Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**846**
Land:	Rusland
Kilde:	Freedom House
Titel:	Freedom on the Net. Russia
Udgivet:	16. oktober 2024
Optaget på baggrundsmaterialet:	6. november 2024

NOW LIVE: Freedom on the Net 2024

Freedom House

FREEDOM ON THE NET 2024

Russia

NOT FREE

20 /100

A. Obstacles to Access	**10** /25
B. Limits on Content	**5** /35
C. Violations of User Rights	**5** /40

LAST YEAR'S SCORE & STATUS

21 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Key Developments, June 1, 2023 – May 31, 2024

The already dire state of internet freedom in Russia worsened during the coverage period. The government continued to block critical news sites and developed increasingly sophisticated technical and legislative measures to block virtual private networks (VPNs). Government agencies go to extensive lengths to surveil those who criticize the government online. Courts have also ordered the imprisonment of online critics of the full-scale invasion of Ukraine, and of the government more broadly.

- During two distinct protests in the republics of Sakha (Yaktusk) and Bashkortostan in January 2024, WhatsApp and Telegram were reportedly inaccessible. Individuals also had issues accessing the internet more broadly in the immediate proximity of a courthouse where the trial of environmental activist Fail Alsynov was held (see A3).
- In November 2023, the Supreme Court named the "international LGBT movement" as an extremist organization, which has facilitated website blocks, content removal, and criminal cases against those who share content that could be construed as LGBT+ (see B1, B2, C2, and C3).
- In March 2024, a law that bans websites from posting information about circumvention tools, including VPNs, or advertising for VPNs came into effect; shortly after, the country's telecommunications regulator blocked 30 webpages, most of which provided instructions on how to access banned social media platforms (see B1, B2, and C4).
- Human rights group OVD-Info reported that as of May 2024, 935 criminal cases were opened against Russians under laws passed since the Kremlin's full-scale invasion of Ukraine that criminalize discrediting or spreading false information about the Russian military, which have resulted in several multiyear sentences (see C3).
- The government introduced new measures expanding its access to individuals' location data, including a September 2023 law that orders taxi services to provide the telecommunications regulator with live location data

and a January 2024 measure that requires internet service providers (ISPs) to provide users' geolocation data (see C6).

Political Overview

Power in Russia's authoritarian political system is concentrated in the hands of President Vladimir Putin. With subservient courts and security forces, a controlled media environment, and a legislature consisting of a ruling party and pliable opposition factions, the Kremlin manipulates elections and suppresses genuine opposition. Rampant corruption facilitates shifting links among state officials and organized crime groups. Since the regime launched a full-scale invasion of Ukraine in February 2022, authorities have intensified restrictions on individual rights and liberties in order to stifle domestic dissent.

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5**/6

Internet access in Russia continues to expand gradually. The International Telecommunication Union (ITU) estimated the country's internet penetration rate at 92.2 percent in 2023. [1] According to 2022 data from the ITU, there were 24.6 fixed-line broadband subscribers per 100 inhabitants, and 110 mobile broadband subscribers per 100 inhabitants. [2]

According to the Institute of Statistical Studies and Economics of Knowledge (ISSEK) of the Higher School of Economics, 86.6 percent of Russian households had internet access at the end of 2022 compared to 69.9 percent in 2014. [3] According to the Economist's 2022 Inclusive Internet Index, 88.7 percent of the population has access to a 3G or 4G network. [4]

The Russian government planned to launch 5G services in Moscow in 2020 and throughout the country in 2021, [5] but the launch has repeatedly been delayed. In January 2022, Rostec presented a plan to develop 5G base stations under an agreement with the government, with production scheduled to begin in 2024. [6]

However, the authorities reduced funding for the frequency conversion of 5G networks from 43 billion rubles ($704 million) to 7.85 billion rubles ($130 million) for the period up to 2024, which could have adverse effects for the Rostec plan. [7] The impact of sanctions imposed by the United States and the European Union (EU) in the wake of the full-scale invasion of Ukraine, as well as the withdrawal of telecommunications equipment manufacturers from the Russian market, have also impacted the 5G rollout plan. [8]

In November 2023, the government approved a new strategy for telecommunications development through 2035. [9] According to the document, from 2023 to 2030 the Russian government plans to develop and operate Russian equipment that meets 5G and eventual 6G standards. In the second stage, encompassing 2031 to 2035, the government plans to deploy 5G networks in all cities with more than 100,000 residents. The main frequency range for creating 5G networks in Russia is 4.4–4.99 gigahertz (GHz), while the 3.4–3.8 GHz range is considered preferable at the global level. [10] In October 2023, MegaFon, a telecommunications operator, signed a contract with equipment manufacturer Bulat for 5,000 telecommunications base stations. [11]

Connection speeds are stable, with median fixed-line broadband download speeds at 87.71 megabits per second (Mbps) and median mobile internet download speeds at 25.51 Mbps, according to May 2024 data from Ookla's Speedtest Global Index. [12]

Maintenance work has sometimes caused internet outages. In March 2024, the internet in the Trans-Baikal Territory was inaccessible [13] due to maintenance. [14] In one of the districts, short emergency number 112 did not work due to communication problems. In other cases, government agencies asserted that maintenance issues caused outages around protests (see A3).

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

The impact of the Russian invasion of Ukraine and the ensuing sanctions continue to affect the cost of internet access. According to 2023 data from the ITU, a

monthly fixed-line broadband subscription cost 0.58 percent of gross national income (GNI) per capita, while a mobile plan offering 2 gigabytes (GBs) of data cost 0.38 percent of GNI per capita. [15] In October 2023, Incorporated Russia reported that telecommunications-company representatives were planning 10–15 percent price increases for home internet and mobile service in 2025, with some predicting higher price increases. Incorporated Russia based that report on a survey and on reporting within Russia; the representatives cited rising costs, sanctions, and the departure of foreign firms from the market. [16]

The rising cost of internet access in Russia, which began to climb notably in 2020, is due in part to costs resulting from the implementation of laws, including the Yarovaya Law, and the law on sovereign Runet (the Russian segment of the internet). [17] The Yarovaya Law, which was enacted in 2018, requires operators to install expensive equipment to record and store user-traffic data on their networks. In addition, it led to an annual increase in traffic-storage volumes, which further affects cost. The law on sovereign Runet also obliges operators to install deep packet inspection (DPI) systems on their networks to filter subscribers' internet traffic. The same equipment is used to slow, censor, and restrict access to websites.

In March 2023, the State Duma adopted a law that obliges owners of technological communication networks with autonomous system numbers to store user data for three years (see C6), which could further raise costs for users. [18] The law came into force in September 2023.

In May 2023, mobile service providers MTS, MegaFon, Beeline, and Tele2 began charging for internet "hotspot" services. In September 2023, the Federal Anti-Monopoly Service issued a warning to operators demanding that fees for internet distribution be canceled and threatening to open cases under antimonopoly laws. [19] As of March 2024, MTS continues to charge additional fees.

In July 2021, President Vladimir Putin signed a law on free access to socially significant websites, [20] which followed a pilot of the program from March 2020 to July 2021. The list of sites for free access included the websites of the president of the Russian Federation and the government of the Russian Federation, sites of federal ministries and nonbudgetary funds, state media, Russian social networks (such as VK and Odnoklassniki) and Russian email services (such as Mail.ru),

among other sites. The law obliges providers and operators to grant access to these sites without charging a fee (see B6).

In November 2021, the four largest mobile service providers in Russia—Beeline, Tele2, MegaFon, and MTS—announced that they would no longer allow subscribers to purchase unlimited internet plans. [21] By 2023, operators had indeed ceased offering unlimited internet plans, though some offer unlimited plans exclusively for messaging.

Significant disparities in internet speed exist among differing regions in 2024. [22] There are no clear digital divides along religious or gender lines.

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**2**/6

The government has continued taking steps to centralize control over the country's internet infrastructure, after it restricted access to widely used social media platforms including Facebook, Instagram, and what was then called Twitter following the full-scale invasion of Ukraine in February 2022. During the coverage period, individuals had difficulty accessing messaging applications and the internet more broadly during protests. In August 2024, after the coverage period, the Federal Service for Supervision of Communications, Information Technology, and the Mass Media (Roskomnadzor) blocked Signal because it failed to remove "extremist" content from the platform. [23] YouTube was reportedly throttled that same month (see B1). [24]

In November 2019, a law aimed at achieving the "sovereignization" of the Runet [25] took effect. The law defines the status of and requirements for the "critical infrastructure" of the Runet, namely international communication lines and internet exchange points (IXPs). Their owners and operators are obliged to ensure the possibility of centralized traffic management in the event of "external threats"—a vague term authorities can potentially invoke to gain control over the relevant infrastructure for almost any reason. The law also provides for the creation of a Russian domain name system (DNS) as an alternative to the global DNS maintained by the Internet Corporation for Assigned Names and Numbers (ICANN), a US-based nongovernmental organization (NGO).

In the process of implementing of the 2019 Sovereign Internet Law, Roskomnadzor expanded its ability to censor the internet in Russia. The installation of Technical Measures to Combat Threats (TSPU) equipment, which is based on the use of DPI technology on telecommunications networks, allows Roskomnadzor to restrict access and block websites. A November 2022 report from University of Michigan's Censored Planet project and Arizona State University [26] identified 6,000 TSPU devices, which are produced by Roskomnadzor, on Russian networks. In contrast to China's Great Firewall, the researchers have noted that the TSPU is "a model of decentralized deployment, centralized control" because Roskomnadzor is able to use these devices to block websites unilaterally across a range of networks.

In January 2023, a law came into force that introduces fines for telecommunications operators who have not installed TSPU equipment (see A4). [27] A new measure set to take effect in September 2024, after the coverage period, prevents operators from providing services without installing TSPU equipment. [28] Also in January 2023, Reuters reported that a document circulated by the Ministry of Digital Development, Communications, and Mass Media (MinDigit) outlines plans to allocate 600 billion rubles ($660 million) to the TSPU system over the next five years. [29]

In October 2023, the Insider, a Russian investigative outlet that operates in exile in Latvia, reported that the government had acquired technology to conduct "protocol-based blocking" under TSPU. With the ability to block unique protocols that specific platforms rely on, the government can more easily block messaging services and social media platforms. [30]

In late January 2024, users in the Republic of Sakha (Yaktusk) reported WhatsApp and Telegram were inaccessible for several days, as residents protested against the murder of a local man. [31] Also in January 2024, WhatsApp and Telegram were inaccessible in the Republic of Bashkortostan, where residents were protesting the trial of environmental activist Fail Alsynov. The internet was reportedly inaccessible within several miles of the courthouse where Alsynov was being tried. An employee at a major telecommunications company reported the authorities had deliberately blocked WhatsApp in Bashkortostan and blocked Telegram across the country more widely because they could not block it locally. The authorities cited Roskomnadzor's maintenance work as the cause of the

disruption (see A1). The Roskomsvoboda digital rights organization reported access difficulties for both services in Kamchatka, Khabarovsk Krai, the Moscow region, Primorye, Sakhalin, St. Petersburg, and the Volgograd region. [32] At the end of February 2024, the authorities attributed a countrywide Telegram outage to the reconfiguration of Roskomnadzor systems. [33]

Internet access faltered during the funeral of opposition leader Aleksey Navalny, who died in a Russian prison, in March 2024. [34] Individuals experienced difficulties at the church where the funeral was held and nearby mass transit stations. When Navalny's body was carried into the church, several Telegram channels, including Navalny's Team, lost the ability to broadcast live. [35]

Following the full-scale Russian military invasion of Ukraine in February 2022, the Russian government restricted access to some social media platforms (see B1). In March 2022, Roskomnadzor fully blocked Facebook and Twitter, following the EU's order mandating social media platforms to block Russian-state affiliated media outlets in member states. [36] Later in the month, Roskomnadzor blocked Instagram. [37] In March 2022, a court in Moscow approved a request by the Prosecutor General's Office to recognize Meta, the parent company of Facebook and Instagram, as an "extremist organization." [38] The request was filed after Reuters published an article about Facebook's decision to temporarily permit posts containing death wishes or calls for violence against Putin, Belarusian president Alyaksandr Lukashenka, and the Russian military to remain on its platform. [39]

In July 2023, the government ran another test to disconnect the Runet from the international internet. [40] The government reported that the test was successful, though many international and government websites were inaccessible during the two-hour test. Previously, in June and July 2021, the Russian government began to test the feasibility of disconnecting the Runet from the global internet, and Russian state-affiliated media reported the tests were successful. [41] Then, in September 2021, Roskomnadzor requested that companies abandon Google and Cloudflare's DNS, and DNS over HTTPs (DoH) generally. In March 2022, the MinDigit ordered state media outlets to stop working with foreign hosting services, and adopt .ru domain names and DNS servers based in Russia. [42]

In August 2023, the government blocked VPN services using the OpenVPN and WireGuard protocols (see B1). Problems were observed for several days for most mobile service providers in different regions. **43** Previously, in January 2022, VPN users from several regions reported problems connecting to VPN services, **44** possibly indicating that protocol blocking was being tested within TSPU.

