Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**877**
Land:	Rusland
Kilde:	Human Rights Watch
Titel:	“Disrupted, Throttled, and Blocked”. State Censorship, Control, and Increasing Isolation of Internet Users in Russia
Udgivet:	juli 2025
Optaget på baggrundsmaterialet:	20. oktober 2025

HUMAN RIGHTS WATCH

“Disrupted, Throttled, and Blocked”

State Censorship, Control, and Increasing Isolation of Internet Users in Russia

HUMAN RIGHTS WATCH

Disrupted, Throttled, and Blocked

State Censorship, Control, and Increasing Isolation of Internet Users in Russia

Printed in the United States of America
ISBN: 979-8-88708-246-2
Cover design by Solé Nazaire

Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amman, Amsterdam, Beirut, Berlin, Brussels, Chicago, Copenhagen, Geneva, Johannesburg, London, Los Angeles, Nairobi, New York, Paris, San Francisco, Sydney, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: http://www.hrw.org

JULY 2025

ISBN: 979-8-88708-246-2

Disrupted, Throttled, and Blocked

State Censorship, Control, and Increasing Isolation of Internet Users in Russia

Glossary

- **Content Delivery Network (CDN):** a network of interconnected servers that speeds up webpage loading for data-heavy websites.
- **Deep packet inspection (DPI):** a technology used to scan the content of each data packet being transferred over computer network. DPI can be used for network management purposes and to filter, block and re-route internet traffic.
- **Domain name system (DNS):** an hierarchical system that translates domain names (name typed in the web browser address bar, like hrw.org) into the numerical identifiers that locate the desired destination (IP-addresses).
- **Hosting server providers:** an IT company that offers server space and resources to store and make websites or other online content accessible to users.
- **Internet exchange points:** hubs allowing internet service providers to exchange internet traffic directly between their networks without third parties transit services.
- **Internet service providers (ISPs):** entities that provide internet access to their customers.
- **Transport Layer Security (TLS) certificates:** digital certificates that secure connections between a web browser and a server.
- **Virtual Private Networks (VPNs):** a type of Proxy which lets users browse the internet as if they were coming from the VPN's servers which are often located in some other part of the world and can be used to bypass internet blocking and manipulation.

Summary

In today's Russia, accessing popular foreign websites and social media platforms, like Instagram, Facebook, or YouTube, is largely impossible without a Virtual Private Network (VPN), a tool that allows users to circumvent censorship. A more tech savvy user will have several VPNs installed in case the state blocks one or more of them. Yet, it is a distinct possibility that none of them will work on a given day.

Thousands of websites are blocked by the Russian authorities for failure to comply with Russia's draconian laws that regulate all forms of online activity. Some foreign websites stopped providing their services to users in Russia due to sanctions and political pressure that arose following Russia's full-scale invasion of Ukraine in February 2022. Some sites, such as Russian governmental websites, can only be opened in Russia. As a result, many Russian users juggle VPNs and web browsers to have access to both foreign and Russian services and sites they need.

However, according to some estimates, about half of the country's population does not know how to use a VPN and only has access to websites and services online that are not yet blocked by the Russian government. For many Russian citizens, an increasing number of independent media outlets, human rights organizations' websites, opposition politicians' web pages, and foreign social media platforms are no longer accessible, turning into "connection timeout" and "this page is blocked" windows.

Authorities have made the use of popular social media platforms, streaming services, and messengers that do not comply with Russia's censorship and users' data disclosure legislation increasingly inconvenient by fully blocking or slowing down access to them. This, along with active state sponsored promotion of Russian alternatives, forced a growing number of users to switch to Russian browsers and social media. On such sites, users are offered state approved interpretations of current and historic events. They also face higher risks of having their personal data passed on to the law enforcement.

At the same time, foreign tech companies whose services are used by the Russians, such as Apple, Google, and Mozilla, are increasingly pressured by the Russian authorities to take down VPNs, independent media apps, podcasts, music records etc. that the government considers subversive, under threat of fines and blocking.

Russian authorities increasingly use internet shutdowns around peaceful protests, elections, or other political events, such as the funeral of the opposition leader Alexey Navalny who died in prison in February 2024. Internet users in Russia also experience occasional and unpredictable internet disruptions due to the authorities' experiments with internet censorship technology, which has resulted in, for instance, failed online banking transactions or disrupted access to state websites and taxi apps.

Ukrainian territories occupied by Russia prior to and following the full-scale invasion in February 2022 are subject to similar online censorship and internet disruptions carried out by the Russian authorities.

The current state of the Russia's internet, referred to as "RuNet," is the result of a longstanding and meticulous state policy designed to carve out Russia's section of the internet into a state controlled and isolated forum.

The 2019 "sovereign internet" law introduced the concept of a separate Russian internet. The Russian government claimed that the law was necessary to respond to a risk that the country would be disconnected from the global internet by creating a backup internet infrastructure for the Russian segment of the internet that could be fully controlled by the government via state-managed equipment. In reality, this equipment, which has since been mandatorily installed in the networks of nearly all of the country's internet service providers (ISPs), has become a powerful information control tool in the hands of the authorities, allowing for a more effective, direct, and non-transparent state censorship and manipulation of internet traffic with no proper oversight or accountability.

The authorities have tightened control over RuNet's architecture by consolidating more than half of the Russian IP addresses in the hands of seven state-tied internet service providers and decreasing the overall number of ISPs. The government also created a

national domain name system (DNS), which works as the address book of the internet, and transport layer security (TLS) certificates, which verify that the website belongs to a trusted entity and that the exchange between the website server and the user is encrypted. As a result, the state obtained more control over internet traffic and enhanced abilities for censorship and potential interception.

Whilst the state might not have fully achieved the stated purpose of the "sovereign internet" law, the authorities' efforts to implement it, many of which remain largely invisible to the majority of the RuNet users, carry serious risks for their rights and freedoms as they enable the state to censor internet traffic as well as control its routing, and intercept and decrypt data, allowing for surveillance on a mass scale.

For an internet user in Russia, these measures mean blocked access to websites and to social media platforms deemed unwanted by the authorities. This is coupled with shrinking availability of tools to circumvent such blocking, which severely limits access to independent and non state-approved information, and occasional inability to access key services, receive information and communicate online due to collateral blockings and local shutdowns. These measures also undermine the security of user communications online, exposing them to threats from external parties and state surveillance.

The Russian authorities' policy on internet censorship, isolation, and increasing control over RuNet's infrastructure, as well as internet shutdowns, violate Russia's obligations under international law. These obligations include the protection of freedom of expression and opinion, access to information, the right to privacy, and adjacent rights protected by the international law, such as freedom of assembly and economic rights.

The Russian authorities should end all censorship of internationally protected expression on the internet and ensure that any restriction online is for a legitimate purpose, has a proper legal basis, is necessary and proportionate, meaning that it is limited in scope, and transparent. The authorities should cease efforts to consolidate and control internet architecture that interfere with the right to seek and impart information and undermine privacy. They should end internet shutdowns and ensure transparency about the ways the state interferes with the RuNet functioning. They should cease pressure on foreign and

Russian tech companies to disclose user data and censor content in ways that are not compatible with international standards.

Foreign and Russian technology companies should resist state pressure to censor content and disclose user data in violation of international law using all available legal means and technological solutions. They should also ensure that they do not engage in proactive censorship.

Methodology

This report is based on analysis of laws and by-laws, the Russian government's press releases, social media posts, and data about RuNet's architecture and state censorship implementation, court documents, academic research, posts on Russian IT forums, media articles, data gathered by Russian and international internet censorship monitoring projects and data published by foreign technology companies.

Between August 2024 and May 2025, Human Rights Watch spoke with 13 Russian and international independent journalists and experts on internet censorship and digital rights, information security, internet governance, and digital policy. Names of some experts interviewed for this report were withheld to protect their security and privacy.

Between August 2024 and April 2025, Human Rights Watch sent letters to foreign technology companies – Google, Amazon, Apple, Mozilla, and Cloudflare – which are the leading foreign technology companies that have faced pressure from Russian authorities for "non-compliance" with the Russian internet censorship legislation. Google did not provide a response; Amazon, Apple, and Mozilla provided short statements; Cloudflare provided a detailed written response.

Human Rights Watch also sent letters to Russian technology companies, namely, Research and Development Partners, a state internet censorship equipment subcontractor, and VK (VKontakte) and Yandex, two major providers of social media, browsers, and other digital economy services. Yandex provided a detailed written response, whilst other companies did not reply on the record.

Human Rights Watch has compiled substantive written responses we received into a downloadable Annex produced online along with this report.

Human Rights Watch also sent a letter to the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) but has not received a response.

I. Technological Means to Conduct State Censorship

The "sovereign internet" law, which entered into force in November 2019, was a pivotal step in the Kremlin's crackdown on human rights online because it introduced new technological means for state censorship. The law requires Internet Service Providers (ISPs) in Russia to install "the technological means for countering threats" (*ТСПУ* or "TSPU") equipment into their networks.[1]

What is TSPU and How Does It Work?

TSPU refers to state censorship equipment, developed and distributed by the state, which allows the government to track, filter, and reroute internet traffic, as well as perform other functions allowing internet traffic manipulation by the state. TSPU provides the government with an ability to centrally and unilaterally control the traffic passing through thousands of privately-owned and distributed ISPs.[2]

TSPU includes deep packet inspection (DPI) technology, which is a type of network blocking that filters based on specific content, patterns, or application types.[3] Because DPI blocking examines all traffic to end users, it is very invasive of privacy.[4]

The Main Radio Frequency Center, a state-owned enterprise under the state media and communications watchdog Roskomnadzor, has been put in charge of implementing the sovereign internet project, including the installation of TSPU equipment in the networks of ISPs via subcontractors.

---

[1] See for background Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship," June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship (accessed July 7, 2025).

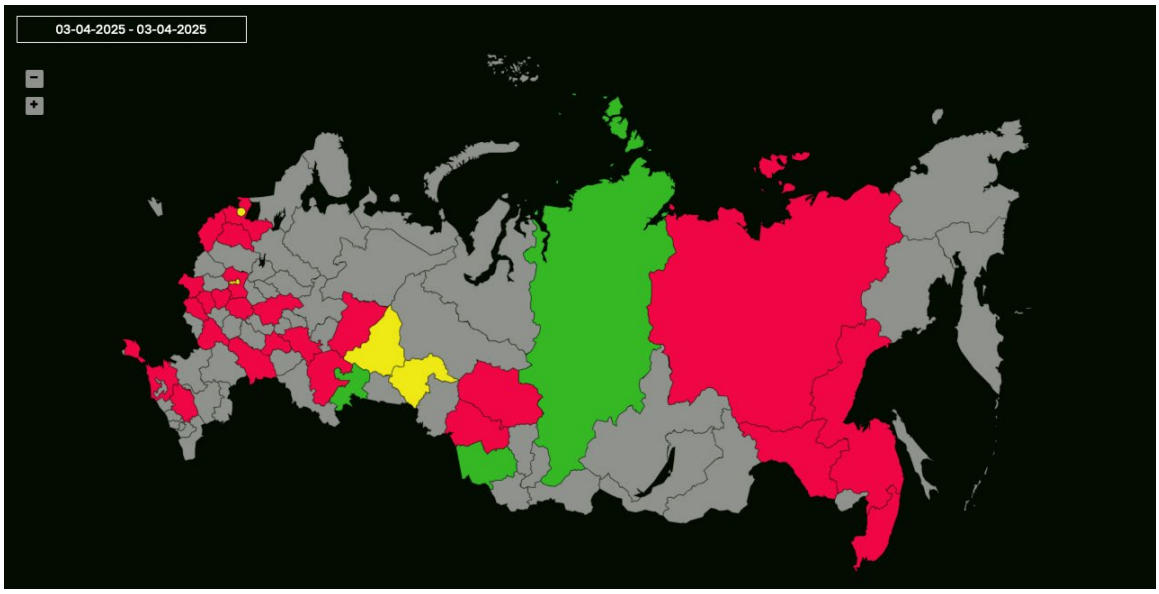
[2] See Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet, March 15, 2025, https://censoredplanet.org/tspu, accessed July 7, 2025.

[3] See "Internet Society Perspectives on Internet Content Blocking: An Overview," Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf (accessed July 7, 2025).

[4] DPI blocking uses devices that can see and control all traffic between the end-user and the content, so the blocking party must have complete control over an end-user's internet connection. DPI blocking systems may no longer be effective when internet traffic is encrypted. Unlike URL blocking, which works with web-based applications and filters URLs against a block list, DPI allows the blocking party, to block or throttle certain applications (like voice over IP or VOIP) or even based on packet sizes or transmission rates.

Over the years since its rollout, TSPU equipment has varied in hard- and software, several versions of which appear to coexist in ISPs' networks.[5] This makes the work of TSPU inconsistent across Russian regions and ISPs. Multiple discrepancies in blocking protocols also create complications in analyzing the work of TPSU and developing uniform, effective tools to bypass state censorship.

For instance, according to data gathered by "DPIdetector," an open-source project that researches internet tracking and blocking of certain tools and protocols in Russia, the blocking of YouTube varies across regions and ISPs, and changes over time.[6]



YouTube availability in Russia as reported by DPIdetector users on April 3, 2025, where red indicates blocked, yellow indicates partially blocked, green indicates available, and gray indicates that no information available due to lack of any data filed by DPIdetector volunteers. © 2025 DPI Detector.

[5] For instance, according to the Director of the Special Projects Center under the Main Radio Frequency Center Sergei Temnyi, before 2022 the hardware for TSPU was supplied by foreign companies, including Chinese ones. However, since 2022 the hardware is produced by a Russian company. Temnyi also claimed that Russia switched from the foreign to Russian software platform for the DPI software in the heart of TSPU. Moreover, another software platform was being tested at the time of his statement. Additionally, Roskomnadzor is planning to upgrade the installed TSPU, both hardware and software, in 2025-2030.

[6] See DPI Detector, a tool for researching internet censorship, which enables the blocking of certain protocols and tools to be tracked, at https://dpidetector.org/en/ (accessed July 7, 2025).

