does not stipulate the exact term within which the Internet resource owner must react to the Roskomnadzor notice, whether the blacklist decision can be appealed or whether access to the resource will remain unhindered during the appeal.⁵⁶

⁵⁴ Procedure for conducting the List of owners of resources in the information-telecommunication network Internet, which are involved in violations of the fundamental rights and liberties of a man, rights and freedoms of citizens of the Russian Federation that guarantee, among others, freedom of the mass media, entry and withdrawal from the List of information on owners of resources in the information-telecommunication network Internet, as well as the types of information on them therein (Порядок ведения перечня владельцев ресурсов в информационно-телекоммуникационной сети “Интернет”, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации, гарантирующих в том числе свободу массовой информации, внесения в него и исключения из него информации о владельцах ресурсов в информационно-телекоммуникационной сети “Интернет”, состав содержащейся в перечне информации о них), approved by an ordinance of Roskomnadzor of 11 March 2021 N 23, http://www.consultant.ru/document/cons_doc_LAW_386221/43734fdff2df2ef4db6a153a096063a104a591d0/.

⁵⁵ Fridman V. and Botvinkina A., “Russia introduces new grounds for blocking websites and social networks”, Gowling WLG, 26 January 2021, <https://gowlingwlg.com/en/insights-resources/articles/2021/russia-blocking-websites-and-social-networks/>.

⁵⁶ Pak M., “Russia Introduces Measures Against Discriminatory Internet Censorship”, 1 March 2021, Petošević, <https://www.petosevic.com/resources/news/2021/03/4429>.

Foreigners involved in the above-mentioned limitations of information from Russian sources will be banned from entering the country and their assets in Russia will be seized.⁵⁷

These amendments should be understood in the context of the earlier demands by Roskomnadzor that Facebook LLC cease, “in the shortest time possible”, limiting access to and blocking both the Instagram accounts of the regional state broadcasters *Stavropolye* and *Lotos* and the Facebook account of *Baltnews* (an affiliate of the *Rossija Segodnya* state news agency), as well as its demands of Google LLC in relation to the latter’s downgrading of the *Solovyov Live* YouTube channel, the blocking of the ANNA News YouTube channels, the “limitations” on documentaries by RT and *Ukraina.ru*, and the labeling of a programme by the state-run *Rossija-1* TV as “inappropriate and offensive for certain audiences”, etc.⁵⁸ The Explanatory Note to the draft law also referred to some 20 “acts of censorship vis-a-vis the accounts” of *Russia Today*, *RIA Novosti*, and *Crimea 24* conducted by Facebook, YouTube and Twitter.⁵⁹

At some point, Roskomnadzor even called on Russian broadcasters and online resources to migrate from YouTube to Russian Internet platforms for the safe distribution of video materials.⁶⁰

⁵⁷ Federal Statute “On amendments to the Federal Statute ‘On measures to influence persons involved in violations of fundamental human rights and freedoms, the rights and freedoms of citizens of the Russian Federation’” (О внесении изменений в Федеральный закон “О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации”), 30 December 2020 N 482-FZ, <http://publication.pravo.gov.ru/Document/View/0001202012300002>.

⁵⁸ See e.g. Press release by Roskomnadzor, 30 October 2020, <http://rkn.gov.ru/news/rsoc/news73130.htm>.

⁵⁹ Explanatory Memorandum on the Draft Law (Пояснительная записка к законопроекту), N1058572-7, 19 November 2020, <https://sozd.duma.gov.ru/bill/1058572-7>.

⁶⁰ Press release by Roskomnadzor, 13 November 2020, <https://rkn.gov.ru/news/rsoc/news73170.htm>.

4. Illegal content

The major reason for sanctioning social media companies remains their dissemination of content deemed illegal in Russia.

4.1. Mechanisms to identify and block content

The legal framework of identifying such prohibited online content and stopping its dissemination presents two distinct mechanisms.