In June 2023, the government announced plans to launch a "secure internet," which will be available only to citizens who register with their passports (see C4). **45** According to Andrey Svintsov, the deputy chairman of the State Duma Committee on Information Policy, Information Technologies, and Communications, users will only be able to access websites and services that fully comply with existing Russian legislation, though it will not replace the existing internet. **46** As of the end of the coverage period, the project has not been launched.

In April 2023, Radio Free Europe/Radio Liberty (RFE/RL) reported that Russian and Chinese officials had shared censorship strategies, with Russian officials aiming to learn how to more effectively restrict VPNs and censor messaging applications. **47**

In March 2021, Roskomnadzor used its DPI equipment to throttle the loading speeds for Twitter in order to punish the platform for what the regulator said was systematic noncompliance with content removal requests (see B1). **48** From 2018 to 2020, the government ordered the blocking of Telegram, a popular messaging application, but it was never fully implemented.

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**1** / 6

Russia's information and communication technologies (ICT) market is concentrated due to regulatory and economic constraints.

Telecommunications providers are licensed by Roskomnadzor. **49** The costs of complying with data-retention requirements under the 2016 Yarovaya Law (see A2 and C6) and the installation of DPI systems under the 2019 law on a sovereign Runet created a financial hardship for existing service providers and a deterrent to

potential new entrants to the market (see A3 and B1). In July 2023, Roskomnadzor announced that it would begin fining providers who do not install TSPU equipment between one and five million rubles ($11,240 and $56,120), after an amendment to the administrative offenses code took effect in January 2023. [50] Additionally, directors of these companies can face up to three years in prison and their companies can be audited if they refuse to install TSPU equipment. [51] Previously, companies spent more than 20 billion rubles ($327.8 million) installing TSPU equipment between 2019 and 2022. [52] Telecommunications service operators will soon be prohibited from providing services without installing TSPU as of September 2024, after the coverage period. [53]

In June 2022, the MinDigit proposed packages of amendments that could lead to further market concentration; these measures took full effect by January 2024. The first of these provides fines for operators that do not install the System for Operational Investigate Measures (SORM), a system developed in various forms since the early 1990s, which allows the government to conduct surveillance (see C5). [54] This system involves storing user traffic and must be approved by the Federal Security Service (FSB). For the first violation, a fine of 0.001 to 0.003 percent of annual revenue is provided. For repeated violations, a fine amounts to 0.01 to 0.03 percent of annual revenue. Service providers must work with the FSB to build a plan for SORM implementation within six months of receiving a license. Roskomnadzor is tasked with monitoring operators' compliance with the measures. [55] The second set of amendments proposed changes to the tax code, which would raise the state tax on "nine types of licenses for communication services" from 7,500 to one million rubles ($84 to $11,220). [56] The State Duma ultimately approved the changes in September 2023. [57]

In the second quarter of 2023, the four largest ISPs—Rostelecom (36 percent), MTS (13 percent), ER-Telecom (12 percent), and Vimpelcom (8 percent)—accounted for 69 percent of the subscriber base of broadband internet access in the business-to-consumer segment in Russia, according to TMT Consulting. [58] In October 2023, Netherlands-based Veon completed its sale of Vimpelcom to its local senior managers, leaving the Russian ICT market entirely. [59]

In June 2022, law enforcement reportedly announced they would not allow the companies Antares, Integral, and Arctur to use 1900–1920 MHz frequencies. They

had planned to use the frequencies to launch a new telecommunications operator. [60]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Roskomnadzor, which regulates the ICT and media sectors, often fails to act fairly or transparently. The agency is under the control of the MinDigit, meaning it has little to no independence from the government.

Roskomnadzor is responsible for implementing the many laws regulating the internet in Russia, including those governing the blocking of online content (see B1 and B3) and the localization and retention of user data (see C6). [61] Roskomnadzor's blocking procedures are not transparent. Often, access restrictions are implemented in violation of procedural rules, including blocking websites without informing their owners. In March 2020, Andrey Lipov was appointed as the new head of the agency. Previously Lipov ran the Presidential Directorate for the Development of Information and Communication Technology and Communication Infrastructure, a key initiator of the law on the sovereign Runet. Several of the directorate's deputy managers also joined Roskomnadzor. [62]

Roskomnadzor's powers have gradually expanded under the Runet law. A body called the Center for Monitoring and Management of Public Communication Networks, which is primarily responsible for the management of data on network infrastructure, [63] was formed within the agency as part of the legislation. [64] At the same time, the Main Radio Frequency Center (GFRC), a preexisting body subordinate to Roskomnadzor, has become responsible for the operation and maintenance of special equipment that ISPs must install in accordance with the law. [65]

The Runet law also gave Roskomnadzor a new role as the government representative at Russia's country code top-level domain (ccTLD) registrar, which administers the .ru and .РФ domains. [66]

In May 2022, President Putin appointed former president Dmitry Medvedev as the head of a newly created interdepartmental commission focused on establishing the technical sovereignty of critical information infrastructure, and ensuring that infrastructure can operate independently of the global internet. [67]

There are several ICT industry associations in Russia, including the Russian Association for Electronic Communications and the Association of Trading Companies and Manufacturers of Household Electrical Equipment and Computers, but they do not have a strong influence on policymaking.

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**1** / 6

Following the full-scale invasion of Ukraine in 2022, Russian authorities intensified their efforts to block access to websites and social media platforms that could host material critical of the authorities or of the invasion, as well as international news sites, civil society websites, and Ukrainian news sites. As of 2023, the number of blocked sites increased by another 219,000. By November 2023, [68] the number of sites blocked by military censorship exceeded 15,000. [69] According to data from April 2024, there are more than 17,000 domain names in the united registry, which logs most banned websites. [70]

Websites featuring content that touches on a host of sensitive topics are subject to blocking under the Law on Information, Information Technology, and Information Protection and associated legislation. Forbidden content formally includes child sexual abuse images; content related to the illegal sale of alcohol; information about illegal drugs; information about illegal gambling; calls for suicide; calls for broadly defined extremist activities, riots, or unsanctioned protests; violations of copyright; violations of data protection legislation; and information about skirting online censorship (see B3). A 2015 law allows the government to designate foreign organizations as “undesirable,” which bars them

from disseminating information (see B3 and B6). In some cases, these organizations' websites are blocked. [71]

Rules requiring companies to store Russian users' personal data on Russian territory (see C6) are invoked by the government as a pretext for restricting access to certain websites. [72]

Roskomnadzor orders the blocking or directly blocks most websites, but other state bodies, including the Ministry of Internal Affairs, [73] the Ministry of Justice and the Prosecutor General's Office, [74] are empowered to order the blocking of web content (see B3). The courts also have wide latitude to block web content.

Before the Russian presidential election in March 2024, websites were blocked, including projects by Navalny supporters. In December 2023, the "Russia without Putin" website, operated by the Navalny-founded Anti-Corruption Foundation, was blocked along with several election-related websites. [75] Similar blockings were observed through March 2024, when the election took place. [76]

Between the start of the invasion of Ukraine and April 2022, the Russian government blocked social media platforms including Facebook, [77] Facebook Messenger, what was then called Twitter, [78] and Instagram. In August 2024, after the coverage period, Roskomnadzor blocked Signal because it failed to remove "extremist" content from the platform (see A3). [79]

In a first wave of website blocking following the full-scale invasion of Ukraine in February 2022, authorities blocked a large number of media sites, including those belonging to the Russia-based student magazine DOXA, [80] the British Broadcasting Corporation (BBC), Voice of America (VOA), Deutsche Welle, Bellingcat, Paper, Meduza, Mediazona, Interlocutor, RFE/RL, Echo of the Caucasus, Republic, Taiga.Info, 7x7 Horizontal Russia, and the Village. Authorities also blocked civil society websites, such as Amnesty International's Russian-language website, For Human Rights, the election observation organization Voice, and Human Rights Watch (HRW). [81] At the end of March 2022, the government blocked Google News after Google announced that it would no longer permit users to monetize content that "exploits, dismisses, or condones the invasion," though access was later restored. [82] Also in March 2022, the government blocked Kazakhstani, Tajikistani, Turkmen, and Uzbekistani outlets under the umbrella of RFE/RL, which

was later recognized as an "undesirable organization" in February 2024 (see B6). [83]

In August 2022, Roskomnadzor blocked the True Story, a prodemocracy news site created by the former head of Yandex.News. [84] In January 2023, Amnesty International's website was also blocked. [85] In February 2023, the government blocked access to the Bell, a prominent online news outlet. [86] The website of Greenpeace, which was named an "undesirable organization," appeared on a blocking list in May 2023 (see B6). [87]

In June 2023, an unspecified government agency ordered the blocking of Medium, the blogging platform, and it was included in the register of prohibited information. [88] Later, Roskomnadzor explained the blocking was due to the failure to remove unreliable materials about the invasion of Ukraine. Also in June 2023, several service providers again blocked Google News as Yevgeny Prigozhin, leader of the Russian paramilitary Wagner Group, and Wagner Group fighters marched toward Moscow. [89] Later in the month, Roskomnadzor blocked news sites linked to Prigozhin, including RIA FAN, Politics Today, Economy Today, Neva News, and People's News. [90]

During the coverage period, the government continued blocking independent media outlets and human rights organizations. In 2024, SovaVision and the affiliated SOTA news site were blocked by Roskomnadzor over coverage of the war against Ukraine. [91] In September 2023, Roskomnadzor blocked access to the Kyrgyzstan-based news outlet 24.kg and the Tajikistan-based outlet Payom because of their coverage of the war in Ukraine. According to Roskomsvoboda, Roskomnadzor initially ordered the blocking of four 24.kg articles and two Payom articles in November 2022 and May 2023, respectively. [92] Also in September 2023, Roskomsvoboda reported that the website of the British *Daily Express* newspaper appeared on the register of prohibited information and was blocked. [93]

In February 2024, the Ministry of Justice ordered the blocking of human rights group OVD-Info's website, [94] which had its original website blocked in December 2021 and was recognized as a foreign agent in 2023. Also in February 2024, an unspecified government body blocked a website related to the 2022 documentary *Navalny*. [95] In March 2024, the Memorial Human Rights Center (PTM) was

blocked by Roskomnadzor; [96] earlier in November 2023, one of its special projects, which discussed the full-scale invasion of Ukraine, was also blocked. [97]

In June 2024, after the coverage period, Roskomnadzor blocked 81 EU-based outlets, including *Der Spiegel*, *Le Monde*, *Politico*, and *La Repubblica*, in retaliation for the EU's May 2024 blocking of Russian outlets. [98]

The authorities have also blocked well-known Ukrainian websites, including news sites. Prior to the invasion, the Prosecutor General's Office had ordered the blocking of popular Ukrainian internet television channel Hromadske (Public) for posting "extremist" information. [99] In March 2022, that office blocked the websites of Ukraine's Ministry of Health, Dnipro State Agrarian and Economic University, and Ukrinform, Ukraine's national news agency. Authorities blocked major Ukrainian news sites and portals, including Correspondent.Net, Ukrayinska Pravda, Left Coast, Novoye Vremya (nv.ua), Depo.ua, Gazeta.uA, Focus.uA, Zakhid.Net, and UAinfo. [100]