One of the software programs used by the Russian authorities for TSPU is EcoSGE software, a product developed by Research and Development Partners, a state-owned company.[7] According to the user manual for the EcoSGE, the system is approved by Roskomnadzor and allows connecting to its Uniform Registry of blocked websites, which can be automatically updated.[8]

In simplified terms, when users try connecting to a banned website, EcoSGE disrupts the connection and redirects users to a "this page is blocked" or "connection timed out" window or the connection gets abruptly terminated.

According to the EcoSGE manual, this software has a variety of functions that are especially effective when dealing with websites operating on HTTP, the unencrypted version of the protocol that enables the transfer of data on the internet so that users can access websites and other online resources. For example, EcoSGE can transmit copies of certain traffic to a third-party monitoring and analysis system ("Sniffer" function) thereby giving such third party (i.e. government) unfettered access to transmitted data. The April 2023 version of the EcoSGE manual also contained the JavaScript injection feature, which allows for malicious manipulation of web page's code and carries high privacy and security risks for users such as hijacking the session and carrying out actions on their behalf.[9] It is unclear whether this feature is available in the newer software versions.

EcoSGE also allows whoever is in charge of it, i.e. the Russian authorities in the context of TSPU, to block all traffic that goes anywhere but "whitelisted" websites. According to several interviewees, whilst this function is not yet used by the authorities, it is deeply concerning that Russian authorities have this capacity.[10]

---

[7] By July 2020 the 100% of RDP's shares were owned by Rostelecom, state owned telecommunication company and Russia's backbone ISP, via Rostelecom's subsidiary company Bashinformsviaz.

[8] User Guide: Installation and Configuration" ("Руководство пользователя: Установка и конфигурирование"), RDP https://www.rdp.ru/doc/ENATD/EcoSGE-UserGuide.pdf (accessed July 7, 2025).

[9] Dmitry Konyukhov, "Digital Sovereignty and Internet Governance in Russia" ("Цифровой суверенитет и управление интернетом в России"), master's thesis, Arizona State University, 2023, https://d1rbsgppyrdqq4.cloudfront.net/s3fs-public/c7/Konyukhov_asu_0010N_23739.pdf (accessed July 7, 2025);

"User Guide: Installation and Configuration" ("Руководство пользователя: Установка и конфигурирование"), RDP, archived at https://web.archive.org/web/20230601194626/www.rdp.ru/doc/ENATD/EcoSGE-UserGuide.pdf (accessed July 7, 2025).

[10] Human Rights Watch online interview with Mikhail Klimarev, November 20, 2024.

How Widespread is TSPU?

According to the head of Roskomandzor Andrey Lipov, in August 2023, TSPU was installed in all "mobile, broadband, and transborder uplinks".[11] Independent researchers confirm that TSPU has significantly penetrated the RuNet infrastructure networks, primarily residential internet connection networks (typically broadband connection designed for using within the home), allowing for more centralized and effective censorship.[12]

In August 2023, the amendments to the Law on Communications No. 126-FZ obliged all ISPs providing faster than 10 gbps internet connection to obtain state approval of the exact placement of the TSPU in order to begin providing services.[13] Such ISPs are required to direct all traffic via TSPU equipment and place such equipment as prescribed by the state's approval or have their obligatory state license revoked.[14] ISPs with slower than 10 gbps internet connection should connect to TSPUs installed in larger ISPs networks (uplink ISPs). The amendments also obliged the internet exchange points (IXPs), key hubs for internet traffic exchange, to install TSPU.

July 2022 amendments to the Code of Administrative Offences introduced fines up to 5 million rubles (about US$62,500) for ISPs that fail to install, maintain, or upgrade TSPU (article 13.42) or fail to direct internet traffic via TSPU (article 13.42.1).[15] In March 2023, a court in Saint Petersburg fined the head of an ISP's IT department 15,000 RUB (about $187) for unsanctioned disconnection of TSPU.[16]

---

[11] "All Communication Nodes in Russia Are 100% Equipped with Threat Counteraction Tools" ("Все узлы связи в России на 100% оборудованы средствами противодействия угрозам"), Interfax, https://www.interfax.ru/russia/927357 (accessed July 7, 2025).

[12] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet.

[13] Federal Law "On Communications," No. 126-FZ, adopted July 7, 2003 (as amended December 28, 2024), http://pravo.gov.ru/proxy/ips/?docbody&nd=102078147 (accessed July 7, 2025).

[14] Federal Law "On Amendments to the Federal Law 'On Communications,'" No. 473-FZ, adopted August 4, 2023 (as amended August 8, 2024), http://publication.pravo.gov.ru/Document/View/0001202308040081 (accessed July 7, 2025).

[15] Federal Law "On Amendments to the Code of Administrative Offenses of the Russian Federation," No. 259-FZ, adopted July 14, 2022, http://publication.pravo.gov.ru/Document/View/0001202207140022 (accessed July 7, 2025).

[16] Telegram post of the account "Chronicle of the sovereign runet" ("Летопись суверенного рунета"), https://t.me/Runet90fz/603 (accessed July 7, 2025).

The amendments also introduced criminal liability for violating the law more than twice – with up to three years in prison (article 274.2 of the Criminal Code).[17]

What is Blocked through TSPU?

Before the "sovereign internet" law, individual ISPs – regardless of the speed of service – were responsible for blocking all websites included on the state blacklist of banned websites. As such, these blockings were public knowledge. The TSPU equipment achieved a fundamental shift in state censorship and became a tool for direct and non-transparent information control in the hands of Russian authorities that allows for more uniform and effective blockings.[18]

According to Open Observatory of Network Interference (OONI), a global network for internet censorship measurements, the majority of website blockings in Russia since the full-scale invasion of Ukraine in February 2022 involved news media websites, with at least 418 such sources blocked.[19] Russian authorities eviscerated independent media reporting on the war by blocking media websites, designating media outlets "undesirable", and introducing draconian war censorship legislation.[20] Other categories of blocked websites since February 2022 include human rights related websites, such as the website of Human Rights Watch, websites concerning the LGBTIQ community, and websites critical of the government. Since February 2022, authorities have blocked more than 236,000 sources allegedly for "spreading fakes" about the war in Ukraine.[21]

---

[17] Federal Law "On Communications," No. 126-FZ, adopted July 7, 2003, https://www.consultant.ru/document/cons_doc_LAW_10699/56d15b1ae0a6eb1d6405f9ffe9aa48e21351f445/ (accessed July 7, 2025).

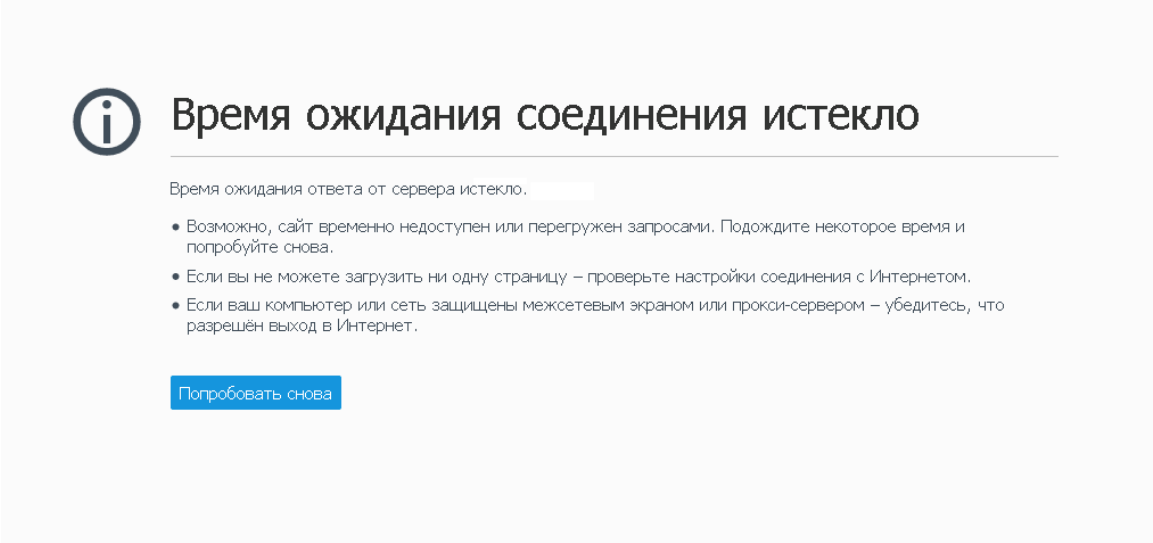
[18] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet.

[19] "Russia: A Year After the Conflict," OONI and Roskomsvoboda, February 24, 2023, https://ooni.org/post/2023-russia-a-year-after-the-conflict/#blocked-websites, accessed July 7, 2025;

RKS Global, Elizaveta Yachmeneva (OONI), Maria Xynou (OONI), Mehul Gulati (OONI), Arturo Filastò (OONI), "Censorship Chronicles: The Systematic Suppression of Independent Media in Russia," OONI, December 9, 2024, https://ooni.org/post/2024-russia-report/ (accessed July 7, 2025).

[20] Human Rights Watch, "Russia's Legislative Minefield: Tripwires for Civil Society since 2020," August 7, 2024, https://www.hrw.org/report/2024/08/07/russias-legislative-minefield/tripwires-civil-society-2020 (accessed July 7, 2025).

[21] "More Than 3,500 Fake or Discrediting Materials About the Special Military Operation Identified" ("Выявлено более 3,5 тыс. фейков и дискредитирующих материалов о СВО"), Interfax, https://www.interfax.ru/russia/1016433, accessed July 7, 2025; "About 236 Websites and Pages Blocked for Fakes About the Special Military Operation Since 2022" ("За фейки об СВО с 2022 года заблокировали около 236 сайтов и страниц"), Parlamentskaya gazeta, https://www.pnp.ru/social/za-feyki-ob-svo-s-2022-goda-zablokirovali-okolo-236-saytov-i-stranic.html (accessed July 7, 2025).



"Connection timed out" window that appears when accessing Human Rights Watch's website, hrw.org, in Russia where it has been blocked since April 2022. The window says "The server did not respond in time. The website is possibly temporarily unavailable or overloaded. Wait for a while and try again; If you are unable to load any pages, try checking the internet connection; If your computer or network are protected by a firewall or proxy server, make sure that the internet connection is not blocked. Try again." © 2025 IFreedomLab.

Blocking websites via TSPU allows the state to block access to sources that are not listed on Roskomnadzor's public registry, making blockings non-transparent.[22] The out-of-registry blockings include, for instance, Google services, censorship circumvention tools, such as Virtual Private Networks (VPNs), and media outlets.[23] Such blockings have temporal and geographic uniformity indicating centralized censorship via TSPU.[24] However, the authorities tend to deny having blocked websites and pages that are not on the official lists.[25]

[22] "Blocking Has Gone into the Shadows" ("Блокировки ушли в тень"), Kommersant, March 15, 2024, https://www.kommersant.ru/doc/6564241 (accessed July 7, 2025).

[23] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet.

[24] Ibid; RKS Global, Elizaveta Yachmeneva (OONI), Maria Xynou (OONI), Mehul Gulati (OONI), Arturo Filastò (OONI), "Censorship Chronicles: The Systematic Suppression of Independent Media in Russia."

[25] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet;

"YouTube Is De Facto Blocked in Russia" ("«YouTube де-факто заблокирован в РФ». Трафик видеохостинга снизился до 20%"), BBC Russian, December 20, 2024, https://www.bbc.com/russian/articles/c3onvn6ngepo (accessed July 7, 2025).

Social Media Platforms and Messengers

Since February 2022, Russian authorities increasingly have blocked or slowed down (throttled) entire foreign social media platforms and messengers that refused to comply with the internet censorship and data collection laws.

On March 1, 2022, Roskomnadzor dramatically throttled home broadband access to Twitter (since renamed "X") for "spreading false information on the situation in Ukraine."[26] On March 4, access to Twitter was fully blocked.[27] Authorities had previously slowed down traffic to Twitter temporarily in March 2021 for "non-compliance" with Russia's censorship laws which was the first instance of state acknowledged application of TSPU for internet censorship.[28] The throttled sites were not listed on the state registry of blocked websites up until they were fully blocked on March 4.[29]

On March 4, the authorities also blocked Meta's Facebook, after partially restricting access to it a week prior, in retaliation for Meta blocking four Russian state media accounts.[30] On March 11, Roskomnadzor announced the full blocking of Instagram after Meta introduced exceptions to its "violent speech" policies, allowing calls for violence against Russian armed forces in Ukraine.[31] The authorities also designated Meta an "extremist organization."

Since July 2024, Russian authorities have been throttling YouTube, the largest video-sharing platform with an average of more than 95 million monthly Russian users before the site was blocked. Government officials largely described the cause of the slow-down as a "technical issue in Google's equipment used in its network infrastructure and peering points," namely, Google Global Cache, and largely denied official involvement in

---

[26] "Roskomnadzor Resumes Throttling Twitter Traffic on Fixed Networks" ("Роскомнадзор возобновил замедление трафика Twitter на стационарных сетях"), Interfax, March 1, 2022, https://www.interfax.ru/russia/825451, accessed July 7, 2025.

[27] "Roskomnadzor Announces Twitter Blocked in Russia" ("Роскомнадзор сообщил о блокировке Twitter в России"), Interfax, March 4, 2022, https://www.interfax.ru/russia/826411, accessed July 7, 2025.

[28] "Human Rights Watch, Russia Slows Down Twitter Access," March 10, 2021, https://www.hrw.org/news/2021/03/10/russia-slows-down-twitter-access, accessed July 7, 2025; "Throttling of Twitter in Russia," Censored Planet, April 6, 2021, https://censoredplanet.org/throttling, accessed July 7, 2025.

[29] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi, "TSPU: Russia's Decentralized Censorship System," Censored Planet.

[30] Human Rights Watch, "Russia, Ukraine, and Social Media and Messaging Apps," March 16, 2022, https://www.hrw.org/news/2022/03/16/russia-ukraine-and-social-media-and-messaging-apps, accessed July 7, 2025.

[31] Ibid.