The first mechanism originates in the amendments made in 2012 to the Federal Statute “On Information, Information Technologies and on the Protection of Information” (henceforth referred to as IT Law) which introduced Article 15.1. This article set forth the procedures to establish, expand, and maintain the “Unified register of the domain names, website references and network addresses that allow identifying websites containing information circulation which is forbidden in the Russian Federation”, (or, Uniform Automated Information System of the Russian Internet Blacklist).⁶¹

Once a website and a webpage are entered into the Russian Internet Blacklist, they are blocked unless the service and hosting providers quickly remove the offending materials.⁶² Roskomnadzor updates the Blacklist following individual court decisions that identify and recognise websites or webpages with “illegal content” (usually extremist statements). It is also updated following decisions of federal executive bodies specifically dealing with child pornography, drugs and suicide. Attempts to challenge in courts the decisions to enter social media materials in the Blacklist have generally failed.⁶³

According to Roskomnadzor, from 2012 to April 2021, it blocked or restricted access to some 164 000 materials, just of an extremist nature, and their copies.⁶⁴

The second mechanism originates in the amendments made in 2013 which introduced Article 15.3 to the IT Law. It set forth the administrative procedures to allow the Prosecutor-General and his deputies to identify illegal content and then pass the case to Roskomnadzor so that it uses its compulsion mechanisms to have the content removed or introduces administrative sanctions, including blocking access to websites containing such content, if this does not take place.⁶⁵ While this non-judicial procedure was originally

⁶¹ It is even available in English at: <http://eais.rkn.gov.ru/en/>. The same page also contains relevant extracts from the IT Law in English.

⁶² Richter A., *Regulation of online content in the Russian Federation*, IRIS Extra, European Audiovisual Observatory, Strasbourg, 2015, <https://rm.coe.int/1680783de3>. See page 14 of this publication.

⁶³ Richter A. (2015), *op.cit.*, p. 15.

⁶⁴ “The Russian practice of counteracting dissemination of extremist and terrorist materials in the Internet” (Российский опыт противодействия распространению в сети «Интернет» материалов экстремистского и террористического характера), OSCE, PC.DEL/532/21 (Security Committee, 12 April 2021, Russian speaker from Roskomnadzor Evgeniy Zaycev) (#C_2104_5042).

⁶⁵ Richter A. (2015), *op.cit.*, pp. 16-17.

introduced only for such “clear” offences as incitement to unsanctioned public protests and to “extremist” activities, over the next few years it was significantly expanded to include new categories of illegal online content.

The second mechanism also encompasses a separate Article 15.1-1, introduced in 2019 to the IT Law, which bans “blatant disrespect for society, government, official state symbols, the constitution or state bodies of Russia”, meaning “expression of apparent disrespect in indecent form” or “sheer disrespect”.⁶⁶ The legislation also allows for fines of up to RUB 300 000 and imprisonment of up to 15 days for its violation.

In 2021, a similar mechanism was established through the new Article 15.3-1 of the IT Law in relation to illegal election canvassing online.

Additionally, in 2013 a separate article (15.2) was added to the IT Law to regulate relations between Roskomnadzor and hosting providers in relation to copyright violations on the Internet, once they are confirmed by a court decision. The procedure is similar to the second mechanism, as blocking and take-down notices for social network accounts were recognized as a more efficient method than imposing liability for copyright violations on the social media companies.⁶⁷

According to Roskomnadzor, from 2012 to April 2021 it blocked or restricted access to some 400 000 materials and their copies banned by Article 15.3 of the IT Law alone.⁶⁸ The same source points to certain problems regarding take-down of content recognized by the Russian prosecutors as extremist or terrorist.