During the coverage period, the government continued to block Ukrainian websites. At the end of 2023, several Ukrainian educational services were blocked in Russia, including a service for distance learning and a platform with video lessons for schoolchildren. [101] In January 2024, the website of the Ukrainian Orthodox Church was blocked in Russia [102] for inciting hatred. [103]

The government continues to block LGBT+ sites after declaring the global movement as an "extremist organization" in November 2023 (see B3). [104] Roskomnadzor announced that month that it would begin to block pirated sites for content deemed to contain LGBT+ "propaganda," but such blocking was recorded several months earlier. [105] The Open Observatory of Internet Interference noted that Roskomnadzor blocked Nuntiare et Recreare, a website dedicated to LGBT+ members of various religious affiliations, and the site of the Museum of LGBT History in July 2022. [106]

The Kremlin has also blocked platforms for allegedly hosting illegal content. In February 2024, the community page of Steam, the video-gaming client, was blocked for promoting drug manufacturing. [107] The site was later unblocked after the violations were addressed according to Roskomnadzor. In February and March 2023, Roskomnadzor began blocking several images from stock photograph

websites Alamy and Depositphotos due to content deemed to suggest acts of suicide. [108] In February 2023, Shutterstock was blocked, though access was later restored. In August 2022, Roskomnadzor began blocking Patreon. In September 2022, Soundcloud was added to the blocking list for hosting "false information" because the website hosted Radio Svoboda, RFE/RL's Russian-language program. [109] Also in September 2022, the Prosecutor General's Office also ordered the blocking of Grammarly, which uses artificial intelligence (AI) to edit texts users submit to the platform. Grammarly was founded in Ukraine, had donated revenue earned from business in Russia and Belarus to Ukraine, and had developed a feature urging users to support Ukraine. [110] Russian authorities claimed they blocked the website because it was spreading false news about the invasion. [111]

In January 2024, Roskomnadzor blocked the websites of the US Central Intelligence Agency (CIA), the US Federal Bureau of Investigations (FBI), and "a number of resources belonging to state structures of 'hostile' countries for disseminating material aimed at destabilizing the social and political situation in Russia." [112] Roskomnadzor alleged that the CIA and FBI had published false information about the invasion.

Though blocked websites can be accessed via VPN services, Roskomnadzor has blocked a large number of these services (see C4). As of March 2022, 20 popular VPN services were blocked in Russia. [113]

In June 2022, Proton VPN and NordVPN users reported problems accessing services. Later, Roskomnadzor confirmed that it had restricted access to Proton VPN and several other VPNs, the names of which were not announced. [114] At the end of May 2023, VPN users reported that the OpenVPN protocol, which several VPNs rely on, was blocked. The protocol is used by banks and other private companies in Russia. [115] In August 2023, reports emerged that OpenVPN and WireGuard, another VPN protocol, were blocked by major mobile service providers (see A3). [116]

In March 2024, a law banning the promotion of bypass-blocking methods came into force. Almost immediately, websites that offered VPN services or posted instructions for installing them faced blocking (see C4). [117] Roskomnadzor blocked more than 30 links for this in one month, most of which concerned instructions on how to access Facebook and Instagram. [118] In April 2024, the

websites of at least eight more VPN services were blocked, including Outline and Amnezia. [119] Since December 2021, access to the Tor Project website has been blocked in Russia. [120] In July 2022, it was unblocked for two weeks, and then became blocked again. [121]

In September 2021, ahead of elections to the State Duma, Roskomnadzor employed DPI equipment to block the Smart Voting website of Aleksey Navalny. [122] That same month, ISPs began blocking Google Docs and telegra.ph, a Telegram tool that allows users to post multimedia stories. [123]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**0** / 4

During the coverage period, Roskomnadzor continued to mandate the removal of online content, including content related to the invasion of Ukraine, LGBT+ rights, and the political opposition. However, many of the platforms that Roskomnadzor issued demands to in the past are now blocked (see B1). When companies have refused to comply, courts have issued escalating fines. Prior to the invasion, Moscow had already attempted to compel social media platforms to remove content. These companies' decisions to restrict access to Russian state media outlets in the EU and elsewhere, however, led to their outright blocking (see B1) in some cases, and heftier fines in others.

The introduction of the law preventing the spread of false information about the Russian military (see C2) and the government's order to refer to the war as a "special military operation" in 2022 has led to further content removal. Articles punishing "fake news" and defamation of the authorities were added to the code of administrative offenses in 2019 (see C2), and these have been actively employed to intimidate users and outlets into taking down content.

In 2023, Russian social networks deleted more than 124,400 items at the request of Roskomnadzor, according to the agency. [124] These requests concerned broadly defined extremist and terrorist content, which can include criticism of the war or the government, materials about suicide and drugs, and child pornography. More

broadly, Roskomnadzor's report for 2023 states that over 558,000 links containing illegal content were identified during the year, 73,500 of which contained "fake information about a special military operation," and 104,000 contained information about drugs. Additionally, 19,000 contained content deemed LGBT+ "propaganda."

To remove some of the content during the coverage period, regulators employed the Vepr and Oculus systems (see C5). [125] In February 2023, Roskomnadzor's GFRC began internal testing of the Vepr system, which is designed to "search for and neutralize information bombs." [126] The system aims to counter information that "creates a threat of harm to the life and/or health of citizens and property or the threat of a mass violation of public order and/or public safety." [127] In February 2023, the GFRC announced that the Oculus system, a surveillance tool, can allegedly identify information in images or video that violates Russian law, which could lead to further content removal. [128]

During the coverage period, Russian courts continued to issue fines to foreign companies and NGOs for failure to remove content prohibited in Russia. In December 2023, Telegram was fined four million rubles ($44,900) for failing to remove information about the losses of the Russian army in Ukraine. [129] In January 2024, Twitch, a live-streaming platform that hosts video-game and other content, received two fines totaling four million rubles ($44,900) for failing to remove prohibited information. [130] For refusing to remove allegedly "extremist" books from Apple Books, Apple was fined 800,000 rubles ($8,980) in January 2024. [131] Viber, the messaging application, received the same fine in March 2024. [132] Fines against Wikipedia also continued. In January 2024, the Wikimedia Foundation was ruled to have failed to remove prohibited information and was fined three million rubles ($33,670). [133] In May 2022, Roskomnadzor issued a four-million-ruble ($44,900) administrative fine against the Internet Archive, an American organization that preserves online content, because of its refusal to remove content prohibited in Russia. [134]

The Kremlin continued to issue fines to Alphabet, Google's parent company, as YouTube remains popular in Russia. A May 2024 report from Svoboda, RFE/RL's Russia-focused outlet, revealed that YouTube had removed videos with guidance on how to avoid conscription from several channels, though some were later reinstated. [135] In December 2023, the Tagansky District Court fined Google fined

4.6 billion rubles ($51.6 million) because the company refused to remove information about the invasion of Ukraine, LGBT+ content, and other material deemed "extremist." [136] In April 2024, a Moscow court rejected Alphabet's appeal of the fine. [137] Earlier in December 2023, Google received several fines totaling more than eight million rubles ($89,790) because it failed to remove YouTube videos about the Russian invasion of Ukraine. [138] In May 2023, a court fined Alphabet three million rubles ($38,600) because YouTube had failed to remove content promoting LGBT+ information as well as news about the invasion of Ukraine. [139] In September 2024, after the coverage period, the Tagansky District Court fined Google and Discord 3.4 million rubles ($38,160) for failing to remove "banned" information. [140] This followed a five-million-ruble ($56,120) fine issued to Google and TikTok by the same court in July 2024, after the coverage period, for the same reason. [141]

Previously, in July 2022, the Tagansky District Court issued a fine of 21.1 billion rubles ($350 million) to Alphabet for failing to remove content, [142] with the order specifically noting YouTube's refusal to remove "fake" news about the war in Ukraine. [143] In May 2022, Google's Russian subsidiary filed an application for bankruptcy to a Moscow court, [144] prompting Russian authorities to seize the company's bank account. [145] The decision to file for bankruptcy stemmed from Google's failure to pay a fine of 7.2 billion rubles ($98 million), which was ordered in a December 2021 by a Moscow court and calculated based on Google's annual turnover in Russia. In this case, Roskomnadzor alleged Google had repeatedly failed remove "prohibited" information.

In December 2022, a law banning LGBT+ "propaganda" came into force (see B1), and in 2023, the authorities began issuing administrative protocols for demonstrating and promoting "nontraditional sexual relations" in films and television shows. In the second quarter of 2023, 33 protocols were issued against Russian online movie and television broadcasters, including Beeline TV, Ivi, MegaFon TV, More.tv, Start, TV-3 Russia, and TNT Music. [146]In January 2024, Roskomnadzor reported [147] issuing fines against television channels and online cinemas amounting to more than 50 million rubles ($561,200) and those against streaming services amounting to 30.5 million rubles ($342,300). [148] In September 2023, Roskomnadzor launched a form for complaints about LGBT+ content. [149]

Russian search engines and platforms routinely remove content, including content related to the war. A July 2023 report from the University of Toronto's Citizen Lab found that takedown orders issued to VK, which is effectively owned by the state through Gazprom and Sogaz, had increased by 3,000 percent since the start of the invasion. According to the report, VK blocked 94,942 videos, 1,569 community accounts, and 787 personal accounts in Russia, [150] including a significant amount of content related to the invasion, Belarusian issues, and LGBT+ terms. Likewise, leaked source code from Yandex revealed the search engine prevents search terms critical of Putin from leading users to images of him. The leaked code also showed that when users search the symbol "Z," the search engine hides terms associated with Nazism. [151] In June 2023, VK restricted a statement shared by Yevgeny Prigozhin prior to his death and Yandex deindexed search results about him. [152] In 2020, VK debuted an algorithm that automatically removes images included in the federal list of extremist materials from users' posts. [153]

Apple and Google have removed applications from the App Store and Google Play, respectively, at the request of Roskomnadzor. In July 2024, after the coverage period, Apple removed 25 VPN applications, including Hidemy.name, Red Shield, and AdGuard, based on a request from Roskomnadzor (see C4). [154] In March 2024, immediately after the presidential election, Apple, at the request of Roskomnadzor, removed the Anti-Corruption Foundation's Photon-2024 application, which was developed to facilitate protest voting, from the App Store. [155] In December 2022, Google was ordered to remove the Tor Browser app from its app store. [156] In September 2021, both Apple and Google removed the Smart Voting application, which was promoted by Navalny ahead of the year's State Duma elections. [157]

Since 2022, due to sanctions, the App Store and Google Play began to remove applications of Russian platforms, banks, [158] and other services. In September 2022, Apple removed VK from its app store to comply with sanctions issued by the United Kingdom, [159] but it was reinstated shortly after. [160]

During the coverage period, Russian authorities continued to require foreign platforms to remove content through formal channels. According to Google's transparency report, the government issued 36,780 takedown requests covering 354,644 items in the first half of 2023 and 25,925 requests covering 299,014 items in the second half. [161] Google removed 47.7 percent of requests filed in the first

half of 2023 and 55.5 percent of requests in the second half. According to the report, "national security" was the leading reason for these requests, amounting to 51 percent of requests in the first half of the year and 41 percent in the second half. [162]

Meta, which has been recognized as an extremist organization, initially satisfied one content removal request from the Russian government in 2023, but later reinstated the content. [163] Microsoft received 477 requests to remove content in the first half of 2023, complying with 319 of them. [164] At the end of 2023, Russia contacted GitHub, a code repository, three times with a request to remove content. [165]

According to its transparency report covering the first half of 2023, Yandex removed 190,000 links from search results at the request of Roskomnadzor, 40,000 more compared to the same period in the previous year. [166] In November 2023, Yandex Music published its first transparency report; it reported removing over 4,000 pieces of content, including songs, videos, podcasts, and album artwork, at the request of authorities in the first three quarters of 2023. [167] The service also stated that it is obligated to remove content within 24 hours of receiving a request from the authorities.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

The government in general and Roskomnadzor in particular justify website blocking and filtering under a range of laws and regulations. The legal framework generally does not provide clear criteria for evaluating the legality of content, and authorities do not always offer a detailed explanation for blocking decisions. Website owners have the right to appeal decisions in court, but they are often given a short time to do so. Furthermore, the judiciary's lack of independence limits the possibilities for redress through the appeals process.