YouTube's throttling.[32] Google stated that problems with accessing YouTube in Russia are not connected to technical issues on Google's side.[33]

In December 2024, Roskomnadzor claimed that violation of Russian laws and "disrespect towards Russia" laid the foundation for "taking measures" against YouTube.[34]

Independent experts studying internet blockings in Russia believe that YouTube is blocked via TSPU.[35] In the end of August 2024, Roskomnadzor reportedly circulated a letter demanding that ISPs stop bypassing TSPU when directing internet traffic to blocked sources after ISPs tried to speed up access to YouTube.[36]

Whilst YouTube blockings appear to be centralized, they vary in intensity, with major traffic slowdowns recorded, for instance, in August, November, and December 2024. According to an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, by disrupting access to YouTube the authorities are trying to force Russian users to switch to Russian platforms instead.[37]

---

[32] "Rostelecom Reports Technical Issues with Google Equipment Affecting YouTube Performance" ("Ростелеком информирует о наличии технических проблем в работе оборудования, принадлежащего компании Google и используемого на сетевой инфраструктуре"), Rostelecom, July 12, 2024, https://www.company.rt.ru/press/news/d470885/ (accessed July 7, 2025); "Shadayev Stated the Ministry of Digital Development's Position on Blocking YouTube Remains Unchanged" ("Шадаев заявил о неизменности позиции Минцифры по блокировке YouTube"), RBC, January 19, 2023, https://www.rbc.ru/rbcfreenews/63c925ec9a7947931832f143, accessed July 7, 2025; "'Ростелеком зафиксировал рост числа жалоб на качество работы YouTube". July 24, 2024.

"Rostelecom Recorded an Increase in Complaints About YouTube Performance" ("'Ростелеком' зафиксировал рост числа жалоб на качество работы YouTube"), TASS, July 24, 2024, https://tass.ru/ekonomika/21441823, accessed July 7, 2025; Schechner, Sam, Mauro Orru, "Google Subsidiary in Russia to File for Bankruptcy," Wall Street Journal, May 18, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-05-18/card/google-subsidiary-in-russia-to-file-for-bankruptcy-bmUqdggeG2UvwVuKIhAg (accessed July 7, 2025).

[33] Yuri Litvinenko and Alexey Zhabin, "There Were Disruptions on YouTube" ("В YouTube выложились перебои"), Kommersant, August 1, 2024, https://www.kommersant.ru/doc/6866088 (accessed July 7, 2025).

[34] "RKN: Disrespect for Russia Became the Basis for Measures Against YouTube" ("РКН: неуважение к России стало основанием для мер против YouTube"), Kommersant, December 19, 2024, https://www.kommersant.ru/doc/7384857 (accessed July 7, 2025).

[35] Irina Pankratova, "Family Values: An Investigation into Who and Why Decided to Shut Down YouTube in Russia" ("Семейные ценности: расследование о том, кто и почему решил отключить YouTube в России"), The Bell, https://thebell.io/semeynye-tsennosti-rassledovanie-o-tom-kto-i-pochemu-reshil-otklyuchit-youtube-v-rossii (accessed July 7, 2025).

[36] "Russian Telecom Operators Warned Against 'Accelerating' YouTube" ("Операторов связи в РФ предостерегли от «ускорения» YouTube"), Habr, https://habr.com/ru/news/839388/ (accessed July 7, 2025).

[37] Human Rights Watch online interview with an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, April 2, 2025.

Since August 2024, the authorities have blocked a number of messaging apps, including Viber, Signal, Session, Simplex chat, and Discord, for failure to store in Russia and disclose users' data as required by anti-terrorism laws. In December 2024, Roskomadzor listed 11 other communication and encrypted messaging apps, namely, WhatsApp, Skype, Wire, Element, Kakao Talk, Crypviser, Dust, Pinngle, Statis, Keybase, and Trillian, as "organizers of information dissemination," requiring them to store the data of their users in Russia and share with law enforcement, supposedly for terrorism prevention. When foreign tech companies choose not to comply, their failure to do so may lead to blocking.

VPNs, Censorship Circumvention Tools

Russian authorities have made particular efforts to block virtual private networks (VPNs) and other censorship circumvention tools. VPNs encrypt all internet communications to VPN servers, which are often located in another part of the world, and allow the user to bypass censorship systems. By October 2024, at least 197 VPN services in Russia had been blocked.[38] In Russia, VPNs are a crucial tool enabling users inside the country to access information in the context of intensifying state censorship.[39]

Although a person cannot be prosecuted directly for use of such tools in Russia, in March 2024, the authorities banned dissemination of information about censorship circumvention tools.[40] Roskomnadzor claimed that by April 10, 2025, at least 8,700 websites containing information on censorship circumvention were blocked.[41] According to an interviewee whose name is not disclosed for security reasons, this measure made it very challenging to have effective discussions on ways to circumvent censorship.[42]

---

[38] "197 VPN Services Blocked in Russia" ("В России заблокированы 197 VPN-сервисов"), Interfax, October 24, 2024, https://www.interfax.ru/russia/988396 (accessed July 7, 2025).

[39] Report on VPN Censorship in Russia, VPN Guild, January 2025, https://files.rks.global/vpn-block-report_01.25.pdf (accessed July 7, 2025).

[40] "In Russia, 197 VPN Services Were Blocked" ("В России могут ограничить доступ к YouTube"), Garant.ru, https://www.garant.ru/news/1687583/ (accessed July 7, 2025).

[41] "Roskomnadzor Reported an Increase in the Number of Blocked Materials Advertising VPNs" ("Роскомнадзор заявил о росте числа заблокированных материалов с рекламой VPN"), TASS, https://tass.ru/obschestvo/23645631 (accessed July 7, 2025).

[42] Human Rights Watch online interview with a digital security expert, whose name is withheld due to security concerns, April 9, 2025.

TSPU, including EcoSGE software, allows ISPs to block traffic by the communication protocol type, for instance, specific protocols used by VPNs. According to DPIdetector project, the authorities block at least seven of the most common VPN protocols, such as Shadowsocks, AmneziaWG, and OpenVPN. These blockings vary in time, region, ISPs, and type of internet connection (landline or mobile).[43]

In addition to blocking VPNs and other proxies by protocol type, the authorities are also testing blockings based on the statistical data on IP address visits, identifying those that might be used as VPNs.[44] This may further increase the number of blocked censorship circumvention tools and further limit the ability of internet users to access independent information.

The authorities are also pressuring foreign tech companies, such as Google, Apple, and Mozilla, into taking down VPNs and other proxy apps and browser extensions.[45]

Foreign Hosting Service Providers

Foreign hosting server companies provide infrastructure to millions of website owners in Russia to improve speed and security as well as decrease costs. Websites (domains) that use the same hosting provider may share the same server and, hence, IP address. According to an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, when the authorities block a specific website by its IP address, this is likely to also affect other websites, including those that are not the target of the blocking.[46]

---

[43] DPI Detector.

[44] Human Rights Watch online interview with an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, April 2, 2025.

[45] Search Results for Roskomnadzor Takedown Notices Related to VPNs, Lumen Database, https://lumendatabase.org/notices/search?page=2&sender_name=Roskomnadzor&sort_by=date_received+desc&term-require-all=true&term=VPN (accessed July 7, 2025).

Anastasiia Kruope, "Russia: Foreign Tech Companies Cave to Authorities' Pressure," Human Rights Watch, December 17, 2024, https://www.hrw.org/news/2024/12/17/russia-foreign-tech-companies-cave-authorities-pressure (accessed July 7, 2025).

[46] Human Rights Watch online interview with an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, April 2, 2025.

Amendments to the law "On Information" (2023) require that hosting service providers that make their services available to Russian users register with the authorities and comply with Russian laws or face being blocked.[47] Relevant laws include anti-terrorism laws that require storing information about users in Russia and sharing data with Russian authorities upon request, as well as censorship laws.[48] Since February 2024, hosting service providers that do not register with the authorities are liable to be banned from providing their services in Russia.[49]

On March 20, 2025, users in Russia began reporting problems accessing websites using IP addresses of the Content Delivery Network (CDN) service provider Cloudflare across several internet service providers in multiple regions of Russia. Internet censorship researchers noted that this was caused by centralized state blocking. Cloudflare is widely used as a CDN service, including in Russia.[50]

Roskomnadzor blamed the issue on the foreign servers that Russian services rely on, implying that it was due to a failure by Cloudflare. In April, Roskomnadzor published a statement threatening to block foreign hosting service providers if they fail to comply with pertinent laws.[51]

On May 21, 2025, Cloudflare replied to HRW's letter of inquiry, stating that it is generally unable to identify or confirm government-directed blocking, has not received any notice from any Russian entity regarding the reported disruptions, and has never blocked websites at the request of the Russian government. On June 26, 2025, Cloudflare

---

47 Federal Law "On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' and the Federal Law 'On Communications,'" No. 406-FZ, adopted July 31, 2023, http://publication.pravo.gov.ru/document/0001202307310022 (accessed July 7, 2025).

48 Federal Law "On the Unified Biometric System and Amendments to Certain Legislative Acts of the Russian Federation," No. 572-FZ, adopted December 25, 2023, https://www.consultant.ru/document/cons_doc_LAW_453265/3docac60971a511280cbba229d9b6329c07731f7/ (accessed July 7, 2025).

49 "As of February 1, Hosting Providers Not Included in Roskomnadzor's Registry Are Prohibited from Providing Hosting Services in Russia" ("С 1 февраля хостинг-провайдерам, не включенным в реестр Роскомнадзора, запрещено оказывать услуги хостинга в России"), Main Radio Frequency Center, February 1, 2024, https://portal.noc.gov.ru/ru/news/s-1-fevralya-hosting-provajderam-ne-vklyuchennym-v-reestr-roskomnadzora-zapreshcheno-okazyvat-uslugi-hostinga-v-rossii/ (accessed July 7, 2025).

50 "Cloudflare Radar 2024 Year in Review," Cloudflare, December 9, 2024, https://blog.cloudflare.com/radar-2024-year-in-review/ (accessed July 7, 2025).

51 "West Hosters Will Be Blocked in Russia," Roskomsvoboda, April 7, 2025, https://roskomsvoboda.org/en/post/west-hosters-will-be-blocked-in-russia/ (accessed July 7, 2025).

published a blog outlining how Russian ISPs have been throttling web services protected by Cloudflare since June 9, 2025, leaving Russian internet users unable to access the open internet.[52]

According to Russian internet freedom watchdogs, Amazon and Fastly services were also affected by the blockings.[53]

In December 2024, Roskomnadzor had already threatened to block eight foreign hosting service providers for failure to comply with Russia's legislation, namely, GoDaddy.com, Amazon Web Services, HostGator.com, Kamatera, Ionos, Network Solutions, DigitalOcean, and Hetzner Online.[54]

Transport Layer Security

On November 5, 2024, users in Russia began reporting problems accessing thousands of websites using TLS Encrypted ClientHello (ECH) protocol with Server Name Indication cloudflare-ech.com.[55] This protocol extension protects the privacy of the users by obfuscating the website they are trying to connect to which makes the traffic interception more difficult.

On November 7, 2024, the Public Communication Network Management and Communication Center of Roskomnadzor, published a statement recommending that users in Russia stop using Cloudflare, claiming that its TLS ECH protocol violates Russia's laws by providing access to banned content. The statement also said that TPSUs were now blocking access to Cloudflare CDN services.[56]

---

[52] "Russian Internet Users Are Unable to Access the Open Internet," Cloudflare, July 15, 2025, https://blog.cloudflare.com/russian-internet-users-are-unable-to-access-the-open-internet/ (accessed July 16, 2025).

[53] "Internet Shutdown in Russia Caused by Blocking of Cloudflare, Amazon, and Fastly Services," Roskomsvoboda, March 20, 2025, https://roskomsvoboda.org/en/post/internet-shutdown-in-russia-by-cloudflare-amazon/ (accessed July 7, 2025).

[54] "Roskomnadzor Allowed for the Possibility of Restricting the Work of Foreign Providers" ("Роскомнадзор допустил ограничение работы зарубежных провайдеров"), Vedomosti, December 7, 2024, https://www.vedomosti.ru/technology/news/2024/12/07/1079961-roskomnadzor-dopustil-ogranichenie-raboti-zarubezhnih-provaiderov (accessed July 7, 2025).

[55] "Blocking of Encrypted ClientHello (ECH) on Cloudflare" ("Блокировка Encrypted ClientHello (ECH) на Cloudflare"), NTC.party, August 7, 2024, https://ntc.party/t/блокировка-encrypted-clienthello-ech-на-cloudflare/12837 (accessed July 7, 2025).

[56] "We recommend stop using Cloudflare CDN service" ("Рекомендуем отказаться от CDN-сервиса CloudFlare"), Roskomnadzor, November 7, 2024, https://shorturl.at/mavzF (accessed April 10, 2025).

According to Cloudflare's written response to HRW, although Cloudflare is "aware of reports related to ECH blocking in Russia, and [it has] observed signals consistent with tampering at various points in time, it can be challenging for a service provider like Cloudflare to confirm intentional blocking of a specific protocol."[57]

[57] Written response of Cloudflare to HRW's letter of inquiry, dated May 21, 2025.

II. State Control over RuNet Infrastructure

The 2019 "sovereign internet" law had an official objective to ensure that the Russian segment of the internet (RuNet) could operate in isolation if cut off from the global internet. In reality, the authorities used this law to consolidate control over the RuNet infrastructure to allow for state interference into its work. After Russia's full-scale invasion of Ukraine in February 2022, and tech and telecom related sanctions that followed, the process of nationalization of internet architecture in Russia accelerated.[58]

Internet Service Providers (ISPs)

Since 2019, the authorities have been engaging in more comprehensive mapping of existing ISPs and Internet exchange points (IXPs), including their connection points. For instance, the 2023 amendments obliged ISPs to provide information about the points of connection with other ISPs and IXPs.[59] In May 2024, a new government decree obliged ISPs to provide information about the planned connections to ISPs and IXPs.[60] According to the authorities, this information was needed to ensure that ISPs direct their traffic via TSPU.[61]

According to an author of a popular Telegram channel on internet blockings, whose name is not disclosed for security reasons, the diversity and multitude of ISPs across the RuNet challenges the state control of the internet infrastructure and censorship.[62] However, the number of all valid telecommunication licenses, which include radio, satellite, and TV broadcasting in addition to internet services, halved over the past ten years from 53,538

[58] Maria Kolomychenko, "The Impact and Limits of Sanctions on Russia's Telecoms Industry," DGAP, March 12, 2024, https://dgap.org/en/research/publications/impact-and-limits-sanctions-russias-telecoms-industry (accessed July 7, 2025); Maria Kolomychenko, "How Sanctions Work: High-Tech Industries Manage to Maintain Services and Infrastructure, but Fail to Develop Them," Re: Russia, March 26, 2024, https://re-russia.net/en/review/707/ (accessed July 7, 2025).