In particular, it notes that Facebook still has not removed 3,600 posts out of more than 15 000 deemed extremist or terrorist, Instagram 370 out of 10,400, YouTube 7,100 out of 41,000 and Twitter 290 out of 2,100.⁶⁹

4.2. “Law on Fake News” and social media

Dissemination of false information under the guise of credible reports has been an offence applicable to social networks for quite a long time.⁷⁰

Even before COVID-19 spread widely, a set of amendments to the IT Law was adopted, in March 2019, to stop online dissemination of certain categories of false information under the guise of credible reports. These amendments are often referred to in

⁶⁶ Letter by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the Russian authorities, 1 May 2019, part 1, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_RUS_01_05_19.pdf.

⁶⁷ <http://merlin.obs.coe.int/article/6162>.

⁶⁸ The Russian practice of counteracting dissemination of extremist and terrorist materials in the Internet, op.cit.

⁶⁹ Ibid., see also Roskomnadzor informs on the results of verification of compliance with the Russian law by the U.S. online platforms and mass media (Роскомнадзор информирует о результатах проверки соблюдения российского законодательства американскими интернет-платформами и СМИ), Press release, 11 June 2021, <https://rkn.gov.ru/news/rsoc/news73688.htm>.

⁷⁰ Richter A., *Disinformation in the media under Russian law*, IRIS Extra, European Audiovisual Observatory, Strasbourg, June 2019, <https://rm.coe.int/disinformation-in-the-media-under-russian-law/1680967369->

the Russian media as the “Law on Fake News”.⁷¹ The law prohibits online dissemination of “unreliable socially significant information”, which would create “a threat or harm to life and (or) the health of citizens, property, the threat of mass disturbance of public order and (or) public security, or the threat to operation of life support facilities, transport or social infrastructure, credit institutions, energy facilities, industry or communications”.

The “Law on Fake News” was accompanied by amendments to the Code on Administrative Offences of the Russian Federation.⁷² Adopted on the same day, they established fines for legal entities and physical persons, including users of social media and bloggers, who spread various types of “knowingly inaccurate socially significant information”, by adding three paragraphs to Article 13.15 (“Abuse of freedom of the media”) of the Code. In 2020, two more paragraphs were added here, while the scale of monetary fines increased tenfold.

Speaking in 2021 of social media regulation in the world in the context of dissemination of disinformation, the UN Special Rapporteur on freedom of expression singled out three countries worldwide (including Russia) which recently “adopted laws that grant the authorities excessive discretionary powers to compel social media platforms to remove content that they deem illegal, including what they consider to be disinformation or ‘fake news’”. The UN Special Rapporteur pointed to the fact that failure to comply with them is sanctioned with significant fines and/or content blocking and concluded that “such laws lead to the suppression of legitimate online expressions with limited or no due process or without prior court order and contrary to requirements of article 19 (3) of the International Covenant on Civil and Political Rights”.⁷³

4.3. Fines for a failure to delete prohibited materials

In December 2020, a new Article 13.41 was added to the Code of the Russian Federation on Administrative Offences.⁷⁴ Under it, inaction by hosting providers and website owners (including foreign ones) with regard to the requirements to block access to information banned in Russia or to remove information recognised as illegal in Russia under the IT Law shall lead to significant monetary fines. The illegal information in question includes

⁷¹ Federal Statute “On amendments to Article 15-3 of the Federal Statute on information, information technologies and protection of information” (О внесении изменений в статью 15-3 Федерального закона “Об информации, информационных технологиях и о защите информации”), 18 March 2019, No. 31-FZ, <http://publication.pravo.gov.ru/Document/View/0001201903180031>. See also Richter A. (2019), *op.cit.*, and Letter by the Special Rapporteur, *op.cit.*

⁷² Federal Statute “On amendments to Code of the Russian Federation on Administrative Offences” (О внесении изменений в Кодекс Российской Федерации об административных правонарушениях), 18 March 2019, No. 27-FZ, <http://publication.pravo.gov.ru/Document/View/0001201903180021>.

⁷³ “Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”, Khan I.. United Nations Human Rights Council. A/HRC/47/25, 13 April 2021, para 57, <https://undocs.org/A/HRC/47/25>.