Roskomnadzor serves as the primary regulator of online content, ordering the blocking of websites and the removal of content based on complaints about "illegal" information from state entities, individuals, and businesses. Roskomnadzor also directly blocks websites using TSPU, a practice that has

become more common since the Sovereign Internet Law (See A3). The agency adds most blocked websites to a registry of blocked sites, which are only accessible to ISPs, search engines, and other intermediaries. [168] However, the regulator increasingly blocks websites directly without adding them to the registry.

The government grants the authority to block various categories of online content to several state bodies. The judiciary also handles blocking orders from other agencies; as well as the Prosecutor General's Office; the Federal Service for Surveillance on Consumer Rights Protection and Human Well-Being (Rospotrebnadzor); the Ministry of Internal Affairs; the MinDigit; the Federal Service for Alcohol Market Regulation; the Federal Tax Service; and the Federal Agency for Youth Affairs (Rosmolodezh). [169] December 2022 amendments to the "foreign agents" law (see B6) empowered the Ministry of Justice to order Roskomnadzor to block websites without obtaining a court order. [170] In June 2023, the Ministry of Justice itself began blocking websites, even though no law supports the practice. [171]

Empowered state agencies can order Roskomnadzor to block content that touches on political and social issues enumerated in the Law on Information, Information Technology, and Information Protection, plus related legislation, including legislation prohibiting "fake news" and content that defames the authorities (see C2). In November 2022, entries began to appear in the blocking registry without indicating the authority that issued the blocking demand, which had previously been standard practice. [172]

In 2021, President Putin signed amendments to the to the Law on Information, Information Technologies, and Information Protection granting the authorities extended powers to block websites without a court order. Amendments signed the same year allow prosecutors' offices to force websites to remove "defamatory information" within a certain time period and to block those websites if they fail to comply. [173] Also in 2021, Putin signed a law allowing the Prosecutor General's Office to extrajudicially block websites that engage in "substantiation and (or) justification for the implementation of extremist activities, including terrorist activities."

In March 2024, a law prohibiting information about bypassing blocking came into force. The law also includes a ban on advertising VPN services. In the month since the law came into force, more than 30 links were banned (see B1). [174]

In January 2024, a bill was introduced to the State Duma which would transfer the powers of the MinDigit to Roskomnadzor, with the bill's authors saying the blocking process would also be faster. [175] In June 2024, after the coverage period, the bill was approved by the State Duma in its third reading and will come into force in October 2024. [176]

In December 2022, Putin signed a law banning "LGBT propaganda," adding the term to the list of information that is illegal to distribute online (see B1 and B2). [177] This includes information promoting "nontraditional sexual relations," and transgender identity alongside acts like "pedophilia." The law, which expands on a 2013 law addressing "propaganda of nontraditional sexual relations" among minors, gives Roskomnadzor the authority to order website blocks or content removal.

In November 2019, Putin signed a law that extended the state's regulation of media outlets designated as "foreign agents" to include individuals who "spread information to an unrestricted number of persons, namely on the internet, and receive funding from abroad." [178] The law empowers the government to block "foreign agents'" websites, and potentially their social media accounts. [179] In March 2023, a decree drafted by the Ministry of Digital Transformation, which enables Roskomnadzor to block mirrors of previously blocked sites, came into effect. [180] By April 2023, Roskomnadzor reported blocking more than 3,500 mirrors of "foreign agents'" websites. [181]

In February 2022, the Ministry of Internal Affairs determined a mechanism for blocking websites containing personal data of persons under state protection. [182] Roskomnadzor was recognized as responsible for entering such sites into the register of prohibited sites; under the mechanism, the regulator is obliged to make an appropriate entry in the register, within 24 hours from the date of receipt of the decision to recognize information as prohibited, and the decision to restrict access to it.

Roskomnadzor can issue warnings to organizations officially designated as mass media if they are deemed to abuse their position. [183] Article 4 of the Law on Mass Media indicates that such abuse can include, among other things, incitement to terrorism, extremism, propaganda of violence and cruelty, information about illegal drugs, and obscene language. If a media outlet receives two warnings within a year, Roskomnadzor has the right to apply for a court order to shut it down.

In July 2021, Putin signed a law obliging foreign technology companies with more than 500,000 Russian users to open representative offices in Russia. [184] Foreign companies face a variety of penalties for noncompliance with the physical-representation requirement, which took effect in 2022, including a ban on search results, restrictions on accepting payments from Russian residents, complete blocking, [185] and fines of up to 20 percent of their annual Russian income. [186] Under another measure, companies must register with Roskomnadzor and add an electronic form on their website to facilitate feedback from Russian citizens or organizations. [187] By February 2022, Apple, Spotify, Viber, TikTok, Likeme, and Twitter had announced that they were taking measures to comply with the measures. [188] However, many of these companies later withdrew from the Russian market following the invasion of Ukraine.

In March 2021, Putin signed a law empowering the Central Electoral Commission and regional electoral commissions to send content removal requests to Roskomnadzor. The law increased fines for illegal electoral campaigning to as much as 500,000 rubles ($5,610). [189]

In February 2021, a law took effect compelling social media companies to coordinate their content moderation efforts with Roskomnadzor, which was tasked with establishing a special e-service for that purpose. When a user issues a complaint about "prohibited content" (for example, online gambling, illicit sales, or material that disrespects society or the state), the company must block it pending a review from Roskomnadzor. The agency will then notify the user who posted the content that it is being reviewed. [190]

A law signed by Putin in late 2020 proscribes fines for failure to remove content prohibited by Roskomnadzor. Fines can reach up to a fifth of a company's revenue in Russia for the calendar year preceding the year in which the violation was discovered. [191]

A 2021 amendment of the administrative offenses code imposes sanctions for alleged censorship of Russian media by foreign online platforms. Those who violate that restriction can face fines ranging from 600,000 to three million rubles ($6,730 to $33,670) for each particular action. This regulation also empowers Roskomnadzor to "restrict access to online resource fully or partially using the technical means for countering threats (i.e., DPI equipment)." **192**

In March 2022, against the backdrop of the invasion of Ukraine, Russia announced its withdrawal from the Council of Europe (CoE), which means Russians can no longer appeal the decisions of national courts to the European Court of Human Rights (ECtHR), **193** and it was expelled from the body a day later. In June 2022, the State Duma adopted a package of bills on the nonenforcement of decisions of the ECtHR in Russia that entered into force after March 15, 2022. **194**

Russians can still apply to the ECtHR if it concerns violations that occurred before this date. In the case of the slowdown of Twitter traffic in 2021 (see A3), a class action complaint was previously filed in Russian courts. **195** In February 2024, the ECtHR notified Roskomsvoboda's lawyers that it had registered a collective complaint from Russian users about the throttling of Twitter, now known as X. **196**

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Laws prohibiting extremist materials and other content, as well as the implementation and expansion of the "foreign agents" law, have contributed to self-censorship online, particularly with regard to sensitive political, economic, and social topics such as the invasion of Ukraine and mobilization, poor governance, corruption, human rights violations, religion, and the LGBT+ community. The vague wording of laws that touch on online expression, the arbitrary manner in which they are enforced, and the general ineffectiveness of judicial remedies make ordinary users more reticent to express themselves online. **197** The government's crackdown on online news media, as well as social media, has exacerbated self-censorship among journalists in particular.

The adoption of laws criminalizing the dissemination of "fake news" about the Russian invasion of Ukraine and preventing the dissemination of nonofficial

information about the war (see C2) further contributed to an environment of self-censorship. Media outlets and individuals who use the term "war" or "invasion" to describe the Russian military's actions in Ukraine face the risk of criminal prosecution. Additionally, media outlets can have their website blocked (see B1). After the adoption of these laws, several media outlets were blocked and threatened with closure due to using "war" or "invasion" instead of "special military operation." Administrative and criminal cases have been opened against several individuals (see C3). [198]

The implementation and expansion of laws that penalize and restrict "foreign agents," which includes individuals and organizations that receive funding from abroad, and "undesirable organizations"—a term often applied to organizations and media outlets that criticize the government—also fuel self-censorship (see B6 and C3).

Prominent Telegram channels can also be pressured to self-censor (see B2). A March 2023 report from Meduza and the Bell noted that administrators had deleted 5,500 posts about Rostec, and had come under pressure from Vasily Brovko, a Rostec director. In some cases, administrators have been prosecuted (see C3), while in others they have removed content in exchange for bribes. [199]

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**0** / 4

Government manipulation, which became more aggressive following the invasion of Ukraine, distorts the online information landscape. Authorities continued to use paid commentators and automated "bot" accounts to influence online content. Additionally, following the invasion of Ukraine, Roskomnadzor banned the use of information from unofficial sources and mandated that all media use the wording "special military operation" to refer to the war (see B4). [200] Further, the government has spread propaganda about conscription as war continued. The Russian government and affiliated online platforms have also co-opted the practice of fact-checking to further spread disinformation, debunking supposed "Ukrainian disinformation" and providing "facts" about events that purportedly occurred. [201]

Meta's adversarial threat report for the second quarter of 2023 [202] noted a disinformation campaign dubbed "Doppelganger," which largely targets European countries. The Doppelganger campaign, a term coined by the EU Disinfolab, [203] initially targeted the United Kingdom and EU member states, mimicking popular news outlets in those countries. The campaign later expanded to target US and Israeli entities and share original articles, videos, and memes that disseminate disinformation about the Kremlin's invasion of Ukraine on social media and via messaging services. A May 2024 report from Qurium highlighted the role UK- and EU-based companies play in setting up shell websites for Doppelganger. [204] In Meta's threat report for the second quarter of 2024, the company identified several coordinated inauthentic behavior campaigns originating in Russia, noting that Doppelganger has spoofed a wider range of sites and used geofenced websites and nonpolitical content to avoid enforcement. [205] Meta previously linked the campaign to the private companies Structura National Technologies and Social Design Agency. [206]

Meta's report for the third quarter of 2023 revealed a network of bots originating in Russia that targeted English-speaking users worldwide on its platforms as well as Telegram, TikTok, YouTube, and X. Meta linked the network to employees at RT, a state-owned media outlet. The network created inauthentic pages that promoted Russian government propaganda about the war in Ukraine, criticized transgender rights, and supported Moscow's interests in West Africa. [207]

In June 2024, Viginum, the French government's agency to address disinformation, published a report detailing the "Matryoshka" campaign, which was comprised of a network of accounts that posted French-language comments with links to false articles. The campaign sought to discredit fact-checking organizations, news agencies, and individuals. Matryoshka-related articles primarily spread narratives critical of Ukraine and France's support for Ukraine, while also criticizing French politicians and the Paris Olympics. The campaign had been active since at least September 2023. [208]

Likewise, a June 2024 report from Check First and Reset Tech, in collaboration with partners in media and civil society, identified a sophisticated campaign employing networks of inauthentic Russia-linked websites, Telegram channels, and X accounts to promote Russian propaganda. The campaign, dubbed "Operation Overload," shared inauthentic content with fact-checking and media organizations

and spread pro-Russia propaganda on X and Telegram. These narratives have primarily targeted France and Germany. Check First and Reset Tech began their investigation after reporting on the Matryoshka campaign emerged. [209]

In February 2024, ESET reported that a Russia-aligned group conducted an email campaign targeting Ukrainians in November and December 2023; that group sought to convince recipients there were food and drug shortages. [210] Moreover, a March 2024 *The New York Times* report noted that Russia-linked groups had promoted the narratives of journalists who purportedly reported on illicit financial dealings of Ukrainian president Volodymyr Zelenskyy; the journalists in fact did not exist. [211]