[59] Federal Law "On Amendments to the Federal Law 'On Communications,'" No. 473-FZ.

[60] Federal Law "On Amendments to Articles 333-33 and 333-40 of Part Two of the Tax Code of the Russian Federation," No. 497-FZ, adopted September 28, 2023, http://publication.pravo.gov.ru/document/0001202309280013 (accessed July 7, 2025).

[61] "Traffic Filtering" ("Справиться с трафиком"), RSpectr, March 27, 2023, https://rspectr.com/articles/trafik-filtruj (accessed July 7, 2025); "MUSE 2022 Sergey Tyomny — Obligations of Telecom Operators to Install TSPU and Route Traffic in the Network" ("MUSE 2022 Сергей Тёмный — Обязательства операторов связи по установке ТСПУ и пропуска трафика в сети"), FORUM MULTISERVICE, YouTube video, October 5, 2022, https://www.youtube.com/watch?v=7aJE8oKTVHM (accessed July 7, 2025).

[62] Human Rights Watch online interview with an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, April 2, 2025.

in May 2016 to 26,229 in April 2025.[63] The consolidation and merger of ISPs does not only increase the efficiency of internet traffic manipulation but also increases the risks for users in case of ISP malfunction.[64]

What is more, from January 2024, the fee for obtaining the obligatory license for providing internet services increased 130-fold from $88 (7,500 RUB) to $11,700 (1,000,000 RUB).[65] This made obtaining a license for small ISPs more challenging.

Whilst there are at least 493 ISPs in Russia, more than half of all IP addresses on RuNet are managed by seven top ISPs, with 25 percent belonging to a state-owned company Rostelecom and the ownership of other IP addresses spread across six companies owned by the Russian government or oligarchs.[66]

---

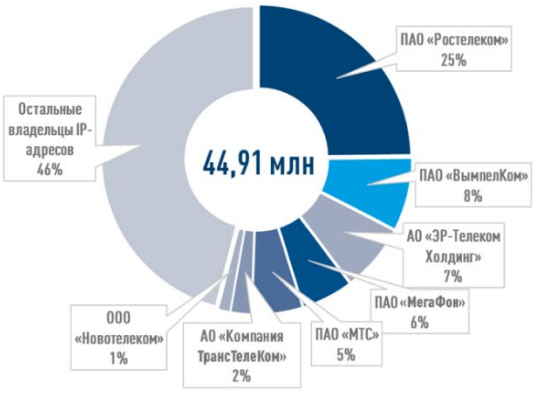
[63] "Licenses in the Field of Communications in the Russian Federation: Issued vs. Active" ("Лицензии в области связи в РФ: выданные vs действующие"), iFreedomLab, https://ifreedomlab.net/connectivity-rating/licenses-russia/ (accessed July 7, 2025); "Licensing and Permitting Activities in the Field of Communications" ("Разрешительно-лицензионная деятельность в сфере связи"), Roskomnadzor, https://rkn.gov.ru/activity/connection/register/license/, accessed July 7, 2025.

[64] "Runet Providers" ("Провайдеры Рунета"), iFreedomLab, https://ifreedomlab.net/connectivity-rating/connectivity-provaders/ (accessed July 7, 2025).

[65] "New Telecom Operators Granted Equal Rights with Established Ones" ("Новых операторов связи уравняли в правах со старыми"), Rossiyskaya Gazeta, February 16, 2024, https://rg.ru/2024/02/16/novyh-operatorov-sviazi-uravniali-v-pravah-so-starymi.html, accessed July 7, 2025; Federal Law "On Amendments to Articles 333-33 and 333-40 of Part Two of the Tax Code of the Russian Federation," No. 497-FZ.

[66] "Public Report, December 2024" ("Публичный отчет, декабрь 2024"), National Coordination Center for Computer Incidents (NCCCI), December 31, 2024, https://portal.noc.gov.ru/documents/235/Публичныи_отчет_декабрь_2024_итог_.pdf (accessed July 7, 2025);
Nika Sizova and Ekaterina Kinyakina, "Roskomnadzor Intends to Monitor All Attempts to Circumvent Blockades," Vedomosti, December 18, 2024, https://www.vedomosti.ru/technology/articles/2024/12/18/1082164-roskomnadzor-nameren-kontrolirovat-vse-popitki-obhoda-blokirovok (accessed July 7, 2025); "Roskomnadzor Will Monitor All Attempts to Circumvent Blockades" ("Роскомнадзор будет отслеживать все попытки обхода блокировок"), Habr, https://habr.com/ru/news/795495/ (accessed July 7, 2025).

Выделенное IP-адресное пространство	
Наименование организации	Количество IP-адресов
ПАО «Ростелеком»	11 139 840
ПАО «ВымпелКом»	3 481 088
АО «ЭР-Телеком Холдинг»	3 222 016
ПАО «МегаФон»	2 440 960
ПАО «МТС»	2 408 704
АО «Компания ТрансТелеКом»	984 832
ООО «Новотелеком»	589 824
Остальные владельцы IP-адресов	20 643 072
Всего	44 910 336



Screenshot from the publicly available 2023 annual report by the Center for Public Communications Network Monitoring and Management, which is a municipal state-funded agency. The table provides data on how many IP addresses have been allocated to eight organizations. The data is as follows: “Allocated IP addresses space; Organization name and number of IP addresses: PJSC Rostelecom – 11,139,840; PJSC VimpelCom – 3,481,088; JSC ER-Telecom Holding – 3,222,016; PJSC MegaFon – 2,440,960; PJSC MTS – 2,408,704; JSC TransTelecom Company – 984,832; LLC "Novotelecom" – 589,824; Other IP address owners – 20,643,072; Total – 44,910,336.” © Center for Public Communications Network Monitoring and Management, 2023.

National Domain Name System

Since January 2021, ISPs have been required to use the national domain name system (DNS), which was created under the “sovereign internet” law. The DNS works as the address book of the internet and translates a domain name (like www.hrw.org) into a numerical IP address, which is needed to locate the website and connect a user.

The core components of DNS infrastructure (root servers) are managed by independent organizations outside Russia. When users type in websites ending in .ru .su and .рф (the country code top-level domains, or ccTLDs, for Russia) into their browser, the DNS system first queries one of the root servers to locate the website. The root server then sends a request to the servers for .ru .su and .рф domains which are located in Russia. By creating its own national DNS alternative, Russian authorities aim to continue the functioning of the RuNet in the event that root servers, which are outside Russia, stop processing requests for websites using Russian ccTLDs. The Coordination Center for .RU/.РФ Domains, a state-affiliated non-profit organization, manages the .ru and .рф domains.

According to interviewees, when a user attempts to connect to a specific website, the national DNS would allow Russian authorities to redirect them to another website or show that the page is unavailable.[67] This provides additional risks both in terms of censorship and surveillance.[68]According to the authorities, the national DNS had 1 million users per day by July 2022.[69]

According to the Internet Society, Russia's National DNS is based on an approach that fundamentally fragments the global DNS, and, as a result, undermines and fragments the global nature of the internet itself, and can be used as a tool for censorship and surveillance, violating citizens' privacy and security.[70] Additionally, even though the stated aim of the national DNS is to mitigate the threat of being disconnected from the global DNS, this approach also creates a single point of failure, increasing the risk of large-scale internet disruptions.

In January 2024, users in Russia reported large scale disruptions when trying to access .ru and .рф websites. The state managed Coordination Center for .ru/.рф domain names published a statement saying that the disruptions were caused by an update in global Domain Name System Security Extensions (DNSSEC) system, which is a security extension that protects users when connecting to the global DNS.[71]

The Coordination Center and Roskomnadzor emphasized that the disruptions did not affect ISPs using the national DNS and recommended switching to the national system to avoid such problems in the future.[72] In May, Roskomnadzor said that the connection to websites via national DNS will be allowed even if the DNSSEC security extension does not

[67] Human Rights Watch online interview with Denis Yagodin, April 7, 2025; Human Rights Watch online interview with a digital security expert, whose name is withheld due to security concerns, April 9, 2025.

[68] Human Rights Watch online interview with a digital security expert, whose name is withheld due to security concerns, April 9, 2025.

[69] "National Domain Name System (NSDI)" ("Национальная система доменных имен (НСДИ)"), NCCCI, August 25, 2022, https://portal.noc.gov.ru/ru/news/2022/08/25/nsdi/ (accessed July 7, 2025).

[70] "Russia's National DNS," Internet Society, December 1, 2023, https://www.internetsociety.org/resources/internet-fragmentation/russias-national-dns/ (accessed July 7, 2025).

[71] "Roskomnadzor and the National Domain Name System (NSDI)" ("Роскомнадзор и Национальная система доменных имен (НСДИ)"), Coordination Center for TLD RU, December 18, 2024, https://cctld.ru/media/news/kc/35566/ (accessed July 7, 2025).

[72] "RKN recommends that ISPs connect to the National Domain Name System to avoid disruptions" ("РКН рекомендует провайдерам подключиться к Нацсистеме доменных имен для избежания сбоев"), Interfax, January 31, 2024, https://www.interfax.ru/russia/943866 (accessed July 16, 2025).

function properly. This significantly increases security risks for the users. Authorities also fined companies that failed to connect to the national DNS.[73]

Since August 2020, the .su domain, which was associated with the Soviet Union and is perceived by the current authorities as one of their country code top-level domains, is managed by the state governed Russian Institute for Public Networks (RIPN).[74] In July 2024, Alexey Soldatov, who is known as one of the RuNet founders, was sentenced to two years in prison for "abuse of power" after allegedly trying to sell IP addresses to a foreign company under his ownership. Independent reporters claimed that Soldatov's prosecution is politically motivated and connected to the state attempt to take over .su domain that had been managed by Internet Development Fund, co-owned by Soldatov, prior to RIPN.[75] At the time of writing, Soldatov, age 73, is serving his sentence at Correctional Colony N2 in Ryazan region, despite serious illness and deteriorating health.[76] According to his family and lawyers, his condition is critical. Soldatov should be eligible for release on humanitarian grounds. In 2025, Internet Corporation for Assigned Names and Numbers (ICANN) announced its plans to retire .su domain.[77]

Russian TLS Certificate Authority

TLS (transport layer security) certificates are another layer of security on the internet that Russian authorities are trying to nationalize. Such a certificate verifies that the website belongs to a trusted entity and that the exchange between the website server and the user is encrypted. If the website does not have a valid TLS, most browsers will notify the user that the connection is not secure.

---

[73] Telegram post of the account "Chronicle of the sovereign runet" ("Летопись суверенного рунета"), "Fine for not using the national domain name system," https://t.me/Runet90fz/480 (accessed July 22, 2025)

[74] "Roskomnadzor Will Create a System to Monitor the Stability of the Runet" ("Роскомнадзор создаст систему мониторинга устойчивости Рунета"), TASS, October 20, 2020, https://tass.ru/ekonomika/9804891 (accessed July 7, 2025).

[75] "EFF Calls for Release of Alexey Soldatov, 'Father of the Russian Internet,'" Electronic Frontier Foundation, September 2024, https://www.eff.org/deeplinks/2024/09/eff-calls-release-alexey-soldatov-father-russian-internet (accessed July 16, 2025).

[76] Maria Kolomychenko, LinkedIn post, "ICANN plans to retire the .SU domain," June 27, 2025, https://www.linkedin.com/posts/kolomychenko_icann-plans-to-retire-the-su-domain-activity-7306023743573708801-ZSaR/ (accessed July 7, 2025).

[77] Andrew Allemann, "ICANN Moves to Retire Soviet-Era .SU Country Domain Name," Domain Name Wire, March 11, 2025, https://domainnamewire.com/2025/03/11/icann-moves-to-retire-soviet-era-su-country-domain-name/ (accessed July 7, 2025).

TLS certificates are issued by certificate authorities (CAs), which are in most cases commercial entities. Whilst there is no official registry of trusted certificate authorities, the web browsers (such as Google Chrome, Safari, or Mozilla Firefox) have a list of CAs that they trust.

Following Russia's full-scale invasion of Ukraine, a number of states, including the United States (US), the United Kingdom (UK), and the European Union (EU) introduced sanctions against specific Russia affiliated entities such as banks and state agencies.[78] In turn, some foreign certificate authorities stopped issuing certificates to Russian websites in an attempt to comply with the sanctions.[79]

This prompted Russian authorities to create their own certificate authorities, such as the Ministry of Digital Development's National Certifying Center. In February 2023, internet users reported seeing notifications prompting them to install the state certificate "for stable functioning" of online payments when trying to pay for online services via Russia's largest commercial bank Sberbank.[80]

According to technology journalist Maria Kolomychenko, the potential danger of a state issued TLS certificate is a threat of cyberattacks such as interception and decryption of the internet traffic between the communicating parties without them noticing.[81] For example, the government of Kazakhstan in 2015 introduced a national certificate that allowed it to intercept traffic that internet users thought was encrypted.[82]

---

78 "Russia Sanctions Guidance," UK Government, updated April 25, 2025, https://www.gov.uk/government/publications/russia-sanctions-guidance/russia-sanctions-guidance (accessed July 7, 2025); "EU Sanctions Against Russia Explained," Council of the European Union, https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/ (accessed July 7, 2025).

79 "Roskomnadzor Restricted Access to Facebook and Twitter" ("Роскомнадзор ограничил доступ к Facebook и Twitter"), RBC, March 3, 2022, https://www.rbc.ru/technology_and_media/03/03/2022/621f8b8e9a794717d8efc87a (accessed July 7, 2025).

80 "Roskomnadzor Blocked Facebook" ("Роскомнадзор заблокировал Facebook"), Habr, March 4, 2022, https://habr.com/ru/news/654421/ (accessed July 7, 2025); "VkusVill, DNS, and Afisha Began Requiring a Digital Ministry Certificate for Order Payments" ("«ВкусВилл», DNS и «Афиши» начали требовать сертификат Минцифры для оплаты заказов"), Retail.ru, February 7, 2023, https://www.retail.ru/news/vkusvill-dns-i-afishi-nachali-trebovat-sertifikat-mintsifry-dlya-oplaty-zakazov--7-fevralya-2023-225453/ (accessed July 7, 2025).