⁷⁴ Federal Statute “On amendments to the Code of the Russian Federation on Administrative Offences” (О внесении изменений в Кодекс Российской Федерации об административных правонарушениях), 30 December 2020 N 511-FZ, <http://publication.pravo.gov.ru/Document/View/0001202012300050>. See <http://merlin.obs.coe.int/article/9069>.



“information with calls to extremist activities”; child pornography; drug use; “information disrespectful to state authorities”;⁷⁵ “unfaithful information”;⁷⁶ and “untruthful socially significant information” (under the Law “On Fake News”);⁷⁷ as well as a new set of prohibited content types introduced to the IT Law on the same day. The only exception made to the norm are copyright violations, punished elsewhere by law.

A failure to comply with the requirements to block (“restrict”) access to prohibited information now leads to fines ranging from RUB 50 000 to 100 000 for individuals; RUB 200 000 to 400 000 for company executives; and RUB 800 000 to four million for legal entities. The penalties for repeat offences by a legal entity amount to between 5% and 20% of the company's year-end revenue.⁷⁸ It remains unclear as to whether the company's head office or its representative office (if any) in Russia are responsible for paying the fines proportionate to the revenue. In a recent interview, Andrei Lipov, the head of Roskomnadzor since March 2020, in reply to a request to clarify, answered: “So far it is about revenues in Russia.”⁷⁹ According to him, it was an effective measure: The process of blocking access by the social media companies “has accelerated,” with their “worldview” changed because “the fines lead not to political considerations, but Key Performance Indicators (KPI) of particular managers”.⁸⁰

As of June 2021, for non-compliance with the requirement to block access to prohibited materials, Facebook/Instagram had accumulated fines totalling RUB 43 million, Twitter RUB 27.9 million, and Google/YouTube RUB 6 million, as well as an additional RUB 9.2 million for “inadequate filtering of a search engine”.⁸¹

In addition to increased administrative sanctions, the Net Freedoms Project, in its 2020 report, noted a significant trend towards criminal prosecution of administrators of popular public groups in the social networks and Telegram or YouTube channels for non-compliance – pointing to about a dozen cases.⁸²

⁷⁵ <http://merlin.obs.coe.int/article/8579>.

⁷⁶ <http://merlin.obs.coe.int/article/7676>.

⁷⁷ <http://merlin.obs.coe.int/article/8578>.

⁷⁸ Ibid.

⁷⁹ Andrei Lipov, op.cit.

⁸⁰ Ibid.

⁸¹ Roskomnadzor informs... (op. cit.)

⁸² Gainutdiniv D. and Seleznev S., “Freedom of the Internet – 2020: Second wave of repression (Свобода интернета 2020: вторая волна репрессий)”, Net Freedoms Project, 2 March 2021, p. 23, <https://runet.report/static/core/doc/Свобода%20интернета%202020.%20Вторая%20волна%20репрессий.pdf>

5. Law “on self-regulation of social media”

A specific law that would regulate social networks has been debated in the State Duma since 2017.⁸³ In late December 2020, the debate suddenly gained momentum, as a particular set of amendments that expanded the scope of the IT Law was adopted on 23 December 2020 and signed by the President already a week later.⁸⁴

The authorities call it the Law “on self-regulation of social media”, and point out that the aim is to place part of the burden of monitoring compliance with the restrictions on the social network companies themselves: “like the owner of the fence carries some responsibility for what is inscribed there, the networks must help catch ‘trash’ online”.⁸⁵

The amendments largely present a new 16-page Article 10-6 (“Specificity of dissemination of information in the social networks”) of the IT Law. It defines a social network as:

a website and/or a webpage of the site on the Internet, and/or an information system, and/or computer software intended for and/or used by their clients to provide and/or disseminate through their personal pages information in the state language of the Russian Federation, state languages of the republics within the Russian Federation and other languages of the peoples of the Russian Federation, which can be used for advertising aimed at attracting the attention of consumers located on the territory of the Russian Federation.