A January 2024 study from Verstka demonstrated that at least 217,000 VK accounts belong to bots, which includes formerly authentic pages that have been hacked. The bots promote anti-Ukraine propaganda, support for the Russian government and authorities, and criticism of dissenting voices. [212] Additionally, in December 2023, Microsoft's Threat Analysis Center reported that doctored videos of American celebrities denigrating Ukrainian president Zelenskyy, which were purchased on Cameo, were gaining traction on VK. [213]

In December 2023, DFR Lab and BBC Verify reported that a Russian influence operation on TikTok targeted former Ukrainian defense minister Oleksii Reznikov. At the time the videos were posted, he was an active minister and a legitimate scandal concerning the Ministry of Defense's inflated food budget had occurred. TikTok removed 12,800 accounts that had over 847,000 subscribers and labeled the operation as the "largest information operation ever uncovered on its platform." The videos employed AI-generated audio and were shared in at least seven languages. [214]

In November 2023, progovernment media spread propaganda that the United States could control the weather as a storm caused power outages affecting millions in Russia, according to a report from DFR Lab. That same month, Russian Telegram channels published deepfakes attempting to demonstrate a split between Valeriy Zaluzhnyi, then the armed forces chief and more recently Ukraine's ambassador to the United Kingdom, and Zelenskyy. [215]

In September 2023, progovernment media received instructions from the Putin administration to limit their coverage about a potential second mobilization. [216] A month later, media were ordered to refrain from writing about crimes committed by war participants after returning from the front. [217]

Yevgeny Prigozhin's June 2023 march towards Moscow, his subsequent expulsion from Russia, and his death in an August 2023 plane crash have left the fate of the Internet Research Agency uncertain. At the end of June 2023, Russian media began to report that Prigozhin had closed all of his companies based in Russia, including the Internet Research Agency, and fired all of its employees. [218] However, following Prigozhin's death, *Wired* reported that trolls that operated similarly to those linked to the Internet Research Agency promoted narratives in favor of Prigozhin on X. [219] Bot researchers did not record a decline in comments, but noticed that since May 2023, paid commentators who had voiced support for Prigozhin began to criticize his actions. [220] In March 2024, Google's Threat Analysis Group reported that influence operations linked to Prigozhin persisted after his death. [221]

A May 2023 joint investigation conducted by a consortium of French, German, Swiss, Danish, Norwegian, and Swedish news outlets obtained leaked documents indicating agents of the Russian government had infiltrated protests that were unrelated to the invasion of Ukraine, held signs in support of the invasion, and shared pictures of the protests on social media. [222]

Telegram has become increasingly popular since the invasion (see B7) and according to an October 2022 study from DFR Lab, 9 of the 10 most popular "political" Telegram channels in Russia spread Kremlin propaganda. [223] In December 2022, Putin established a working group on mobilization that included "military bloggers," who regularly spread pro-Kremlin propaganda. [224] In March 2022, online media outlet Fontanka reported that the Cyber Front Z Telegram channel had recruited people en masse to write comments in support of the actions of the Russian army. [225] Following this report, Meta removed 45 Facebook accounts and 1,037 Instagram accounts associated with Cyber Front Z. [226] Additionally, the Telegram channel Война с фейками ("War on Fakes"), which amassed 62,500 subscribers between the start of the war and early March 2022, claims to fact-check "the information war against Russia" but actually disseminates Moscow's talking points. [227]

Officials have also propped up newer platforms that are rife with disinformation. For example, in August 2022, State Duma deputy Anton Gorelkin promoted the launch of "Runiversalis," a website that mirrors Wikipedia's architecture but largely promotes Kremlin propaganda, including about the invasion of Ukraine. When the site was launched, Gorelkin stated it will follow "the requirements of the legislation of the Russian Federation and our traditional values. This means that any attempts to give the articles a left-liberal and Western-centric bias will be thwarted." Unlike Wikipedia, which Moscow has repeatedly tried to pressure to remove or alter content (see B2), only Runiversalis members may contribute to articles. [228] More recently, the government has promoted Ruwiki, a similar entity, as a feasible alternative. [229]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0**/3

Several economic and regulatory constraints limit users' ability to publish content online. Onerous regulations and restrictive laws—including the ever-expanding "foreign agents" law—affecting online news media have pushed some outlets to downsize, change owners, or exit the market altogether.

Since 2017, authorities have increasingly used the 2012 "foreign agents" law to limit users' ability to publish content online and have repeatedly expanded its scope. Russians are prohibited from reposting materials from "undesirable" organizations, publishing links, and providing financial support. The law initially required NGOs and other entities that received foreign funding in Russia to register as "foreign agents" and label their content or face escalating fines. [230] By June 2022, the law defined foreign agents as any individual or entity "under foreign influence," [231] and contained rules obliging media to identify "foreign agents" when they are mentioned in a publication. [232] In March 2022, the State Duma approved amendments that created a register with information about individuals considered foreign agents and people associated with them. [233] As of December 2022, [234] the Ministry of Justice gained the right to publish personal data of designated individuals and maintain a list of their affiliates. In June 2023, the State Duma's Committee on Foreign Interference revealed 861 people are listed as affiliates of "foreign agents" under the law. [235]

In August 2023, a law came into effect that outlines penalties for "persons under foreign influence" and prohibits individuals and state agencies from supporting entities recognized as "foreign agents." Violators will receive an initial warning, and then fines ranging from 30,000 to 300,000 rubles ($337 to $3,370). [236] In March 2024, Putin signed a law banning advertising on information resources of "foreign agents." [237] Violators face fines ranging from 50,000 rubles ($561) for designated individuals to 500,000 rubles ($5,610) for organizations. After this law came into force, journalist Alexey Pivovarov's "Redakcia" ("Editorial") project was forced to significantly change the format of its work because it struggled to attract advertising. Pivovarov himself left the project, and most of its employees were dismissed. [238]

The lists of "foreign agents" continue to grow. [239] At the end of May 2024, the list included 98 NGOs, 81 media outlets, 317 individuals recognized as media foreign agents, 83 additional individuals, and 23 unregistered public associations. The government has also revoked media licenses for outlets that fail to mention that organizations they cover have been placed on the "foreign agents" list. [240]

During the coverage period, the scope of the list of "undesirable organizations" was also expanded. The list includes the human rights organization Article 19, the Anti-Corruption Foundation, the Free Buryatia Foundation, Dozhd TV, and Radio Liberty. At the end of March 2024, there were 152 groups on this list.In 2023, the Ministry of Justice began employing a 2015 law to name media outlets and organizations, including Bellingcat, Insider, [241] Meduza, [242] the Andrei Sakharov Foundation, [243] Transparency International, [244] Greenpeace, and the Anti-Corruption Foundation [245] as "undesirable" organizations, which restricts their online activities and criminalizes the sharing of their content (see B4). Administrative fines range from 5,000 to 15,000 rubles ($56 to $168) for citizens, 20,000 to 50,000 rubles ($224 to $561) for officials, and 50,000 to 100,000 rubles ($561 to $1,120) for legal entities, [246] though repeated offenses can result in fines up to 500,000 rubles ($5,610) or four years of correctional labor. Participation in "undesirable" organizations' activities is also punishable under criminal law. In this case, the punishments are stricter: Fines start at 300,000 rubles ($3,370) and violators face prison terms as long as six years. [247] Throughout 2023, the Ministry of Justice added the World Wildlife Fund (WWF) [248] Agora, [249] and Novaya Gazeta Europe [250] to the list of "undesirable

organizations." In May 2024, prosecutors named Freedom House an "undesirable" organization. [251]

The Anti-Corruption Foundation, the Foundation for the Protection of Citizens' Rights, and the headquarters of the late Aleksey Navalny remain on the list of extremist organizations. The "international LGBT+ movement" was deemed extremist in November 2023. In February 2024, Russian courts handed down the first guilty verdicts associated with that designation (see C3). According to a February 2024 document from HRW, at least three LGBT+ groups have ceased operating as a result of this law. [252]

Users convicted of extremism or other offenses involving mass media or the internet are legally barred from serving as editors in chief at publications. [253]

Following the invasion of Ukraine, several social media platforms and other online platforms limited advertising services in Russia, preventing outlets and individuals from monetizing their content. For example, in March 2022, Google and its subsidiary YouTube stopped all advertising in Russia. [254]

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**1** / 4

The diversity and reliability of the online landscape deteriorated since the start of the Kremlin's full-scale invasion of Ukraine, as the range of news and opinion available to ordinary users has been severely curtailed by the government and social media platforms have been blocked (see B1 and B4). The government has also continued to order the blocking and removal of LGBT+ content (see B1 and B2).

According to Mediascope data as of February 2024, 85 percent of Russian residents use the internet at least once a month. [255] Research conducted in May 2022 suggests that Russians have become less trusting of television sources and more trusting of media consumed online since the invasion. [256]

Following the invasion of Ukraine, social media platforms, including Facebook, Twitter, and Instagram, were blocked. In October 2022, Roskomnadzor added Meta, which was labeled an "extremist" organization in March 2022, to the list of

"terrorist and extremist organizations," which means anyone who buys advertisements on Meta platforms could face up to 10 years in prison. [257]

Users of platforms that were blocked in the wake of the invasion primarily flocked to VK, which has hidden information about the war and criticism of the Russian government (see B2), and Telegram. In September 2022, VK purchased Zen and News from Yandex, two of the company's most popular services, further restricting diversity in the online space. [258]

Telegram has grown in popularity in recent years, with usage spiking after the Kremlin's full-scale invasion. According to a June 2024 report from DFR Lab, the top 15 Russia-focused channels on the platforms had a cumulative 16 billion views in 2021 and 109 billion views by 2023. The report also notes that these channels routinely share content from prominent Telegram channels, contributing to "an echo chamber" for Kremlin propaganda. [259]

Although YouTube is one of the most popular online platforms in Russia, the Kremlin used to promote RuTube, a competitor owned by state-owned Gazprom-Media, and VK Video. [260] Additionally, government authorities reportedly offered prominent YouTube and TikTok users $1,700 a month to use RuTube and Yappy, a Russian application that resembles TikTok, instead. [261] Though YouTube had not been blocked by the end of the coverage period, its speeds were throttled in August 2024 (see A3).

Other blocked websites include Ukrainian news sites, international news sites, and Russian news sites that tried to accurately report on the invasion (see B1). After the invasion, a wide range of media outlets shut down, reduced their coverage, or moved their websites outside of the Runet. Many became more active on Telegram. Even beforehand, many independent online media outlets within Russia were forced to shut down due to government pressure (see B4, B6, and C3). [262]

VPN users were able to access a diverse range of media and news sources in Russia. However, it has become more difficult for users to access internationally available VPNs since the Russian government intensified its efforts to block them in 2021. [263] March 2024 legislation further criminalizes the use and promotion of VPNs, and additional VPNs were blocked in August 2023 (see B1 and C4).