81 Human Rights Watch online interview with tech journalist Maria Kolomychenko, April 8, 2025.

82 Eva Galperin and Amul Kalia, "Kazakhstan Considers Plan to Snoop on All Internet Traffic," Electronic Frontier Foundation, December 7, 2015, https://www.eff.org/deeplinks/2015/12/kazakhstan-considers-plan-snoop-all-internet-traffic (accessed July 7, 2025).

Some Russian websites, such as those belonging to the State Duma and the Federal Security Service, continue operating without a TLS certificate, because they use unencrypted protocol HTTP, rather than HTTPS. When a user accesses a website that uses HTTP, all of their requests and responses are unencrypted and can be read by anyone who is monitoring the session, including malicious actors. However, some websites, such as that of the Ministry of Defense, require anyone accessing the website to use the encrypted HTTPS protocol for all users with a certificate issued by Russian Certificate Authorities, which means that users have to install Russian CA's certificates to access the website.

Apart from Russian Yandex and Atom, no commonly used web browsers added Russian TLS certificates to the trusted list.[83] Hence, in order to visit the websites that only use Russian certificates, users either have to manually mark them as trusted or access such websites via Russian browsers, which exposes them to security and privacy risks. In March 2022, authorities recommended that Russians exclusively use Yandex as their browser to ensure uninterrupted access to all government websites.[84]

Some Russian programs that require installation on a user's device, such as accounting software or Yandex browser software, encourage adding the state certificate to the trusted list in order to function "properly."[85] Furthermore, the Android phone apps of Yandex and Atom, another browsing software, allow access to websites with Russian CA's TLS by default when browsing inside the apps.

In its written response to Human Rights Watch's letter of inquiry Yandex stated that its "browser recognizes National Certification Authority certificates for domains included in the Certificate Transparency public log," which is a public list of certificates that confirms their authenticity and allows to detect malicious ones.[86]

---

[83] "State Hacking" ("Государственный хакинг"), Teplitsa of Social Technologies, December 20, 2023, https://te-st.org/2023/12/20/state-haking/ (accessed July 7, 2025).

[84] Fabian Burkhardt and Mariëlle Wijermars, "Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions Are Reshaping Russia's Repressive Capacities," The SAIS Review of International Affairs 42, no. 2 (April 27, 2023): 21–43, https://doi.org/10.1353/sais.2022.0009 (accessed July 7, 2025).

[85] "TLS Certificate from the Ministry of Digital Development on Applications" ("TLS-сертификат Минцифры на приложениях"), NTC Forum, December 20, 2023, https://ntc.party/t/tls-сертификат-минцфиры-на-приложениях/15748 (accessed July 7, 2025).

[86] Written response of Yandex to HRW's letter of inquiry, dated June 20 ,2025.

The use of the state CA certificates can expose users to data interception and increase their security risks online.

Network Routing

In November 2024, the Russian authorities announced their plans to create their own infrastructure for validating the internet routing, or a path that data packets take across the internet.[87] This would allow the authorities, for instance, to route traffic via a path that does not cross the country's border. In the past, Roskomnadzor tried controlling internet routing by pressuring ISPs to change their internet routing path.[88]

Internet routing protocols generally choose the most efficient path, forwarding packets to devices in the network (hops) until the information reaches the final destination. Interfering with internet routing can cause slower connections, disruptions, and security risks.

The "sovereign internet" law already grants the authorities the power to manage the traffic routing in case of supposed threats.

[87] "Russia Is Creating Its Own Platform for Distributing Applications" ("Россия создаёт собственную платформу для распространения приложений"), CNews, November 5, 2024, https://www.cnews.ru/news/top/2024-11-05_rossiya_sozdaet_sobstvennuyu (accessed July 7, 2025).

[88] "Russia Is Creating Its Own Platform for Distributing Applications" ("Россия создаёт собственную платформу для распространения приложений"), Habr, March 27, 2023, https://habr.com/ru/articles/735482/ (accessed July 7, 2025).

III. Internet Shutdowns

Internet shutdowns are measures taken by a government to intentionally disrupt access to, and the use of, information and communications systems online. Experts define internet shutdowns to include actions that restrict access to the internet completely, or slow down speed, or restrict certain content, or block certain social media platforms and messaging apps.[89]

Regional Shutdowns

Over the past years, Russian authorities have intensified regional shutdowns, limiting internet access or restricting messaging apps in specific regions, often in apparent connection with political events, including during mass protests.[90]

On January 17, 2024, a court in Baymak, Bashkortostan, sentenced Bashkir environmental activist Fail Alsynov to four years in prison for "inciting hatred," a politically motivated prosecution in reprisal for a speech he had given at an environmental rally.[91] His sentencing sparked protests that were then brutally dispersed by the police.

The night before Alsynov's sentencing, users reported hindered access to WhatsApp and Telegram in Bashkortostan.[92] Mobile communication networks and calls/texts in proximity to the court building also appeared to have been shut down.

---

[89] UN Human Rights Council, "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights," Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/50/55, May 2022, https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts (accessed July 7, 2025).

[90] "Authorities Tested at Least 11 Types of Different Blockades in 2024" ("Власти протестировали не менее 11 типов разных блокировок в 2024 году"), Агентство, February 11, 2025, https://www.agents.media/vlasti-protestirovali-ne-menee-11-tipov-raznyh-blokirovok-v-2024-godu/ (accessed July 7, 2025).

[91] "We Consider Failya Alsynov a Political Prisoner," Memorial, May 22, 2024, https://memopzk.org/en/news/my-schitaem-politzaklyuchyonnym-failya-alsynova/ (accessed July 7, 2025).

[92] Telegram post of the account "Roskomsvoboda," "Protests in Bashkortostan Took Place Amid Shutdown and Blocking of Telegram Channels." ("Протесты в Башкортостане прошли под шатдаун и блокировку Telegram-каналов"), https://t.me/roskomsvoboda/11916 (accessed July 7, 2025).

A week later similar disruptions to Telegram and WhatsApp were reported in other regions of Russia. In Yakutiya, the blockings lasted from January 23 to 27 which corresponded with a period when protests were taking place regarding a local murder; in addition to blocked messaging services, bank card payments that rely on internet connections were affected in some shops, banks, and postal offices.[93] The local authorities claimed to have been running "maintenance work."[94]

On October 10, 2024, users in Dagestan, Chechnya, Stavropol, and Ingushetia reported that Telegram was blocked.[95] After six months of blockings, on March 6, 2025, Dagestan's minister of digital development said that Telegram was blocked in Dagestan and Chechnya at the request of the federal law enforcement authorities,[96] because, among other things, Telegram had been used by people linked to an antisemitic attack on Makhachkala airport in October 2023.[97]

The authorities also increasingly shut down internet in connection with the possible drone attacks by the Ukrainian army.

In December 2024, the ministry of internal policies, information and communications in Russia-occupied Crimea announced the possible shutdown of mobile internet to "ensure

---

93 Elena Belyaeva, "Regions Are Being Silenced: How Russian Authorities Learned to Block Messengers and Protest Channels" ("Регионам режут языки. Как российские власти научились блокировать мессенджеры и протестные каналы"), Novaya Gazeta, February 3, 2024, https://novayagazeta.ru/articles/2024/02/03/regionam-rezhut-iazyki (accessed July 7, 2025).

94 Telegram post of the account "Roskomsvoboda," January 24, 2024, https://t.me/roskomsvoboda/11942 (accessed July 7, 2025); "A Failure Occurred in the Operation of Telegram, WhatsApp, and Viber" ("В работе Telegram, WhatsApp и Viber произошел сбой"), Holod, January 24, 2024, https://holod.media/2024/01/24/v-rabote-telegram-whatsapp-i-viber-proizoshel-sboi/ (accessed July 7, 2025); "Training, Rights Violations, and Charm: Yakutia Officials on Messenger Outages" ("Тренировка, нарушение прав, прелесть: госдеятели Якутии о сбоях мессенджеров"), SakhaDay, January 26, 2024, https://sakhaday.ru/news/trenirovka-narushenie-prav-prelest-gosdeyateli-yakutii-o-sboyah-messendzherov (accessed July 7, 2025).

95 "Dagestan, Chechnya, and Ingushetia to Be Connected to the Sovereign Internet" ("Дагестан, Чечню и Ингушетию подключат к суверенному интернету"), Chernovik, December 6, 2024, https://chernovik.net/index.php/news/dagestan-chechnyu-i-ingushetiyu-podklyuchat-k-suverennomu-internetu-skoro-vtoroy-mesyac-kak-v, accessed July 7, 2025.

96 Katya Zagvozdkina, "Telegram Blocked in Dagestan and Chechnya" ("В Дагестане и Чечне заблокировали Telegram"), Forbes Russia, March 8, 2025, https://www.forbes.ru/tekhnologii/532303-v-dagestane-i-cecne-zablokirovali-telegram (accessed July 7, 2025).

97 "Russia: Inadequate Response to Antisemitism in North Caucasus," Human Rights Watch, November 9, 2023, https://www.hrw.org/news/2023/11/09/russia-inadequate-response-antisemitism-north-caucasus, accessed July 7, 2025.

[public] security."[98] Experts suggested that this was likely linked to the possibility of drone attacks by the Ukrainian army.[99]

In April 2025, Rostov regional authorities confirmed that they and nine other regional authorities had slowed down mobile internet at night in their respective regions due to the threat of drone attacks.[100]

On May 5, internet users in Moscow, the region surrounding Moscow, and in Saint Petersburg reported mobile bandwidth and internet access disruptions on four major mobile service providers, which cited "external causes" for disruptions.[101] The authorities accused Ukraine of drone attacks and published a warning that such disruptions were due to "ensuring security" ahead of the annual Victory Day celebrations that commemorated the Soviet Union's victory over Nazi Germany in World War II.[102] Between May 5 and 9, users in over 30 regions of Russia reported communication disruptions.[103]

In March 2025, the chair of the Digital Economy Development Fund German Klimenko stated that "regional blockings were very easy to carry out" via TSPU equipment.[104] However, in practice different regions might rely on the same underlying infrastructure and thus the regions that are not the intended targets might be also affected by the shutdowns.

---

[98] Telegram post of the account "Mininform Crimea Z," "To Ensure the Safety of Crimean Residents, Mobile Internet May Be Disconnected Starting Today" ("Для обеспечения безопасности жителей Крыма с сегодняшнего дня возможны отключения мобильного интернета"), https://t.me/MiniformRK/5354 (accessed July 7, 2025).

[99] "Mobile Internet Outages Announced in Crimea" ("В Крыму анонсировали отключения мобильного интернета"), CNews, December 18, 2024, https://www.cnews.ru/news/top/2024-12-18_v_krymu_anonsirovali_otklyucheniya (accessed July 7, 2025).

[100] Alexey Zhabin, "Rostov-on-Don Sets Up Networks" ("Ростов-на-Дону расставил сети"), Kommersant, April 24, 2025, https://www.kommersant.ru/doc/7677443 (accessed July 7, 2025).

[101] "Mobile Network Outage in Russia During May Holidays" ("Предпраздничный сбой связи затронул операторов в Москве и регионах"), Roskomsvoboda, May 5, 2025, https://roskomsvoboda.org/en/post/mobile-network-outage-russia-holiday-may-2025/ (accessed July 7, 2025).

[102] "Internet Disruptions Reported Across Russia" ("Сбои в работе интернета"), Vedomosti, May 5, 2025, https://www.vedomosti.ru/society/news/2025/05/05/1108307-sboyah-v-rabote-interneta (accessed July 7, 2025); Alexey Zhabin, "Rostov-on-Don Sets Up Networks" ("Ростов-на-Дону расставил сети").

[103] Ibid.

[104] "Klimenko: All Russian Regions Have Tools to Block Telegram" ("Клименко: у всех регионов в РФ есть возможности блокировки Telegram"), Argumenty i Fakty, https://aif.ru/society/klimenko-u-vseh-regionov-v-rf-est-vozmozhnosti-blokirovki-telegram (accessed July 7, 2025).

RuNet Isolation Drills

Since December 2019, authorities have carried out at least seven "drills" to test the RuNet's "resilience" against "unwanted external interference" by "unfriendly countries." In September 2022, a representative of the National Coordination Center for Computer Incidents under the Federal Security Service (FSB) said that the state was "seriously considered cutting RuNet off from the rest of the internet" due to a wave of cyberattacks following Russia's full-scale invasion of Ukraine in February 2022.[105]

Some of the drills reportedly tested the functioning of the RuNet in case it is "cut off from the global internet," including in separate regions of Russia.[106] According to the authorities, the goal was to identify vulnerabilities, i.e. dependencies on foreign infrastructures. The authorities did not disclose the details of the tests' procedure and outcomes.

Despite the authorities repeatedly stating that the tests do not affect average users, users have reported internet disruptions during those "drills." For example, in December 2024, users in Dagestan, Chechnya, and Ingushetia reported being unable to access foreign websites, apps, and messengers such as Telegram, YouTube, and Google. Also, most VPNs did not work.[107] Some users were unable to order a taxi via Russian app Yandex.[108]

---

[105] Yulia Tishina, "Without Exercises—Darkness" ("Без учений — тьма"), Kommersant, December 13, 2022, https://www.kommersant.ru/doc/5705859 (accessed July 7, 2025).

[106] Anastasia Gavrilyuk, "Runet in Its Own Juice: Will Russia Disconnect from the Global Internet?" ("Рунет в собственном соку: ждать ли отключения интернета от международной Сети"), Forbes Russia, July 7, 2023, https://www.forbes.ru/tekhnologii/492400-runet-v-sobstvennom-soku-zdat-li-otklucenia-interneta-ot-mezdunarodnoj-seti (accessed July 7, 2025);

"Roskomnadzor Reports Annual Runet Resilience Test" ("В Роскомнадзоре сообщили о ежегодной проверке устойчивости Рунета"), TASS, November 14, 2024, https://tass.ru/obschestvo/22403517, accessed July 7, 2025.

[107] Yulia Rybina, "Dagestan Operator Explains Website Outages as Roskomnadzor Drills" ("Оператор в Дагестане объяснил сбои в работе сайтов учениями РКН"), Kommersant, December 12, 2024, https://www.kommersant.ru/doc/7361237 (accessed July 7, 2025).