The Law “on self-regulation of social media,” entered into force on 1 February 2021 and applies to the owners of social networks, both Russian and foreign, which have at least 500,000 users accessing them daily from the territory of the Russian Federation. To verify their number, the owner must incorporate one of the software programmes recommended by Roskomnadzor for counting the number of users.

The owners of such large social networks shall:

- 1) not allow their use in order to commit criminal offenses, disclose information constituting a state secret or other secret specially protected by law, disseminate materials containing public calls to conduct terrorist activities or publicly justifying terrorism, other extremist materials, as well as materials promoting pornography, the cult of violence and cruelty, and materials containing obscene language;

⁸³ Klyuchevskaya N., “Stop, content: New responsibility of owners of social networks and rights of users” (Стоп, контент: новые обязанности владельцев соцсетей и права пользователей), (Garant.Ru, 3 February 2021.

⁸⁴ Federal Statute “On amendments to the Federal Statute ‘On Information, Information Technologies and on the Protection of Information’” (О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”), 30 December 2020, N 530-FZ, <http://publication.pravo.gov.ru/Document/View/0001202012300062>.

⁸⁵ Andrei Lipov, op.cit.

- 2) prevent the dissemination of information aimed at defaming a citizen or certain categories of citizens on the basis of their gender, age, race or ethnicity, language, attitude to religion, profession, place of residence and work, as well as in connection with their political convictions;
- 3) comply with the prohibitions and restrictions provided for by the Russian federal legislation on referendum and on elections;
- 4) observe the rights and legitimate interests of citizens and organizations, including honour, dignity and the business reputation of citizens, the business reputation of organizations.

An owner of a large social network is also bound to self-monitor the contents of the social network so as to detect the following types of information:

- a. materials with pornographic images of minors and/or notices aimed to get minors involved as performers in entertainment events of a pornographic nature;
- b. information on the methods of development, manufacture and use of narcotic drugs, psychotropic substances and their precursors, new potentially dangerous psychoactive substances, places of their purchase, methods and places of cultivation of narcotic plants;
- c. information on the ways of committing suicide, as well as calls to commit suicide;
- d. information that violates the prohibition of organization and conduct of gambling and lotteries using the Internet and other means of communication;
- e. information that violates the prohibition of remote retail sale of alcoholic drinks and/or alcohol-containing food and non-food products;
- f. information aimed at soliciting or otherwise involving minors in committing illegal acts that pose a threat to their life and/or health or to the life and/or health of other persons;
- g. information expressing in an indecent form that offends human dignity and public morality, blatant disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation or bodies exercising state power in the Russian Federation;
- h. information containing calls for mass riots, for conduct of extremist activities, participation in mass public events held in violation of the established procedures, unreliable socially significant information disseminated under the guise of reliable messages, which creates a threat of harm to life and/or health of citizens, property, the threat of mass disturbance of public order and/or to public safety or the threat of interfering with the functioning or termination of the functioning of life-supporting facilities, transport or social infrastructure, credit organizations, energy, industry or communications facilities;
- i. information materials of a foreign or international non-governmental organization recognized as “undesirable” on the territory of the Russian Federation;⁸⁶

⁸⁶ Richter A. (2020), *op.cit.*, pp. 10-11.

- j. any information on how to [technically] get access to the above-listed types of information or materials.

An owner of a large social network is expected by the Law “on self-regulation of social media” to provide therein an e-mail address to which legally significant messages can be sent, a surname and initials (for an individual) or name (for a legal entity), and an electronic form for sending complaints on information disseminated in violation of the law. Particular elements of the form are to be approved by Roskomnadzor.

The owner must annually post a report on the results of consideration of complaints filed using the electronic form, as well as on the results of content monitoring carried out in accordance with the above-noted demand of the law. Again, Roskomnadzor shall instruct the owners on their reports’ structure and placement.