In April 2022, government agencies, including the Federal Tax Service, stopped accepting emails from foreign domains, citing fears of cyberattacks originating from abroad. [264] In February 2023, reports surfaced that major Russian companies and Russian state agencies were abandoning Google products and limiting employees' use of them, in favor of domestically produced alternatives. [265] In July 2023, the government mandated the preinstallation of the RuStore, VK's joint application with the MinDigit, on all phones. [266]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**2**/6

Although the internet remains a platform for activism in Russia, this function has come under significant pressure, particularly since the full-scale invasion of Ukraine. Those calling for demonstrations on the internet can face criminal or administrative penalties. Other tactics the government employs to constrain mobilization include cyberattacks against activists, blocking social media platforms, monitoring activists' social media profiles, placing informers in public or private chat groups that are used to organize demonstrations, harassing journalists who cover protests, and otherwise preventing journalists from gathering information about protests and protesters. [267] The authorities continue to prosecute individuals who organize and participate in protests, including those protesting the war (see C3). [268]

Law enforcement officials have searched protesters' phones and utilized facial-recognition systems in the Moscow metro to prevent people from protesting (see C5). [269] A September 2022 investigation by the *New York Times* also shed light on Roskomnadzor's efforts to surveil users that attend or organize protests (see C5). [270]

Authorities have taken a range of measures, including ordering website blocking [271] and content removal, [272] to stifle the late opposition figure Aleksey Navalny and individuals associated with his Smart Voting movement and the Anti-Corruption Foundation, which a Moscow court ruled qualified as an "extremist movement." In March 2022, Navalny was sentenced to nine years in a maximum-security prison on charges of fraud and contempt of court; [273] he died in custody

in February 2024. [274] After Navalny's funeral on March 1, 2024, attendees were detained by authorities in Moscow; [275] at least 15 people are known to have been detained, having been identified using a facial-recognition system. Additionally, users experienced issues accessing the internet (see A3). [276]

The designation of media outlets and NGOs as "undesirable" and "extremist" also threaten Russians' ability to organize online. For example, Russians cannot publish links to materials from "undesirable" organizations, share their content, or send donations without facing criminal liability (See B6). [277]

In November 2023, a law was signed prohibiting the use of websites previously blocked by Roskomnadzor for election campaigning. [278]

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**1** / 6

Although the constitution guarantees freedom of expression, [279] this right is subject to numerous legislative restrictions and is routinely violated. Censorship is nominally prohibited by the constitution. There are no laws that specifically protect online expression. Several restrictive laws, coupled with repressive law enforcement and judicial systems, have also eroded freedom of expression in practice (see C2).

Russia's judiciary is not independent. The courts tend to side with the government, including in cases where constitutional protections or provisions of international treaties apply. In 2019, the courts acquitted defendants in fewer than 1 percent of criminal cases. [280]

In March 2022, Russia was expelled from the CoE, [281] with the council's Committee of Ministers noting that Russian military actions in Ukraine represented a serious violation of Article 3 of the charter on the principle of the rule of law. The expulsion also means Russia is no longer party to Convention for

the Protection of Rights and Fundamental Freedoms. In June 2022, the State Duma passed a law invalidating ECtHR decisions made after March 15 of that year and stipulating that Russians will no longer be able to appeal to the court. [282]

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

Users in Russia can face civil and criminal penalties under a range of laws, the majority of which are contained in the criminal code and the code of administrative offenses. New laws and amendments that can be invoked in order to criminalize legitimate, nonviolent expression online are introduced regularly.

The criminal code imposes penalties, usually in the form of fines, for defamation (Article 128.1); slandering judges, public prosecutors, or other members of the justice system (Article 298.1); and insulting representatives of the authorities (Article 319). [283] Article 6.21 of the administrative code prescribes fines for "advocacy of nontraditional sexual relations among minors," [284] while Article 148 of the criminal code bans insulting religious feelings, which is punishable by fines or imprisonment. [285]

Articles 20.3 and 20.29 of the administrative code prescribe fines for displaying extremist symbols (such as Nazi symbols) and distributing extremist materials, [286] and Article 354.1 of the criminal code bans spreading false information about the Soviet Union's actions in World War II. [287] In March 2020, Article 20.3 of the administrative code was amended to allow extremist symbols to be displayed without penalty for nonpropagandistic purposes. [288] In April 2022, Putin signed a law that criminalized equating the role of the Soviet Union and Nazi Germany in World War II. [289]

In addition, more severe criminal penalties are also provided for public calls to commit suicide (Article 110.2 of the criminal code) and incitement to mass riots (Part 3 of Article 212 of the criminal code).

In March 2022, Putin signed a law that amended the criminal code and criminal procedure code to outlaw the dissemination of "knowingly false information

about the activities of the armed forces of the Russian Federation" and discrediting the actions of the Russian military. Spreading "knowingly false information" results in up to 15 years' imprisonment in a penal colony in cases where it causes "serious consequences." In other cases, the offense results in a fine ranging from 700,000 to 1.5 million rubles ($7,860 to $16,840), to up to three years in prison. The amendments regarding knowingly "spreading false information" were codified under Article 207.3 of the criminal code, and the crime of "public actions aimed at discrediting" the military were introduced under Article 280.3 in the criminal code and Article 20.3.3 of the code of administrative offenses. [290]

In March 2023, the State Duma passed amendments that broaden the definition of discrediting the military. [291] The amendments criminalize "discrediting" any participants in the "special [military] operation," with violators facing a punishment of up to 15 years in prison. These measures would now apply to volunteer formations, organizations, and individuals who assist in the fulfillment of the tasks assigned to the Russian army, including the activities of private military companies, as well as information on the collection of equipment, food, and other materials. The amendments provide for fines, correctional or forced labor, or imprisonment for up to 15 years. [292] In December 2023, criminal penalties were also introduced for discrediting Russian National Guard volunteers. [293] The maximum sentence is up to 15 years in prison.

There are also further penalties for disseminating purportedly false news online. In March 2019, Putin signed two bills punishing the dissemination of purportedly false news (and giving the prosecutor general the wide ability to block such information at their initiative) and expressing disrespect for the state. Both bills carried fines, while the bill on respect for the state allows Roskomnadzor to block offending content. [294] In April 2020, as the COVID-19 pandemic became a global crisis, Putin signed a law making the spread of purportedly false news a criminal offense, with violators potentially risking a prison sentence as long as five years. [295]

In July 2022, the State Duma adopted amendments to the criminal code that introduce penalties for "public calls to carry out activities directed against the security of the state" and for "confidential cooperation of Russians with foreign intelligence services" and "international or foreign organizations." [296] For those

who make public calls against the security of the state, fines range from 200,000 to one million rubles ($2,240 to $11,220). Criminal liability for cooperation with foreign intelligence services, or with international or foreign organizations, results in three to eight years' imprisonment and a fine of up to one million rubles ($11,220).

Articles 280 and 280.1 of the criminal code punish online calls for extremism and separatism with up to five years in prison. **297** Article 20.3.1 of the administrative code assigns fines or up to 15 days in jail for those found guilty inciting hatred online, **298** and repeat offenders can face longer prison terms under Article 282 of the criminal code. **299** If a criminal case is opened against an individual for "extremist" activities, that person could be included on a list maintained by the Federal Financial Monitoring Service (RosFinMonitoring). **300** Those on the list are banned from certain professions, and their bank accounts can be frozen, even if they are not convicted of a crime.

In November 2023, the Supreme Court, at the request of the Ministry of Justice, recognized the "international LGBT movement" as an "extremist organization." **301** This threatened criminal prosecution of all LGBT+ people living in Russia. In 2022, the court recognized Meta as an "extremist organization." **302** Earlier in 2020, the "Prison. Order. Universal" organization, which the Moscow Times outlet described as "based on prison culture...ruled indirectly by adult criminals" was recognized as an "extremist organization." **303** The maximum penalty under Article 282.1 of the criminal code ("organization of an extremist community") is 12 years in prison.

In December 2023, amendments to the code of administrative offenses came into force, providing for the ban on "LGBT propaganda," "pedophilia," and gender confirmation surgery in advertising, books, films, and other media. A Roskomnadzor order on similar content pertaining to the internet was due to take effect in September 2023. **304**

The 2016 Yarovaya Law altered nearly a dozen existing laws, with significant ramifications for internet freedom. **305** Among these changes were amendments to Article 205.2 of the criminal code, which imposed prison terms of up to seven years for calling for or justifying terrorism online. **306**

The authorities have used various drug-related charges as pretexts to censor the news media. [307] In December 2020, [308] the government adopted a law that imposed fines of up to 1.5 million rubles ($19,700) for promoting drugs and psychotropic substances on the internet. [309] In February 2021 the government adopted amendments to Article 230 of the criminal code ("inducement to use of narcotic drugs, psychotropic substances, or their analogues") that would punish "narcotic drug propaganda" with a minimum of 10 years in prison. [310]

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**1** / 6

Criminal and administrative charges are widely used to stifle critical discussion online. Numerous individuals have been charged for their posts or reposts on social media, including a number of users charged under legislation that criminalizes discrediting the Russian military and participants in the special military operation (see C2). According to OVD-Info, from the beginning of the war to the end of May 2024, 935 criminal cases were opened against Russians under "anti-war" articles. Another 9,495 cases were opened under Article 20.3.3 of the code on administrative offenses on discrediting the army. [311]

According to a February 2024 report from OVD-Info, 19,855 people in Russia were detained for expressing antiwar sentiments since the beginning of the full-scale invasion of Ukraine in February 2022. [312] As of February 2024, 287 defendants in these criminal cases have been imprisoned. [313] Out of all the cases, 126 criminal cases were initiated over comments made via VK, 84 cases were related to posts on Telegram, 28 involved Instagram, 14 related to comments on Facebook, and 5 involved WhatsApp messages. Cases include:

- In August 2024, after the coverage period, a Moscow court sentenced Andrey Kurshin, who previously served in the Russian military, to six and a half years in prison for spreading false information about the military. The charge stemmed from his reporting on the Russian military restricting access to water in Kryvyi Rih in Ukraine and bombing maternity wards on his "Moscow Calling" Telegram channel. [314]

- In July 2024, after the coverage period, RFE/RL journalist Alsu Kurmasheva, who is American, was sentenced to six and a half years in prison in a secret trial for spreading false information about the Russian army. She was initially arrested for failing to register as a foreign agent (see B6). **315** In August 2024, she was included in a prisoner swap involving Germany, Norway, Poland, Slovenia, Russia, and the United States, and ultimately returned to the United States. **316**
- In February 2024, a Moscow court sentenced Oleg Orlov, cochairman of the Memorial Human Rights Center (PTM), to two and a half years in a general regime colony for "discrediting" the army, though he was initially issued a fine. He was detained in March 2023 along with other PTM employees, but the criminal case, which concerned an article he wrote about the war, was opened in October. **317** In July 2024, after the coverage period, a Moscow court denied his appeal. **318**
- In February 2024, the editor in chief of *Novaya Gazeta*, Sergey Sokolov, was fined 30,000 rubles ($337) in an administrative case because a post in the outlet's Telegram channel included "signs of verbal discrediting the actions of government agencies," according to law enforcement. **319**
- In January 2024, a court in the Rostov region sentenced a 72-year-old pensioner to five and a half years in a general regime colony because of two VK posts concerning the number of Russian soldiers who had died in Ukraine. The woman was found guilty of distributing "fake news" about the army. **320**
- In January 2024, a court in the oblast of Orenburg fined Marina Tarbaeva 30,000 rubles ($337) for writing "Glory to Ukraine" and opposing the invasion in WhatsApp messages. **321**
- In December 2023, a court in Moscow fined Pavel Muntyan, the animator and author of the online television series *Mr. Freeman*, 40,000 rubles ($449) over a video created by rapper Legalize and posted on the *Mr. Freeman* YouTube channel. The video contained "statements aimed at discrediting the Russian armed forces and its citizens." **322** Muntyan has been declared a foreign agent since April 2023, and in March 2024 he was fined other 40,000 rubles ($449) for failure to fulfill the duties of a foreign agent. **323**
- In October 2023, a St. Petersburg court drew up 15 protocols against Ilya Khrapko, a retired soldier, under the article of "discrediting" the army

because of his posts on VK. The court combined all the reports into one case and fined the man 20,000 rubles ($224). **324**

- In September 2023, Aleksandr Nozdrinov, a blogger who covers corruption in Novokubansk, was sentenced to eight and a half years in prison for spreading false information about the military. The court alleged that he had administered a Telegram channel that shared photographs of the Russian military's attacks on Kyiv in March 2022, when he was initially detained, but his lawyer contends that he is not affiliated with the channel and the sentence is a reprisal for his coverage of local corruption. **325**
- In August 2023, Yelena Dovrovskikh, a progovernment editor in chief of the Rostov-on-Don-based 1RND news site, was charged with "discrediting the army" over an article the site had published about bulletins posted in the city that instructed people on how to surrender to the Ukrainian army. **326**
- In June 2023, blogger Roman Ushakov was sentenced to eight years in prison by a military court in Moscow, and he was prohibited from running websites for an additional three years. The conviction stemmed from comments Ushakov made about the invasion of Ukraine on Telegram. He was arrested in December 2022 and claimed law enforcement had used "electric shocks" to torture him while he was detained (see C7). **327**
- In March 2023, Andrei Novashov, a freelance journalist who had previously worked with the RFE/RL-affiliated Siberia.Realities outlet, was sentenced to eight months of corrective labor over social media posts covering the Russian military's attacks on civilian targets in Mariupol. **328**
- In February 2023, journalist Alexander Nevzorov was sentenced to eight years in a penal colony in absentia for publishing material about the shelling of Mariupol by the Russian army. **329**
- Also in February 2023, the Leninsky District Court in Barnaul sentenced Maria Ponomarenko, a journalist who worked for the online website RusNews, to six years in a penal colony for social media posts about the Russian military's attack on a theatre in Mariupol. She was initially arrested in April 2022. **330**