[108] "Drills Begin to Connect Dagestan, Ingushetia, and Chechnya to the Sovereign Internet" ("Учения по подключению Дагестана, Ингушетии и Чечни к суверенному интернету начались"), Chernovik, December 6, 2024, https://chernovik.net/news/ucheniya-po-podklyucheniyu-dagestana-ingushetii-i-chechni-k-suverennomu-internetu-nachalis (accessed July 7, 2025).

Several ISPs published announcements confirming the disruptions in accessing "foreign websites" and VPNs. They stated that disruptions were caused by Roskomnadzor's drills and might last for a day.[109]

The law requires that competent authorities publish the drills' annual schedule in advance, however, they have consistently failed to do so. Internet users get no warning of the upcoming drills, nor any clarity on what services may be affected. The tests are carried out by the state directly via TSPU, and ISPs have neither control nor insight into the testing.

Collateral Blockings

According to a digital expert whose name is withheld due to security reasons, increasing accidental disruptions of internet network connectivity that arises from the internet traffic manipulation by Russian authorities raise serious concerns for the rights of internet users.[110]

Internet traffic and routing is a complex and interconnected system that is intended to be self-regulating. By meddling with it, authorities create erratic disruptions that are hard to predict and often difficult to fix.

In Russia, such collateral internet disruptions have often prevented internet users from accessing key websites and services online.[111]

On February 27, 2024, internet users all over Russia reported major issues accessing the internet across all major ISPs, including messengers WhatsApp, Telegram, Viber, and Gosuslugi portal providing key state services online.[112] The next day, the deputy chair of

[109] Telegram post of channel "Ellco," December 6, 2024, https://t.me/ellco_ru/785, accessed July 7, 2025; Yulia Litvinenko, "Roskomnadzor Disconnects North Caucasus from the Global Internet" ("Роскомнадзор отключил Северный Кавказ от мирового интернета"), Novye Izvestia, December 6, 2024, https://newizv.ru/news/2024-12-06/roskomnadzor-otklyuchil-severnyy-kavkaz-ot-mirovogo-interneta-434828 (accessed July 7, 2025).

[110] Human Rights Watch online interview with a digital security expert, whose name is withheld due to security concerns, April 9, 2025.

[111] "Roskomnadzor Conducts Drills to Test Runet's Resilience" ("Роскомнадзор: на учениях с операторами связи проверяется работа ключевых сервисов на случай внешнего воздействия"), Habr, December 6, 2024, https://habr.com/ru/news/796569/ (accessed July 7, 2025).

[112] "Telegram and Half of Runet Experience Major Outage" ("Telegram и пол-Рунета пережили удивительный сбой"), CNews, February 27, 2024, https://www.cnews.ru/news/top/2024-02-27_telegram_i_pol-runeta_perezhili, accessed July 7, 2025.

the State Duma's Committee on Information Policy Anton Tkachev claimed that the disruptions were caused by Roskomnadzor adjusting the settings of TSPU.[113]

On January 14, 2025, customers of most ISPs across Russia reported short-term inaccessibility of state websites, Google services, and other websites.[114] ISPs commented that the disruptions were not caused by problems on their side.[115] According to an author of a popular Telegram channel on internet blockings, whose name is withheld for security reasons, the disruptions were caused by a TSPU update and were resolved once the traffic was directed to bypass TSPU.[116]

On March 20, 2025, when the authorities began blocking Cloudflare IP addresses, internet users across numerous regions and ISPs in Russia reported mass disruptions across numerous popular foreign and Russian websites and online services, such as YouTube, Duolingo, Twitch, and others.[117] On March 24, users reported being unable to access the app of Sberbank, the biggest bank in Russia.[118]

In response to this, Roskomnadzor stated that the disruptions were caused by the malfunctioning of "foreign server infrastructure" used by the affected websites and services and recommended switching to Russian servers.[119]

---

[113] "Massive Runet Outage Caused by Roskomnadzor's Overblocking" ("Грандиозный сбой в Рунете: Просто Роскомнадзор перестарался с блокировками"), CNews, February 28, 2024, https://www.cnews.ru/news/top/2024-02-28_grandioznyj_sboj_v_runete (accessed July 7, 2025).

[114] Anna Ustinova and Liana Lipanova, "Major Outage in Runet Services" ("В работе сервисов рунета произошел масштабный сбой"), Vedomosti, January 14, 2025, https://www.vedomosti.ru/technology/articles/2025/01/14/1086185-runeta-masshtabnii-sboi (accessed July 7, 2025).

[115] "Runet Experiences Total Outage, YouTube Becomes Accessible" ("Рунет пережил тотальный сбой, после которого начал работать YouTube"), CNews, January 14, 2025, https://www.cnews.ru/news/top/2025-01-14_runet_perezhil_totalnyj (accessed July 7, 2025).

[116] Human Rights Watch online interview with an author of a popular Telegram channel on blockings, whose name is not disclosed for security reasons, April 2, 2025.

[117] "Timeline of Internet Blocking Events" ("Таймлайн хроники блокировки интернета"), Taimlain Runeta, https://timeline-ru.net/timeline?article=350 (accessed July 7, 2025).

"DownDetector Russia Homepage," archived at Wayback Machine, March 20, 2025, http://web.archive.org/web/20250320103527/https://downdetector.su/ (accessed July 7, 2025).

[118] "Users Report Outages in Sberbank App and Mobile Networks; Roskomnadzor Again Blames Foreign Infrastructure" ("Пользователи сообщили о сбоях в работе приложения Сбербанка и операторов связи. В РКН снова объяснили это использованием иностранной инфраструктуры"), Meduza, March 24, 2025, https://meduza.io/news/2025/03/24/polzovateli-soobschili-o-sboyah-v-rabote-prilozheniya-sberbanka-i-operatorov-svyazi-v-rkn-snova-ob-yasnili-eto-ispolzovaniem-inostrannoy-infrastruktury (accessed July 7, 2025).

[119] Telegram post of "RBC. Novosti. Glavnoye" channel, March 20, 2025, https://t.me/rbc_news/114236 (accessed July 7, 2025).

Following YouTube throttling, the users reported widespread disruptions of Google services, such as maps, cloud storage, and Android devices.[120]

[120] Alena Epifanova, "Throttling of YouTube Shows That Russia Is Getting Better at Online Censorship," Carnegie Endowment for International Peace, February 12, 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/02/russia-youtube-block-attempt?lang=en (accessed July 7, 2025).

IV. Russian Tech Companies' and State Censorship and Propaganda

Censorship

With foreign platforms becoming less convenient to use in Russia without VPNs due to blockings and throttling by the authorities, internet users increasingly switch to Russian alternatives.[121] At the same time, registration of Russian tech companies and their physical presence in the country expose them to higher risks and significantly limit their ability to resist state censorship, which makes them more inclined to fall in line with the censorship and surveillance legislation.

Since February 2021, according to amendments to the Law on Information, social media platforms are required to proactively monitor and censor content that violates Russia's legislation, including information that offends "society, the state, state symbols or public officials," or information disseminated by organizations deemed "undesirable" by the state, such as Russian and international independent media and human rights groups.[122]

VK (also, "VKontakte"), initially a Russian version of Facebook, consolidated its position as the most prominent social network in Russia with more than 91 million users in the country by the end of 2024.[123] VK is also popular in some countries outside Russia, including Belarus and Kazakhstan. VK is owned and controlled by companies and persons with close ties to the Russian government, increasing the risk that they could exert control over VK's data and algorithms.[124]

---

[121] "Users Migrate to Russian Social Networks While Retaining Foreign Ones" ("Исследование: пользователи переходят в российские соцсети с сохранением зарубежных"), TASS, April 6, 2022, https://tass.ru/obschestvo/14298299 (accessed July 7, 2025).

[122] Federal Law "On Amendments to the Federal Law 'On Information, Information Technologies and the Protection of Information,'" No. 530-FZ, adopted December 30, 2020, http://publication.pravo.gov.ru/document/0001202012300062 (accessed July 7, 2025).

[123] "VK Research: Russians Are Spending More Time on Domestic Services" ("Исследование VK: россияне стали больше времени проводить в отечественных сервисах"), VK, April 24, 2025, https://vk.company/ru/press/releases/11976/ (accessed July 7, 2025).

[124] Julia Kling, Florian Toepfl, and Pascal Jürgens, "Entertainment Interspersed with Propaganda: How Nonlegacy News Accounts Deliver Explicitly Political Content to Mass Audiences on Russia's Most Popular Social Network," Information, Communication & Society 28, no. 7 (May 19, 2025): 1252–1269, https://doi.org/10.1080/1369118X.2024.2420029 (accessed July 7, 2025).

In recent years, VK became a popular video streaming platform. Over the 2024/2025 winter holidays against the backdrop of a decrease in the general traffic to YouTube following the state blockings, the number of views on VK exceeded that of YouTube. [125] Since 2022, VK has been actively carrying out a campaign to attract bloggers to its platform, with a contractual requirement to publish their videos exclusively on VK.[126]

The company, however, has been actively complying with the censorship regulations and data disclosure requests from the authorities and has become increasingly less transparent about its policies, instead of at least using all available legal means to appeal decisions and exhaust local legal remedies.[127]

A study published by Citizen Lab in July 2023 found that VK blocked thousands of videos by independent media, as well as videos containing information about the war in Ukraine and human rights issues in Belarus, about lesbian, gay, bisexual, and transgender (LGBT) people, or criticism of the Russian authorities. The same study stated that VK specifically restricted search results for LGBT-related keywords, such as "gay."[128]

In the first eight months following Russia's full-scale invasion of Ukraine in February 2022, Citizen Lab discovered a 30-fold increase in the rate of takedown orders issued against VK. For instance, VK took down 33,252 blocked videos that were analyzed in the study, citing an order by the Prosecutor General's office dated February 24, 2022.

---

[125] "VK Research: Russians Are Spending More Time on Domestic Services" ("Исследование VK: россияне стали больше времени проводить в отечественных сервисах"), VK;

"Russian Government Bond Index Up Above 114 Points First Since Last April," TASS, June 26, 2025, https://tass.com/economy/1881411 (accessed July 7, 2025).

[126] Valeria Pozychanyuk and Irina Pankratova, "YouTube Killer: Who Is Stepan Kovalchuk, Tasked with Turning VKontakte into the First Channel on the Internet" ("Убийца YouTube: кто такой Степан Ковальчук, который должен превратить ВКонтакте в Первый канал в интернете"), The Bell, October 10, 2023, https://thebell.io/amp/ubiytsa-youtube-kto-takoy-stepan-kovalchuk-kotoryy-dolzhen-prevratit-vkontakte-v-pervyy-kanal-v-internete (accessed July 7, 2025).

[127] "VK," Ranking Digital Rights: The 2025 Big Tech Edition, https://rankingdigitalrights.org/bte25/companies/VK (accessed July 7, 2025).

[128] Jeffrey Knockel, Jakub Dalek, Levi Meletti, and Ksenia Ermoshina, "Not OK on VK: An Analysis of In-Platform Censorship on Russia's VKontakte," Citizen Lab Report No. 169, University of Toronto, July 26, 2023, https://citizenlab.ca/2023/07/an-analysis-of-in-platform-censorship-on-russias-vkontakte/ (accessed July 7, 2025).

In March 2022, Kremlin-critical media TJournal reported that VK had blocked their accounts at the request of the Prosecutor General.[129] By October 2022, only a small fraction of the followed accounts on VK that were not blocked in Russia published content critical of the government.[130]

Promoting State Agenda

At the same time, Russian authorities and Kremlin-affiliated projects use VK to promote content supportive of the government, criticizing political opposition, or promoting state narratives, including on the war in Ukraine.[131] For instance, Russian language media outlet Meduza reported that 146,000 VK pages managed by "Dialogue," a state-funded organization working on state propaganda, were used to "promote state agenda" ahead of the 2024 presidential election.[132]

Yandex, another Russian tech giant, is a conglomerate of numerous digital services, including a web browser, email, taxi, movie streaming, food delivery, and much more.

Most of Yandex services are listed as information dissemination organizers and are thus obliged to store and pass on data of their users to law enforcement agencies upon demand.[133]

---

[129] "TJ Community on VK Blocked by Order of the Prosecutor General's Office" ("Сообщество TJ во ВКонтакте заблокировали по решению Генпрокуратуры"), TJ, March 26, 2024, https://tjournal.ru/news/573326-soobshchestvo-tj-vo-vkontakte-zablokirovali-po-resheniyu-genprokuratury (accessed July 7, 2025).

[129] Julia Kling, Florian Toepfl, and Pascal Jürgens, "Entertainment Interspersed with Propaganda: How Nonlegacy News Accounts Deliver Explicitly Political Content to Mass Audiences on Russia's Most Popular Social Network," Information, Communication & Society, November 15, 2024, https://doi.org/10.1080/1369118X.2024.2420029 (accessed July 7, 2025).

[130] Julia Kling, Florian Toepfl & Pascal Jürgens (15 Nov 2024): Entertainment interspersed with propaganda: how non-legacy-news accounts deliver explicitly political content to mass audiences on Russia's most popular social network VK, Information, Communication & Society, DOI: 10.1080/1369118X.2024.2420029.

[131] "Viewers Are Not Real, Views Are Boosted—But That's Not a Problem" ("Зрители не настоящие. Просмотры накручены. Но это не проблема"), Meduza, December 25, 2023, https://meduza.io/feature/2023/12/25/zriteli-ne-nastoyaschie-prosmotry-nakrucheny-no-eto-ne-problema (accessed July 7, 2025).

[132] Presidential Order No. 62919, "On the Development of the Russian Federation State Policy Guidelines Regarding Local Self-Government Until 2030," issued May 9, 2025, http://kremlin.ru/acts/assignments/orders/62919 (accessed July 7, 2025); "Viewers Are Not Real, Views Are Boosted—But That's Not a Problem" ("Зрители не настоящие. Просмотры накручены. Но это не проблема"), Meduza, December 25, 2023, https://meduza.io/feature/2023/12/25/zriteli-ne-nastoyaschie-prosmotry-nakrucheny-no-eto-ne-problema (accessed July 7, 2025).