The Rules of Service of large social networks shall, in addition, be made available in Russian, and such access shall be unlimited and free. These Rules of Service shall not contravene Russian law governing content dissemination. If they are amended, the owners must individually inform all users within three days. In case of limiting access to certain prohibited information, the user who made it available is also informed about the grounds of such a limitation.

Whenever self-monitoring of content or complaints about information disseminated in violation of the law point to the presence of the above-outlined content, the owner shall take, without delay, measures to limit access to it.

The requirement for such an immediate reaction may be waived if the owner of a social network cannot assess the degree of compliance of the information identified with the legal requirements. Then the owner shall, within 24 hours from the discovery of potentially illegal information, forward it to Roskomnadzor in accordance with the procedures determined by this authority. Until Roskomnadzor makes its decision on the (in-)admissibility of the material in question, the owner of a social network shall restrict access to it. In turn, Roskomnadzor, prescribes the Law “on self-regulation of social media,” and communicates to other governmental agencies with regard to reaching a conclusion in line with articles 15.1, 15.1-1 and 15.3 of the IT Law (see section 5 above).

In addition, if a social media user disagrees with the decision of the owner of a social network to restrict access to information made available through his/her account, a complaint can be submitted, first to the owner (to be replied to within three days), and – if there is a need to “appeal” – to Roskomnadzor. The latter may instruct the owner to unblock the content in question.

Roskomnadzor shall establish a Registry of Social Networks (those that fall under the regulation of the Law “on self-regulation of social media”). Once a social network is entered into the Registry by a sole decision of Roskomnadzor, the latter determines its hosting provider, and requests from it the information necessary to determine the network’s owner. The hosting provider is given three days to reply. Once the owner is determined, Roskomnadzor sends it a notice on inclusion of the social network in the Registry and on relevant provisions of Russian law. There is a grace period of two months for the owners of social networks entered into the Registry to comply with Russian law.



Roskomnadzor shall organise its own monitoring of the networks' content and request information necessary for running the Registry from the owners and others through the communication lines and procedures approved by the authority. This information shall be provided within 10 days.

6. Case law of the Supreme Court of Russia

Legal experts in Russia point to the availability of important case law related to content regulation on social networks, although in most cases the liability was not with the owners of the social networks, a new term in Russian law, but with the users.⁸⁷

A stand-alone judgment is the procedural decision of the Supreme Court of the Russian Federation on a complaint of four citizens to Facebook, Inc. The four persons, all Facebook users, challenged in a district court in Moscow the social network's decisions to take down some of their posts, block access to their accounts and remove them.⁸⁸ They claimed the defendant had in this manner violated their right to freedom of expression and the copyright to their materials; moreover, they believed that Facebook collected their personal data beyond the scope of its Terms of Service. They asked the court to oblige the company to cease such activities. Both the district court and the Moscow City Court returned the complaint without consideration as the defendant was outside their jurisdiction.

The Judicial Chamber on Civil Cases struck down these decisions by providing the following arguments: According to the Civil Procedure Code of the Russian Federation (Article 29), national courts are competent to consider complaints on the violation of rights of Russian residents as subjects of personal data. Therefore, as the collection of the plaintiffs' personal data took place on the territory of the Russian Federation, the social network contained advertising aimed at consumers in Russia, and the two sides are in a contract (that is the Facebook Terms of Service) that should (at least partially) be implemented on the territory of the Russian Federation; national courts may not avoid considering such complaints.

One of the most important conclusions of this judgment for further case law is connected with the place of the execution of the Terms of Service of a social network. In the future, such criteria may be also used to define an applicable law – not only courts' jurisdiction.⁸⁹ No wonder this judgment was further promoted by the Supreme Court in its quarterly review of important national case law.⁹⁰ It was also cited in a ruling by the Moscow City Court on the appeal of the district court's ruling on the lawsuit of Aleksandr Malkevich, president of the Foundation for the Protection of National Values, against Twitter Inc. with a demand “to cease blocking access to his personal account, and illegal storage of his

⁸⁷ Klyuchevskaya N., op.cit.