Additional cases of individuals being punished for their online speech surfaced during the current coverage period:

- In April 2024, blogger Alyona Agafonova was sentenced to ten months of correctional labor for posting an Instagram video where she pretended to tickle a World War II statue in Volgograd. She was charged with "rehabilitating Nazism." **331**
- In February 2024, Bjorn Blaschke, a journalist working at German radio station Westdeutscher Rundfunk (WDR), was removed from a train in the city of Birobidzhan and fined 40,000 rubles ($449) for a Twitter post from 2022, which discussed the effects of the invasion of Ukraine on commodity prices. The journalist was planning to travel across the Trans-Siberian Railway and discuss the March 2024 presidential election with Russians. **332**
- In April 2024, a resident of Krasnodar Krai was fined under the article on "LGBT propaganda" because her VK profile contained screenshots from films and clips which were ruled to depict "nontraditional" relations. The woman mentioned that some of the photographs cited were simply memes; for instance, one of the screenshots is a still from the video for the Hozier song "Take Me to Church." **333**
- In April 2024, a St. Petersburg court sentenced a man to pretrial detention center for a "cynical" comment about the March 2024 terrorist attack at the Crocus City Hall concert venue in Krasnogorsk. **334** He was charged under Part 2 of Article 205.2 of the criminal code (public justification of terrorism), under which he could receive a prison term as long as seven years. **335**
- In January 2024, Igor Girkin, a former officer in the FSB who fought and led militias in Crimea in 2014, was sentenced to four years in prison over posts that criticized Putin in his Telegram channel. He was charged with "inciting extremism." In May 2024, a court in Moscow upheld Girkin's sentence for "extremism," which his lawyer vowed to appeal. **336** Previously, in 2022, a court in the Netherlands issued him a life sentence in absentia because of his role in downing Malaysia Airlines Flight MH17 in 2014, which killed 298 people. **337**
- In February 2024, the Pskov City Court ordered an arrest in absentia for editor in chief of Pskovskaya Guberniya, Denis Dmitriev, because he failed to perform his duties under the "foreign agent" law (see B6 and C2). The court also opened a case of "discrediting" the army against him because of a video covering a Russian missile strike. In December 2023, he was put on the wanted list. **338**

- In January and February 2024, two individuals, in the Volgograd region and Saratov, were fined 1,500 rubles ($16.84) and 1,000 rubles ($11.22), respectively, for posting rainbow flags on social media. **339**
- In January 2024, a Krasnodar Krai resident was sentenced to one and a half years in a general regime colony for an image he posted on VK in May 2023 that depicted a St. George's ribbon on a penis and a caption critical of Putin. He was found guilty of desecrating symbols of Russia's military glory using the internet. **340**
- In January 2024, journalist Andrey Serafimov was put on the federal wanted list. Previously, a criminal case was opened against him for calls for activities directed against national security. The journalist himself suggests that the persecution is related to his posts on Telegram posts about military conscription. **341**

In September 2022, journalist Ivan Safronov, who worked for Vedomosti and *Kommersant*, was sentenced to 22 years in prison in a treason case for allegedly sharing information about Russia's military in the Middle East with the Czechian government. **342** In August 2023, the Supreme Court upheld the sentence. **343** In March 2023, *Wall Street Journal* reporter Evan Gershkovich was arrested on charges of espionage in Yekaterinburg, and a court in that city sentenced him to 16 years in prison in July 2024, **344** before he was returned to the United States as part of a prisoner swap in August 2024. **345** In July 2022, Andrei Pivovarov, the former director of opposition group Open Russia, was sentenced to four years in a penal colony for "running an outlawed prodemocracy movement." **346**

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**1** / 4

Anonymous communication is restricted in Russia, as are encryption tools. The Russian government continues to block internationally available VPNs. The authorities used TSPU equipment (see A3 and B1), which relies on DPI technology, to restrict access to VPN services. **347** As of March 2024, approximately 20 additional popular VPN services had been blocked in Russia. **348** VPN access is also impacted by targeted protocol blocking.

A 2017 law mandates the blocking of VPN services that allow their clients to access banned content. **349** In March 2019, Roskomnadzor began to enforce this law for the first time, sending 10 VPN services a request to connect to the Federal State Information System, which is Roskomnadzor's list of banned content (see B1). **350** In March 2024, a law prohibiting information about bypassing blocking and advertising VPNs came into force. After this, the authorities began blocking VPNs and websites that contained information about bypassing government restrictions (see B1), **351** and issued removal requests to 34 websites within days of that law entering force. **352**

In July 2024, after the coverage period, Apple removed 25 VPN services, including NordVPN, Red Shield, and Proton VPN, from the App Store in Russia based on a request from Roskomnadzor (see B2). **353**

In June 2024, after the coverage period, Mozilla announced that it had blocked censorship-circumvention add-ons in its Firefox browser at the request of Roskomnadzor, **354** but it reinstated those add-ons shortly after.

In August 2023, reports emerged that WireGuard, an open VPN protocol, as well as OpenVPN were blocked across several mobile operators. **355** Previously, in May 2023, VPN users reported that the OpenVPN protocol, which is used by many private institutions in Russia, was blocked (see B1 and A3). **356**

In June 2022, Roskomnadzor began blocking Proton VPN. **357** January 2022, the authorities blocked the TunnelBear VPN, **358** which was included in the register of prohibited sites in 2018. **359** In September 2021, Roskomnadzor announced the blocking of six additional VPN services, including ExpressVPN and NordVPN (see B1). **360**

In May 2022, Roskomnadzor's Public Council met and listed VPN services as tools in the information warfare campaign against Russia. **361** In December 2021, Roskomnadzor ordered the blocking of Tor and blocked the service using DPI technology, but after lawyers from Roskomsvoboda appealed the ruling, it was overturned in May 2022 (see B1). In July 2022, Roskomnadzor briefly unblocked the Tor browser, **362** though a court banned Tor again in the same month.

In June 2021, Russia authorities banned the use of certain VPN services, restricting access to VyprVPN and the browser extension OperaVPN, which refused to

provide its services to users located in Russia. **363** In July 2021, at the request of authorities, Google agreed to remove hundreds of thousands of links to VPN services from search results **364** over a two-year period. **365**

Russian authorities had initiated a campaign against encrypted email services in early 2020. Services including SCRYPTmail.com, Mailbox.org, Proton Mail, Tutanota, and StartMail were blocked. **366**

Since 2014, mobile phone subscribers in Russia have been required to register with their official state identification in order to purchase a SIM card, limiting anonymity for mobile users. **367** A 2017 amendment to the Law on Information, Information Technology, and Information Protection requires users of social media platforms and communication applications to register with their mobile phone numbers, further restricting online anonymity. **368** In May 2019, **369** rules requiring such platforms to verify users' phone numbers with the help of mobile service providers took effect. **370** If a user's phone number cannot be verified, they will no longer be able to send messages. Furthermore, mobile service providers are now obliged to inform communication and social media platforms when users cancel their contracts. In those cases, users will no longer be able to send messages unless they reregister with a new phone number. **371** Roskomnadzor interprets the rules to apply to both foreign and domestic platforms. **372**

Since August 2023, Roskomnadzor has required telecommunications operators to block the numbers of subscribers with inaccurate personal data, giving them 15 days to update their data after notification. **373** By the end of 2023, at least 600,000 SIM cards were blocked. **374**

The authorities have also sought to limit the privacy safeguards of encryption tools. The Yarovaya Law requires online services that offer encryption to assist the FSB in decoding encrypted data, including by providing encryption keys. Companies that fail to cooperate can currently face fines of up to six million rubles ($67,340). Fines for failure to hand over encryption keys were increased in December 2019 (see B3). The Electronic Frontier Foundation (EFF) has suggested that the impossibility of full compliance is a deliberate feature of the law, giving authorities leverage over the affected companies. **375** In February 2020, it was reported that in 2019, the FSB had sent letters to a dozen Russian online services

—including Avito, Habr, and RuTube—demanding that they provide the agency with encryption keys allowing it to decrypt users' correspondence, and that they organize "around-the-clock access to their information systems." [376] Exactly how these services responded is not publicly known.

In February 2024, the ECtHR published a ruling on the first case regarding "Telegram keys," [377] recognizing that the Yarovaya Law compromised the right to privacy. Telegram initially filed a complaint to the ECtHR in 2019, [378] which was related to the service's refusal to hand over encryption keys to the FSB. Telegram was first fined and then blocked in Russia for refusing, before it was later unblocked in 2020. [379]

In June 2022, the MinDigit announced plans to establish a single database for international mobile equipment identity (IMEI) numbers for mobile phones, which could facilitate surveillance. [380] As of April 2024, the project has not yet been implemented.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

State surveillance of internet activities greatly affects users' privacy rights, and several laws have increased authorities' power to conduct intrusive surveillance.

The government utilizes the SORM for its online surveillance activities. Under current legislation, to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. Providers that do not comply with SORM requirements are fined and may lose their licenses. SORM-3, an evolutionary variant of the system that collects a wider variety of data than SORM-1 or SORM-2, [381] uses DPI technology, enhancing the ability of security services to monitor content on all telecommunications networks in Russia. The law on the Runet provided authorities with additional DPI capabilities (see A3). [382]

Some researchers have argued the sanctions imposed on Russia by the United States and EU in response to the full-scale invasion of Ukraine have made it more difficult for the Kremlin to acquire the necessary technology to maintain and upgrade SORM. Nokia, which pulled out of the country in March 2022, had

previously supplied telecommunications operators and the government with much of the technology necessary to operate these systems. **383** However, a July 2023 *New York Times* investigation revealed that Russian firms had produced tools that can "track certain kinds of activity on encrypted apps like WhatsApp and Signal, monitor the locations of phones, identify anonymous social media users and break into people's accounts." **384**

A September 2022 *New York Times* investigation, which relied on leaked data from Roskomnadzor's Bashkortostan office, shed light on the scope of the agency's social media monitoring activities. According to the investigation, Roskomnadzor regularly monitored social media platforms, including Telegram chats and Instagram pages, with a particular focus on individuals who were supportive of the late Aleksey Navalny. The agency also targeted those who played roles in organizing protests, identified individuals who ran critical accounts, and produced reports on the general reaction to political situations, including the invasion of Ukraine. **385**

A separate investigation published by RFE/RL in February 2023, which relied on a second set of leaked Roskomnadzor data published in November 2022, found that Roskomnadzor's GFRC engaged in similar social media monitoring. The investigation revealed that the GFRC had a "Protest Moods" chatroom, which included employees from other government agencies, and monitored the likelihood of protests based on what people shared on social media platforms and messenger services. The GFRC also used bot farms in attempts to infiltrate closed groups and channels. **386**

Additionally, in August 2022, the GFRC spent 57 million rubles ($637,800) on an AI monitoring system known as Oculus (see B2), which allows employees to identify "prohibited information" in social media posts, including multimedia posts. **387** RIA Novosti quoted a GFRC official who claimed that Oculus could examine a large amount of data that was purportedly "extremist" or contained "LGBT propaganda," at a scale far beyond what Roskomnadzor staff could examine manually; DFR Lab cited this domestic reporting in a February 2023 article. **388**

The Kremlin has also used facial-recognition software to detain people (see B8). In July 2021, the Ministry of Internal Affairs reported that more than 5,000 cameras with facial-recognition capabilities were installed across the country, excluding

Moscow. [389] Internal government documents leaked in 2024 reveal the Russian presidential administration plans to create a unified video surveillance system nationwide. [390]

In September 2023, Access Now and Citizen Lab reported that Galina Timchenko, who runs the Latvia-based online news outlet Meduza, reported that her iPhone had been infected with NSO Group's Pegasus spyware, which allows the attacker to gain access to the infected device, in February 2023. The Ministry of Justice in Moscow had listed Meduza an "undesirable organization" in January 2023 (see B6). [391] The case marked the first time a Russian journalist's device had a confirmed Pegasus infection. Researchers were not able to definitively identify the attacker. A May 2024 investigation from Access Now, Citizen Lab, and independent researcher Nikolai Kvantiliani found that three Russian journalists living in exile had been targeted by Pegasus between 2020 and 2022. They all either lived in Latvia or had visited Latvia around the time of the reported infection. [392]

In December 2019, President Putin signed a law requiring that mobile devices in Russia come preloaded with Russian software, raising privacy concerns among advocates who suspect that such software could be compromised. [393] As of April 2021, Russian smartphones have come with predetermined Russian software after the MinDigit expanded the scope of the law. [394]

Russian authorities are nominally required to obtain a court order before accessing electronic communications. [395]

The authorities are not required to show interception warrants to service providers to obtain metadata, and FSB officers have direct access to providers' servers through local control centers. [396] Experts note that there is no publicly available information about accountability for FSB officers who may abuse this power. [397]

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**0** / 6

Score Change: The score declined from 1 to 0 because of laws that provide authorities with increased access to location data from taxi companies and

telecommunications operators.