[133] "Roskomsvoboda 2024 Highlights: Video Summary," Roskomsvoboda, January 11, 2025, https://roskomsvoboda.org/en/post/roskomsvoboda-2024-highlights-video/ (accessed July 7, 2025).

In a written response to Human Rights Watch's letter of inquiry, Yandex stated that when dealing with government requests for users' data, the company adheres strictly to the law and its own principles of user protection whilst "rigorously assessing" each such request "for legal validity, examining the basis, scope, and necessity of the demand" and "actively challenging overbroad and insufficient demands through legal channels."[134]

According to Yandex's transparency report, the Yandex browser automatically deletes links to the websites listed by the authorities as banned from its search results.[135]

Additionally, Yandex Music deleted thousands of music tracks following the request of Russian law enforcement, which alleged that they contained "fake information about the Russian army" or LGBT friendly content, among other reasons. The company made no apparent attempt to legally challenge these decisions.[136] It also labeled the music as "foreign agents," in compliance with the labeling requirement under the "foreign agents" law, which Russian authorities use to smear their critics.[137]

According to several studies by research groups and academics conducted over the past four years, Yandex's search engine algorithms have a reference bias (refer users to significantly fewer websites, sometimes with unrequested information) and source bias (direct users to fewer websites that regularly featured criticism of Russia's leadership).[138]

---

[134] Written response of Yandex to HRW's letter of inquiry, dated June 20 ,2025.

[135] "Transparency Report," Yandex, https://yandex.ru/company/privacy/transparencyreport, accessed July 7, 2025.

[136] "Transparency Report" ("Отчёт о прозрачности"), Yandex Music, https://yandex.ru/support/music/ru/rules/transparencyreport.html (accessed July 7, 2025).

[137] "Yandex Music Censors Thousands of Tracks by Government Demand," Roskomsvoboda, February 21, 2024, https://roskomsvoboda.org/en/post/yandexmusic-censors-thousands-of-tracks-by-gov-demand/, accessed July 7, 2025; "Russia: New Restrictions on 'Foreign Agents,'" Human Rights Watch, December 1, 2022, https://www.hrw.org/news/2022/12/01/russia-new-restrictions-foreign-agents (accessed July 7, 2025).

[138] Daria Kravets-Meinke, "The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool," ZOiS Spotlight, May 15, 2024, https://www.zois-berlin.de/en/publications/zois-spotlight/the-sad-fate-of-yandex-from-independent-tech-startup-to-kremlin-propaganda-tool (accessed July 7, 2025); Daria Kravets and Florian Toepfl, "Gauging Reference and Source Bias Over Time: How Russia's Partially State-Controlled Search Engine Yandex Mediated an Anti-Regime Protest Event," Information, Communication & Society, vol. 25, no. 15 (2022): 2207–2223, https://doi.org/10.1080/1369118X.2021.1933563 (accessed July 7, 2025); Evan M. Williams and Kathleen M. Carley, "Search Engine Manipulation to Spread Pro-Kremlin Propaganda," HKS Misinformation Review, February 16, 2023, https://misinforeview.hks.harvard.edu/article/search-engine-manipulation-to-spread-pro-kremlin-propaganda/ (accessed July 7, 2025).

In its June 20, 2025 letter to Human Rights Watch, Yandex stated that "search results are generated exclusively through machine learning algorithms, ensuring unbiased ranking and presentation of information," and that "all modifications to the ranking system are implemented exclusively through algorithmic updates, completely eliminating any possibility of manual interference." According to Yandex, it removes links from search results and its services like Yandex Music in compliance with local legislation, such as websites listed by Roskomnadzr, or due to violation of the platform rules.

In accordance with the December 2024 amendment to the Law on Advertisement, the owners of websites that place advertisements should dedicate 5 percent of all annual advertisements to "social advertisement."[139] The law defines such advertisements as those aimed at "charity or other socially valuable goals, as well as ensuring state interests."[140] Social advertisements are state-procured and managed, but can be posted by physical persons, legal entities, or state and municipal bodies.

The Institute of Internet Development is an organization appointed by the government to distribute the state subsidies to fund "socially valuable internet content."[141] In 2020, the Institute signed a memorandum on social advertisements with both Yandex and VK Group to place social ads on their platforms.[142] According to the institute's report, in 2024, state-funded social advertisements were shown on more than 200 websites with the highest user base on RuNet and were displayed more than 17.9 billion times.[143]

---

[139] Federal Law "On Information, Information Technologies and the Protection of Information," No. 149-FZ, adopted July 27, 2006, as amended, https://www.consultant.ru/document/cons_doc_LAW_58968/f98edd6a9fb0881245dfb14c4d05c1842f907350/ (accessed July 7, 2025).

[140] Federal Law "On Information, Information Technologies and the Protection of Information," No. 149-FZ, adopted July 27, 2006, as amended, https://www.consultant.ru/document/cons_doc_LAW_58968/4f41fe599ce341751e4e34dc50a4b676674c1416/ (accessed July 7, 2025).

[141] Government Order of the Russian Federation No. 1907-r, "On Designating the Autonomous Nonprofit Organization 'Internet Development Institute' as the Operator of Social Advertising," issued July 13, 2021, https://base.garant.ru/401491599/ (accessed July 7, 2025).

[142] "About the operator" ("Об Операторе"), IRI, https://соцреклама.ири.рф/operator (accessed July 7, 2025).

[143] "Placement of Social Advertising on the Internet in 2024 with the Participation of the Operator" ("Размещение социальной рекламы в сети Интернет в 2024 году с участием Оператора"), Institute for Internet Development, https://соцреклама.ири.рф/year-total/2024-totals (accessed July 7, 2025).

At least some of the social advertisements funded by the institute promoted "patriotic upbringing and traditional values," support for Russian soldiers fighting in Russia's war in Ukraine and their families, and support for residents of the newly occupied Ukrainian territories.

According to Yandex's social advertisements report, among the social advertisements Yandex showed were those placed by organizations promoting and supporting the Russian army (for instance, by "Zashitnik Otechestva," and the Association of SVO [the Kremlin's euphemism for Russia's war in Ukraine] Veterans), and promoting the state's agenda, the Russian authorities, and Putin personally (All-Russia People's Front (Narodny Front) and Movement of the First (Dvizheniye Pervykh), both launched by Putin) hundreds of millions times.[144] A Human Rights Watch researcher who opened the page for Yandex's social advertisement report noted that the page displayed a social advertisement by the Ministry of Digital Development urging people to join the army. Advertisements urging people to join the Russian army were shown more than 2 billion times by Yandex in the past two years.[145] In its June 20, 2025 letter to Human Rights Watch, Yandex said it strictly prohibits political advertising.[146]

[144] "Social Advertising Report" ("Отчёт о социальной рекламе"), Yandex, https://yandex.ru/socialads-transparency-report (accessed July 7, 2025).

[145] Ibid.

[146] Written response of Yandex to HRW's letter of inquiry, dated June 20 ,2025.

V. International Standards

Russia's constitution guarantees the right to privacy, including the privacy of communications, as well as freedom of opinion and the right to freely search, receive, transmit, produce, and disseminate information. Russia is also a party to the International Covenant on Civil and Political Rights (ICCPR) and other human rights treaties, which guarantee those rights among others and obligate Russia to respect, protect and fulfil them.

Access to the internet is increasingly recognized as an indispensable enabler of a broad range of human rights guaranteed in those instruments. According to the former United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, the internet is "a key means by which individuals can exercise their right to freedom of opinion and expression."[147]

International law allows for certain restrictions on these rights for specific, legitimate aims such as protection of national security or of public order, health, or morals. Those restrictions, however, should be in line with the criteria of necessity, proportionality, and legal certainty. According to UN Human Rights Committee's General Comment No. 34, these limits should be provided for in law, which is clear and accessible to everyone, and be predictable and transparent. Article 17 of the ICCPR provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and "[e]veryone has the right to the protection of the law against such interference or attacks." The special rapporteur on freedom of expression has interpreted "correspondence" to encompass all forms of communication, both online and offline. In its General Comment No. 16, the Human Rights Committee affirmed that the right to privacy applies to electronic communications, and that communications surveillance should be prohibited.[148]

[147] UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27 (16 May 2011), https://undocs.org/en/A/HRC/17/27.

[148] United Nations Human Rights Committee, General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), adopted 8 April 1988, https://www.refworld.org/docid/453883f922.html.

The European Convention on Human Rights to which Russia was a party until September 16, 2022, provides that limitations imposed on freedom of expression and right to privacy be prescribed by law and "established convincingly" to be necessary in pursuit of a legitimate goal in a democratic society.[149] When limiting these rights to protect legitimate national security objectives, the limitations must be established under clear legal criteria, and the least restrictive means of achieving these objectives.

The recent developments in Russian internet regulations and policies are inconsistent with Russia's international law obligations and violate the human rights of internet users in Russia.

Internet Censorship

As a party to the ICCPR, Russia has an obligation to refrain from non-permissible interference with the rights to expression and information, to protect freedom of expression and information from harm including by private persons and entities, and to facilitate their exercise.

Arbitrary blockings of websites and filtering of content online in Russia, including by technology companies in response to orders from the authorities, which is often based on politically motivated grounds (i.e. independent reporting on Russia's war in Ukraine), constitute non-permissible interference with freedom of expression and access to information of internet users in Russia.

In its February 2025 judgment in the case of *Novaya Gazeta and Others v. Russia*, the European Court of Human Rights acknowledged "a systemic and widespread pattern of unjustified restrictions on expression related to the war in Ukraine ... indicating a coordinated effort by the Russian authorities to suppress dissent rather than mitigate

[149] Russia was expelled from the Council of Europe on March 16, 2022 following its full scale invasion of Ukraine, and as a consequence ceased to be a party to the European Convention on Human Rights 2 months later. Articles 8 and 10 of the European Convention on Human Rights protect the right to privacy, including correspondence, and the right to freedom of expression, respectively.

specific security threats."[150] It ruled that such restrictions, including prosecution for content published online and blockings of online media "appeared to be part of a broader campaign to stifle criticism or dissent concerning military actions in Ukraine."[151]

The state use of TSPU equipment that allows for non-transparent internet blockings, does not fulfil the criteria of legal certainty and does not allow for accountability nor judicial or other independent oversight over state censorship.

The blocking of VPNs and other proxies that guarantee user privacy online as well as allow circumvention of state censorship, is condemned by multiple UN human rights institutions as violating the right to privacy, freedom of expression, access to information, right to peaceful assembly, and other rights and freedoms.[152] Blocking such tools that are essential for safeguarding rights online, cannot be justified as they are disproportionate and affect the general population.[153]

Internet Shutdowns

Internet shutdowns in Russia, including the collateral blockings and slowing down access to entire social media platforms, violate the fundamental human rights of internet users in Russia.

The United Nations has repeatedly condemned internet shutdowns and stressed the crucial importance of internet access for exercising fundamental human rights, such as freedom of expression, access to information, freedom of assembly and association.[154]

---

[150] Although Russia ceased to be a party to the European Convention on Human Rights on September 16, 2022, the European Court of Human Rights continued to have jurisdictions over all cases filed with it prior to that date when Russia was still a party. As a matter of international law the judgements of the court in such cases are legal binding on Russia, and would still be relevant were Russia ever to rejoin as a party to the convention.

[151] See Application Nos. 11884/22 and 161 others, judgement of February 11, 2025 which became final on May 11, 2025, available at https://hudoc.echr.coe.int/?i=001-241738

[152] Guide to International Law and Surveillance, Version 4.0, Privacy International, March 2024, https://privacyinternational.org/sites/default/files/2024-09/2024%20GILS%20version%204.0.pdf (accessed July 7, 2025).

[153] Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/51/17 (4 August 2022), https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age (accessed July 7, 2025).

[154] UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc. A/HRC/41/41 (17 May 2019), para. 21, https://undocs.org/A/HRC/41/41 (accessed July 7, 2025).

Internet shutdowns also interfere with economic, social and cultural rights, as well as health and life of everyone who is denied access to the internet.[155] For instance, as noted in the report, during blockings in Russia, users could not use online banking, taxi services, state services website, and other key sites and services online.

The UN human rights institutions and experts, as well as regional experts agree that shutting down the internet "can never be justified, including on public order or national security grounds."[156] Such measures are "generally disproportionate," because "even if they are premised on national security or public order, they tend to block the communications of often millions of individuals."[157] While the specific context of temporarily suspending mobile internet access as a means to interrupt a potential drone, or similar, attack has not been explicitly addressed by these bodies, such a measure is clearly an interference in the exercise of many rights and has to be strictly justified. This means the state has to demonstrate that it is an effective means of disrupting a potential armed attack, that the collateral harm to other rights of such a measure is proportionate given the goal of disrupting an armed attack, and that other effective measures, which cause less interference with rights, are not available.

The generic blocking and filtering of services violate international human rights law.[158] In its General Comment No. 34 on the right to freedom of expression, the UN Human Rights Committee indicated that permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with ICCPR article 19(3).[159]

---

[155] UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/44/49 (23 April 2020), para. 24, https://undocs.org/A/HRC/44/49 (accessed July 7, 2025).

[156] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression, and ACHPR Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet (1 June 2011), para. 6(b), https://www.osce.org/files/f/documents/e/9/78309.pdf (accessed July 7, 2025).

[157] UN General Assembly, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/71/373 (6 September 2016), para. 22, https://undocs.org/en/A/71/373 (accessed July 7, 2025).

[158] UN General Assembly, Road Map for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation, UN Doc. A/74/821 (29 May 2020), para. 41, https://undocs.org/A/74/821 (accessed July 7, 2025).

[159] United Nations Human Rights Committee, General Comment No. 34: Article 19 – Freedoms of Opinion and Expression, UN Doc. CCPR/C/GC/34 (12 September 2011), https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed July 7, 2025).

In Russia, internet shutdowns lack legality as they are not envisaged by law, predictability, as they are not announced by the state, and proportionality, as they affect millions of internet users.

Mass Surveillance

By meddling with internet infrastructure and introducing TSPU equipment, national DNS, TLS certificates and other tools for state interception of internet traffic, the Russian authorities have further expanded mass surveillance in violation of the right to privacy.