⁸⁸ Ruling of the Judicial Chamber on Civil Cases of the Supreme Court of the Russian Federation, 9 June 2020 N 5-KG20-49, M-10004763/19, <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-09062020-n-5-kg20-49-m-1000476319/>.

⁸⁹ Lysachkina D., “Recent updates in personal data regulation in Russia”, Maxima Legal LLC, 8 July 2020, <https://www.ilnipinsider.com/2020/07/recent-updates-in-personal-data-regulation-in-russia/>.

⁹⁰ Review of the Case Law of the Supreme Court of the Russian Federation (Обзор судебной практики Верховного Суда Российской Федерации), No 1 (2021), para 18, <http://supcourt.ru/documents/practice/29857/>.

personal data, as well as for compensation of moral and material damages”.⁹¹ The appeals instance returned the case to the district court (which originally dismissed it for lack of jurisdiction) for a full consideration of the lawsuit. By the time of this publication no decisions on the lawsuits against Facebook and Twitter had been made.

Several cases adjudicated by the Supreme Court in relation to dissemination of information through social networks were: (1) the public display in Odnoklassniki of a swastika, which was later found not to be a swastika, but another symbol, but was nonetheless found to be “extremist;”⁹² (2) the use of a social network account to disseminate “hate speech” in relation to a “religious group” defined as “[Russian] Orthodox believers;”⁹³ and (3) the retention of a comment by a third party to one’s post on a social network account – the comments contained the legally prohibited call “Orthodoxy or death!”⁹⁴ In all three cases the judgments of the Supreme Court were to dismiss the complaints and uphold the lower courts’ decisions.

Yet, in one other case, the Judicial Chamber on Cases with Military Servicemen, found that the lower courts were wrong in dismissing criminal accusations related to terrorism propaganda against a person who three times posted comments on his Vkontakte account that experts recognized as calls for violence against those who do not share adherence to Islamism. The Supreme Court argued its position by noting that the serviceman additionally discussed issues relevant to his posts with two witnesses in the case.⁹⁵

In yet another case, the Supreme Court reviewed earlier adjudication of a conflict when a bank in Bashkortostan tried to collect a car loan debt from an individual debtor. The bank found the personal account of the debtor on Vkontakte and put her under “psychological pressure” by sending her messages and disseminating negative information about her among her “friends”. While this was a violation of the personal rights of the debtor, the decision by the lower courts to impose an administrative fine of RUB 20,000 on the bank were struck down, as credit organizations are exempted from liability for such actions if they are caused by arrears of their debtors.⁹⁶

⁹¹ Appeal Ruling of the Moscow City Court of 26 November 2020 N 33-416426/2020, <https://mosgorsud.ru/mgs/services/cases/appeal-civil/details/9ec90640-25a8-11eb-aa19-23acf0476297>.

⁹² Judgment of the Supreme Court of the Russian Federation, 11 December 2018 N 24-AD18-6, <https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-11122018-n-24-ad18-6/>.

⁹³ Judgment of the Supreme Court of the Russian Federation, 20 December 2019 N 1-AD19-4, <https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-20122019-n-1-ad19-4/>.

⁹⁴ Judgment of the Supreme Court of the Russian Federation, 10 April 2019 N 31-AD19-4, <https://legalacts.ru/sud/postanovlenie-verkhovnogo-suda-rf-ot-10042019-n-31-ad19-4/>.

⁹⁵ Review of the Case Law of the Supreme Court of the Russian Federation (Обзор судебной практики Верховного Суда Российской Федерации), No 1 (2020), para 60, <http://supcourt.ru/documents/practice/28993/>.

⁹⁶ Judgment of the Supreme Court of the Russian Federation, 15 February 2019 N 48-AD19-2, <https://www.v2b.ru/documents/postanovlenie-verhovnogo-suda-rf-ot-18-06-2019-49-ad19-2/>.