The legal system requires service providers and technology companies to cooperate with the government in its surveillance operations. According to the Law on Communications, service providers must grant network access to law enforcement agencies conducting search operations and turn over other information requested by the Prosecutor General's Office, the Ministry of Internal Affairs, the FSB, or the Investigative Committee. **398** The Law on Investigative Activities states that court orders are needed to intercept the content of communications, although exceptions can be granted if there is an "immediate risk" that a serious crime, defined as a crime that can draw 10 or more years of prison time, will be committed or if an "immediate threat" to national security is ascertained. **399**

In December 2022, Putin signed a law obliging taxi-ordering services to register as information dissemination organizers to provide the FSB with access to their databases, including geolocation and payment information, **400** as well as remote access to their systems. **401** In September 2023, the new requirement came into force. **402** Under the law, the FSB has access to the geolocation of drivers and passengers in real time, should those taxi services be registered under the December 2022 law. As of May 2024, the law has only been applied to Yandex Go, which is the most popular ride-hailing application in the country.

Under provisions of the Yarovaya Law that came into force in July and October 2018, **403** service providers and "information dissemination organizers," which includes people or entities that own a site that facilitates communications between users, are required to store the content of users' online communications —including video, text, and audio communications—for six months. Metadata must be stored for three years by service providers and one year by other entities. **404** Service providers must store users' browsing history for 30 days. **405** Companies are required to arrange a storage plan with the authorities and increase their storage capacity by 15 percent annually, beginning five years after implementation. **406** Under the law, the authorities are nominally obliged to obtain a court order to access the data. In March 2024, the government expanded the list of data that owners of websites and services included in "information dissemination organizers" list, which included 417 platforms and companies at that

time, [407] will be required to store. [408] The user's geolocation and means of payment will also be added to this data. [409]

In January 2024, Roskomnadzor announced that telecommunications operators must provide information about the geolocation of all customers' internet protocol (IP) addresses to prevent distributed denial-of-service (DDoS) attacks, [410] but this information could be used to increase surveillance of individuals.

In December 2019, it was disclosed that ISPs had purchased 10 billion rubles ($112.2 million) in special equipment from Rostec in order to comply with the Yarovaya Law. [411] Previously, service providers had warned that the legislation would impose excessive costs on them, estimating the cost could reach as high as 60 billion rubles ($673.4 million).

In March 2023, the State Duma passed a law that obliging owners of communication networks with autonomous system numbers to store user data for three years. [412] The law also obliges them to provide information upon request to law enforcement agencies. Network owners must store voice information, text messages, images, sounds, video, and other message content. Previously, according to the Yarovaya Law, such data was stored and transferred to the security forces by telecommunications operators only in relation to end users, but now the data includes that of company employees and internal networks. [413]

Beginning in March 2023, telecommunications providers must notify Roskomnadzor of the implementation of cross-border data transfers. [414] At the same time, Roskomnadzor may decide to ban or restrict these transfers "in order to protect the morality, health, rights and legitimate interests of citizens."

In June 2022, the FSB sent letters to telecommunications operators demanding they provide SORM compliance plans under the Yarovaya Law by the end of the second quarter of 2022. [415] In this letter, the FSB indicated that operators are required by law to organize and store text messages, voice information, video, and other data of their users. Some large operators did not initially implement the required technical measures, which prevented the FSB and other security services from collecting user data. In August 2022, the MinDigit issued a fine scheme for

operators who refuse to install SORM, [416] which came into effect in May 2023 (see A4).

In July 2023, Roskomnadzor announced It would begin issues fines ranging from one to five million rubles ($11,220 to $56,120) to ISPs and mobile operators that fail to install the TSPU system (see A3, A4, and B1), the DPI system it uses to block websites and collect data on user traffic. [417]

Due to the COVID-19 pandemic, the government in 2020 temporarily eased traffic-storage requirements for service providers under the Yarovaya Law. In particular, it approved a one-year suspension of increases in traffic storage requirements and a one-year moratorium on the storage of heavy video traffic until September 1, 2021. [418] The government introduced a similar measure in March 2022, after the invasion of Ukraine.

Service providers operating in Russia typically do not disclose the scale and scope of government requests for user data. It is not clear whether they may do so under Russian law. [419]

The data-localization law enacted in 2015 requires foreign companies that possess Russian citizens' personal data to store their servers on Russian territory (see B1), potentially enabling easier access for security services. [420]

Roskomnadzor's leadership has repeatedly asserted the need to apply data-localization measures to online platforms, and it continued to issue fines during the coverage period. Fines were first issued April 2019, when Twitter and Facebook were fined a token 3,000 rubles ($33.67) for their noncompliance. [421] Legislative amendments that were adopted in late November 2019 and signed by President Putin that December gradually increase such fines until they are large enough to affect companies' revenues without exposing their platforms to the threat of blocking. [422]

In November 2023, a court fined Google 15 million rubles ($168,400) because it did not store the personal data of residents. [423] For the same offense, Google was previously issued the same fine in June 2022 [424] and a three-million-ruble ($33,670) fine in July 2021. [425] In August 2023, the court issued the first fine to Telegram for refusing to localize data; it amounted to 50,000 rubles ($5,612). [426] In July 2022, WhatsApp and Snapchat were fined 18 million rubles ($295,000) and

1 million rubles ($16,390), respectively, for failing to store user data locally. [427] WhatsApp was previously fined four million rubles ($53,690) in August 2021, marking the first fine for the messaging service. Facebook and Twitter were fined in 2021 before they were blocked. [428]

In July 2022, a Moscow court fined Apple two million rubles ($32,780) because the company did not store user data locally. [429] In June 2022, a Russian court fined Twitch, Pinterest, Airbnb, and United Parcel Service (UPS) for refusing to localize Russian data. [430] The latter three companies received a fine of two million rubles ($32,780), while UPS was fined one million rubles ($16,390). In August 2023, the court first fined Telegram for refusing to localize data. The fine amounted to 50,000 rubles ($5,612). [431]

The government has also fined companies based in the country for refusing to share data with the security services. In June 2023, Yandex was fined two million rubles ($22,450) because it reportedly refused to share data, including encryption keys, with the FSB, as is required under the Yarovaya Law. [432] The company was previously fined 400,000 rubles ($6,560) for the same reason in 2022. [433]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**1** / 5

Physical attacks on online activists and journalists by state and nonstate actors are relatively common in Russia, and authorities rarely conduct meaningful investigations of such incidents. Law enforcement agents also apply other forms of extralegal pressure against journalists and break into their devices. [434]

During the coverage period, some users who were arrested for spreading false information about or discrediting the Russian military (see C2 and C3) reported that they were tortured or attacked. For example, Roman Ushakov, a blogger who was sentenced to eight years in prison for spreading false information about the military in June 2023 (see C3), alleged that law enforcement agents tortured him with "electric shocks" during his initial detention in December 2022. [435]

The authorities of the Chechen Republic have kidnapped and tortured activists. [436] Additionally, Elena Milashina, a Russian journalist working for *Novaya Gazeta*,

has regularly faced death threats for her coverage of human rights issues in Chechnya. **437** In July 2023, Milashina and lawyer Alexander Nemov was severely beaten as she was on her way to the Chechen regional capital of Grozny to cover the trial of a human rights activist. **438** Their car was blocked by three cars with armed people, who confiscated their equipment and documents. Milashina was shaved and doused with green paint. **439**

Online intimidation and physical violence against LGBT+ people have escalated since the adoption of the 2013 law banning so-called propaganda of nontraditional sexual relations to minors **440** and one journalist was beaten shortly after the 2023 law labelling the "LGBT movement" as extremist. **441**

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**0**/3

Since the Kremlin's full-scale invasion of Ukraine, state websites have continued to face significant cyberattacks.

In March 2024, Ukraine's Defense Intelligence Agency announced that it had hacked the Russian defense ministry and obtained data about military units and structures. **442**

In February 2024, Roskomnadzor reported that 500 million records of Russians' personal data had been leaked from government databases. **443** The agency did not specify what data was publicly available but announced it had begun an investigation. For the duration of 2023, Roskomnadzor recorded 168 leaks of personal data. **444**

In November 2022, the Cyber Partisans announced that had hacked Roskomnadzor's GFRC (See B2 and C5). This followed a 2022 hack of Roskomnadzor's office in the Republic of Bashkortostan. **445**

In July 2022, it was reported that Turla, a hacker group aligned with the Russian government, had launched a spoof application that claimed to launch DDoS attacks on Russian websites, but in reality it enabled the hackers to siphon user data. **446**

Following the Russian invasion of Ukraine, Ukrainian hackers formed an "IT Army" and launched DDoS attacks on Russian websites. The hackers targeted a range of companies and government agencies, issuing instructions and updates via Telegram. **447**

In February 2022, the hacking group Anonymous claimed responsibility for cyberattacks that displayed antiwar messages on the websites of the Russian government, Roskomnadzor, and other state entities, as well as state-affiliated media outlets including RT, TASS, and *Kommersant*. **448** Following the first week of Anonymous's campaign, more than 2,500 Russian- and Belarusian-linked websites faced cyberattacks. **449**

Hacks on government websites can result in imprisonment. For instance, In February 2024, the FSB detained a hacker in Moscow who is accused of launching DDoS attacks on critical information infrastructure facilities in Russia. **450**

In April 2022, in response to the barrage of attacks on government websites and private companies, Roskomnadzor announced plans to create a national system for protecting online resources from DDoS attacks originating from abroad **451** by upgrading its DPI equipment. **452**

Footnotes

1 International Telecommunication Union (ITU) Datahub, "Russia, Individuals Using the Internet," accessed September 2024, https://datahub.itu.int/data/?e=RUS.

2 ITU Datahub, "Russia, Active Mobile Broadband Subscriptions," "Russia, fixed-broadband subscriptions," accessed September 2024, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3 "Almost all households in Russia access the network at high speeds, [in Russian]," HSE, April 18, 2023 https://issek.hse.ru/news/828416272.html

4 Economist Impact, "The Inclusive Internet, Russia 2022," accessed August 2022, https://impact.economist.com/projects/inclusive-internet-index/2022/cou....

5 "Deputy PM sees commercial 5G in major cities in 2021 (but Moscow maintains 2020 vision)," TeleGeography, September 7, 2018,

https://www.commsupdate.com/articles/2018/09/07/deputy-pm-sees-commerci...

More footnotes

On Russia

See all data, scores & information on this country or territory.

See More ›

Country Facts

Population

144,200,000

Global Freedom Score

13 /100 **Not Free**

Internet Freedom Score

20 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2024

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org