7. Law on “grounding foreign IT companies” as new compliance mechanism

Despite the fact that the State several times raised the stakes for noncompliance with a variety of regulations coming from the booming Russian legislation governing online content, for example by setting higher fines for social media companies, the issue of lack of compliance remains high on its agenda.

On 1 July 2021, a law was signed into force by the President, with the aim to provide “equal conditions for work for Russian and foreign entities on the territory of the Russian Federation” (Article 2). It foresees that all Internet companies, including social media, that service (daily) at least 500 000 users in Russia and do so by (1) either providing resources in Russian (or other languages of the RF), or (2) publishing advertising targeting customers in Russia, or (3) processing personal data of clients from Russia, or (4) receiving monetary means from Russian individuals and legal entities shall, through their official branches, representative offices or subsidiaries, open a direct online account with Roskomnadzor and strictly follow the norms of Russian law (Article 4).⁹⁷

A failure to comply with this requirement shall result in sanctions for the foreign entity such as a ban on advertising by or on this entity, a ban on search results with its resources, a ban on personal data concerning trans-border transfers, limitation of money transactions, and a partial or complete ban on access to the services provided (Article 9).

When commenting on the draft law, which he called the Law “on grounding IT companies”, the speaker of the State Duma noted that “foreign companies had a chance to go along the road of self-regulation”, apparently referring to the Law “on self-regulation of social media ... They’ve failed to do it. That means there is a need for legal instruments, including relevant means of compulsion, first of all economic ones”.. The parliamentary speaker added that the forthcoming law would first and foremost concern Facebook, Instagram, Twitter, TikTok, Google, YouTube, WhatsApp, Viber, Telegram, and the World of Tanks online multiplayer game. “This list is open,” he observed.⁹⁸

Legal experts in Russia point out that the law has generated a lot of controversy, as it significantly changes the legal landscape for non-Russian IT companies. Among other things, it purports to grant “extraordinary powers” to Roskomnadzor to make a

⁹⁷ Federal Statute “On activity of foreign entities in the information-telecommunication network Internet on the territory of the Russian Federation” (О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации), N236-FZ of 1 July 2021, <http://publication.pravo.gov.ru/Document/View/0001202107010014?index=0&rangeSize=1>.

⁹⁸ Interfax news agency, “Law on offices in RF of big IT companies will primarily affect Facebook, Twitter and Google” (Закон о представительствах крупных IT-компаний в РФ коснется в первую очередь Facebook, Twitter и Google), 24 May 2021, <https://www.interfax-russia.ru/main/zakon-o-predstavitelstvah-krupnyh-it-kompaniy-v-rf-kosnetsya-v-pervuyu-ochered-facebook-twitter-i-google>.



determination at its discretion, to impose sanctions without a court judgment, and to exercise powers in areas that are within the domain of other public authorities. For example, the Federal Antimonopoly Service is in charge of advertising matters, and the Central Bank oversees payment rules.⁹⁹

⁹⁹ Dergacheva A. and Strizh V., “Non-Russian Online Businesses May Be Forced to Open Offices in Russia and Submit to Russian Jurisdiction”, Morgan, Lewis & Bockius LLP, 26 May 2021, <https://www.morganlewis.com/blogs/sourcingatmorganlewis/2021/05/non-russian-online-businesses-may-be-forced-to-open-offices-in-russia-and-submit-to-russian-jurisdiction#page=1>.



8. Conclusion

Specific regulation of social networks in Russia is a very recent phenomenon. At the core of the regulation are various efforts to make the policies of foreign social networks fully compliant with federal legislation and regulations, especially in regards of the availability and dissemination of content found to be illegal in Russia, and to ensure that this compliance is efficient and quick.

So far, the regulation has taken into account possible social discontent in the case of general blocking of access to major social networks, and technical difficulties in fully implementing such a block. Therefore, the current policy appears to achieve its aims through forcing the social media companies to open formal branches in Russia and imposing on them significant monetary penalties.

A publication
of the European Audiovisual Observatory