These highly intrusive policies are inconsistent with the principles of legality, necessity, and proportionality, and constitute a violation of Russia's obligations under international human rights law as they are neither clear nor precise, but instead are discriminatory and arbitrary in nature.[160] The laws regulating state interference with the internet lack clarity, are broad in scope, and often envisage no effective oversight body or ways to challenge the human rights implications caused by these measures.[161]

As the European Court of Human Rights has found, the legislation "providing for the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications" is not necessary in a democratic society and "impairs the very essence of the right to respect for private life".[162]

Human Rights Responsibility of Tech Companies

All companies have a responsibility to respect human rights and remedy abuses as articulated in the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises.[163] The UN Guiding Principles call on companies to

[160] UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017).

[161] European Court of Human Rights, Podchasov v. Russia, App. No. 33696/19, Judgment (Merits and Just Satisfaction), 13 February 2024, https://hudoc.echr.coe.int/eng?i=001-230854 (accessed July 7, 2025).

[162] Ibid, para. 80.

[163] OECD, Responsible Business Conduct and Human Rights, https://mneguidelines.oecd.org/Responsible-business-conduct-and-human-rights.pdf (accessed July 7, 2025).

prevent and mitigate human rights risks and remedy harms that they cause or contribute from their practices or operations, including the company's actions and omissions. Actions that companies take should be in line with international human rights standards, conducted in a transparent and accountable way, and enforced in a consistent manner. This applies to both Russian technology companies and foreign technology companies that provide services to users in Russia.

Recommendations

To Russian Authorities

- End all censorship of internationally protected expression on the internet, including independent media, and ensure any restriction of online expression is lawful, necessary, proportionate, and limited in scope.
- End all persecution and harassment of individuals using the internet for peaceful political and other expression.
- Publish information about websites that are blocked outside the official blocked list and acknowledge the state interference with access to foreign websites.
- Disclose full information about the software, hardware, technical specifications, and capabilities of tools used by the authorities to censor and manipulate internet traffic.
- End blockings of VPNs and other proxies that protect users' identity and facilitate access to information on the internet; abolish legislation that prohibits spreading information about such tools.
- End broad, indiscriminate, and indefinite internet shutdowns, including restriction of specific messengers, social media platforms, and internet access in the regions.
- Publish orders before any internet suspension is carried out, with details on the legal provision under which the internet was suspended, the reasons for and duration of the shutdown, what services might be affected, and what steps were taken to ensure the suspension is necessary and proportionate.
- Establish a national-level database for all internet shutdowns and blockings in the country, recording all suspensions ordered, the legal provision invoked, the reasons for and duration of the suspension, the decisions of the competent authority, and decisions of an independent oversight body. The database should be available publicly to ensure full transparency and accountability. Ensure that suspension orders can be challenged before an independent body.
- Refrain from imposing measures throughout the internet stack that interfere with the right to freedom of expression and undermine online privacy and security.

- Review the Law on Information and anti-terrorism legislation after consultation with civil society groups, digital rights experts, and other stakeholders to bring the rules in line with international legal standards.
- Rescind the "Sovereign Internet" law amendments that grant authorities the power to control the Russian segment of the internet at their discretion, without any meaningful safeguards, limitations, or remedies to ensure transparency, accountability, and redress.
- Cease putting pressure on or ordering companies to engage in censorship.
- As requests to companies to interfere with access or content or enable any form of surveillance, constitute interferences with freedom of expression and other rights, ensure they can only be made in the exceptional cases foreseen under international norms and are made pursuant to a strict legal basis, following formal written procedures that allow companies to challenge them before an independent adjudication body, and that there are formal, transparent legal procedures for a member of the Russian public to safely and fairly challenge the legality of any government attempt to restrict freedom of expression without fear of reprisal.

To the US, the UK, the EU and Other Foreign Governments and Intergovernmental Organizations

- Ensure that any sanctions and other measures taken against Russia in response to its war in Ukraine do not interfere with access to independent information from within Russia or exacerbate violations of freedom of expression and right to privacy. Separately, provide clear guidance to foreign companies on how to comply with sanctions without violating such rights.
- Provide financial and other support for civil society groups and others working to preserve access to information and developing VPNs and other technological solutions to overcome state censorship and surveillance in Russia.

To Internet Service Providers

- When possible, send prior notification to all subscribers ahead of carrying out an internet suspension order; disclose when internet disruptions are caused by the government.
- Explore all lawful measures to challenge the implementation of internet shutdowns and blockings, especially when the authorities are denying their involvement.
- Collaborate with local and international stakeholders to mitigate harms.

To Russian and Foreign Technology Companies

- Use all legal means to resist demands for censorship. Companies should only comply with such demands if they are made via legally binding, documentable procedures and the company has exhausted all reasonable legal means to resist them.
- Do not proactively censor any material, for instance, by manipulating search results or censoring by terms or website address, unless required by legally binding and written government request.
- Disclose information on how the algorithms are tweaked to accommodate the requirements of censorship laws.
- To the extent legally possible, document all cases in which content has been censored in compliance with legally binding government demands, and law enforcement requests for user information disclosure, and make this information publicly available.
- Incorporate end-to-end and strong encryption into products and services by default wherever possible, and refrain from complying with any demands to weaken security features or build "back doors" into encryption to facilitate abusive surveillance.

To Foreign Technology Companies

- Assess government requests to censor content against international human rights standards and refrain from complying where the underlying law or specific request is inconsistent with those standards.

- Adopt human rights policies outlining how the company will resist government requests for censorship or surveillance, including procedures for narrowing requests that may be disproportionate, or challenge requests not supported by law.
- Look for ways to ensure continuous provision of services in Russia in case of state blocking, including, where possible, by building in censorship circumvention tools.
- Carry out a human rights impact assessment of the decision to leave the Russian market or stop providing services to internet users in Russia and ensure that such decisions are taken strictly in line with international sanctions law and do not constitute overcompliance.
- Engage in regular, meaningful dialogue with Russian and international civil society to inform policy decisions and human rights due diligence.

To Activists, Civil Society Organizations, Charitable Foundations, and Other Groups Concerned With Promoting Global Freedom of Speech Online

- Continue the work on developing VPNs, proxies, and other technologies that maximize privacy, ensure anonymity, and enable internet users around the globe to circumvent internet censorship, filtering, and blocking.
- Conduct independent research and documentation of the ways in which companies are or are not complying with international human rights standards.

Acknowledgments

This report was researched and written by Anastasiia Kruope, assistant Europe and Central Asia division researcher. Etienne Maynier, technologist at the Infosec team, and Aleksandr Lokhmutov, research assistant at Europe and Central Asia division contributed research support.

Tanya Lokshina, associate director for Europe and Central Asia, edited the report. Aisling Reidy, senior legal advisor, provided legal review. Holly Cartner, deputy program director, provided programmatic review.

Specialist reviews were provided by Deborah Brown, deputy director at Tech, Rights and Investigations division, Aruna Kashyap, associate director and Economic Justice and Rights division. Iskra Kirova, advocacy director in the Europe and Central Asia division reviewed the recommendations set forth in the report. Elida Vikic, senior coordinator at the Europe and Central Asia Division, provided editing, and production assistance.

The report was prepared for publication by Travis Carr, publications manager.

Annexes

Annex I Letter from Cloudflare from May 21, 2025, in Response to Human Rights Watch Request

CLOUDFLARE

May 21, 2025

Cloudflare
101 Townsend Street
San Francisco, CA 94107

Dear Mr. Arvind Ganesan,

Thank you for your letter regarding Cloudflare services and potential disruptions in Russia. We appreciate the ongoing work of Human Rights Watch to document Internet blocking efforts and raise awareness of their impact on international human rights.

Cloudflare is a leading connectivity cloud company. We empower organizations to make their employees, applications, and networks faster and more secure everywhere, while reducing complexity and cost. We operate one of the world's largest and most interconnected networks, which allows us to block billions of threats online every day.

Cloudflare's services are accessible in Russia, consistent with applicable United States, United Kingdom, and European Union sanctions laws.[1] Although we have minimal sales and commercial activity in Russia, we believe that an important part of our mission is helping provide more Internet access -- not less. Continuing to provide access to our services not only allows individuals in Russia to more securely connect to the global Internet, but also helps Cloudflare identify and mitigate cyber attacks originating inside the country.

To enable individuals around the world to reach the content on Cloudflare's network as efficiently and securely as possible, Cloudflare interconnects with more than 13,000 networks, including major ISPs. Because users usually connect to the Internet over their own last mile network, however, an individual may experience difficulty connecting to our services for a variety of reasons unrelated to Cloudflare, including technical error, network outages, shutdowns, blocking, or connection tampering. Typically, government-directed blocking is carried out by local Internet Service Providers (ISP). ISPs may use a variety of techniques to block content, including blocking Cloudflare IP addresses, which prevents their users from accessing Cloudflare's network.[2] However, Cloudflare servers, like other server-side devices, are generally unable to identify or confirm such attempts to block without notice or additional evidence.

[1] Prince, Matthew.,'Steps we've taken around Cloudflare services in Ukraine, Belarus, and Russia," March 2022.
[2] Starzak, Alissa., Fayed, Marwan., "The unintended consequences of blocking IP addresses," December 2022.

Cloudflare has no direct knowledge of how Russian authorities block access to websites or services, but public research suggests it is decentralized in function and centralized in control.[3] Cloudflare is aware of media reports related to the blocking of parts of our network in Russia, although our research suggests it may have been more limited in scope and duration than publicly reported. Cloudflare has not received any notice from Russian ISPs or any other Russian entity regarding the reported disruptions.

Cloudflare is also aware of reports originating about five years ago that the Russian government was seeking to ban the use of certain secure protocols.[4] Most recently, the media has reported efforts to block access to websites with Encrypted Client Hello (ECH) enabled. ECH is a protocol designed to improve the privacy and security of users' Internet requests. ECH encrypts the Transport Layer Security (TLS) handshake, including the Server Name Indicator (SNI), which is currently transmitted in plain text and may allow a third-party to track a user's behavior online. In 2024, Cloudflare enabled ECH for free and by default for millions of customers using our free services. Although we are aware of reports related to ECH blocking in Russia, and we have observed signals consistent with tampering at various points in time, it can be challenging for a service provider like Cloudflare to confirm intentional blocking of a specific protocol. We would note that external parties have collected information about Russia's blocking of ECH in a GitHub repository.[5]

Cloudflare publishes comprehensive, anonymized data regarding Internet traffic, outage, cyberattack, and connection tampering trends through Cloudflare Radar. As described in more detail in a Cloudflare blog on global third-party tampering, connection tampering information is contained within the TCP resets and timeouts data that we release on Cloudflare Radar.[6] Efforts to directly block ECH would most likely be reflected in the data in increases in TCP connections terminated at the Post ACK (where the middlebox almost assuredly sees the SNI data packet sent by the client, but dropped them so they do not reach the server) or Post PSH (where Cloudflare sees the SNI, which means the middlebox has, too) stage. The data on Cloudflare Radar is sortable by country, and by a network's Autonomous System Number. Radar provides a limited historical record, which may help corroborate Human Right Watch's other research regarding unexpected drops in Internet traffic from Russia.

---

[3] Xue, Diwen., et. al., "TSPU: Russia's decentralized censorship system," ACM Internet Measurement Conference, October 2022, doi:10.1145/3517745.3561461

[4] Cimpanu, Catalin., "Russia wants to ban the use of secure protocols like TLS 1.3, DoH, DoT, ESNI," ZDNET, September 2022, available at: https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/

[5] Available at https://github.com/net4people/bbs/issues/417.

[6] See also, Valenta, Luke.,"Bringing insights into TCP resets and timeouts to Cloudflare Radar," September 2024.

Cloudflare also provides detailed information regarding our interactions with governments and law enforcement agencies in our Transparency Report and our ongoing participation in the Global Network Initiative (GNI). We maintain an up-to-date list of actions we have never taken on our network, called Warrant Canaries. Cloudflare has never had a corporate entity, an office, or employees in Russia, we are not registered in the country, and we have never blocked websites in Russia at the Russian government's request. As detailed in our Transparency Report, when we receive legal requests from non-U.S. governments, we generally ask them to route the requests to the U.S. government pursuant to a Mutual Legal Assistance Treaty (MLAT). We have received no MLATs originating from the Russian government in recent years. However, any such request we might receive would be processed consistent with our general approach to law enforcement: due process, respect privacy, and provide notice, as well as the GNI Principles.

Thank you again for your attention to these issues. Please let us know if we can be of further assistance in your research.

Sincerely,

Alissa Starzak
VP, Deputy Chief Legal Officer and Global Head of Public Policy
Cloudflare

101 Townsend Street, San Francisco, California 94107 | cloudflare.com | +1 (888) 99 FLARE

Annex II – Letter from Yandex from June 20, 2025, in Response to Human Rights Watch Request

Human Rights Watch – Yandex response

Russian TLS Certificate Authority

Since spring 2022, Russian authorities have been promoting the use of state-issued transport layer security (TLS) certificates, such as the one issued by the Ministry of Digital Development's National Certifying Center acting as a certifying authority.

According to our findings, a state-issued TLS certificate presents a risk of enabling man-in-the-middle attacks, allowing traffic interception and decryption between communicating parties without their knowledge.

Questions:

1. Does Yandex browser software list the Ministry of Digital Development's TLS certificate or any other TLS certificates issued by the Russian authorities as a trusted certificate?
2. Are users notified when these are added to the list of trusted certificates? If so, can users decline?
3. Has Yandex verified that the state TLS certificates in fact guarantee safety from man-in-the-middle and other attacks? If so, how? Can Yandex share the assessment with Human Rights Watch?
4. Has Yandex promoted or pre-installed state TLS certificates to users of its services on any of its platforms?

Answer:

Yandex apps and services do not add any third-party root certificates, including ones issued by the National Certification Authority, to a system's trusted root store.

Yandex Browser recognises National Certification Authority certificates for domains included in the Certificate Transparency public log. The log allows both users and browsers to verify the authenticity of domain certificates. Certificate Transparency is an IETF Internet

standard developed specifically to prevent a man-in-the-middle attack, with implementations across the web browser industry.

Yandex had publicised its efforts to support secure connections to domains using National Certification Authority certificates while maintaining public auditability. Yandex Browser's Certificate Transparency policy is available on the browser's help page available here: https://browser.yandex.ru/help/en/security/policy-ct-log

RuNet Isolation Drills and Collateral Blockings

According to our findings, since December 2019, the Russian authorities carried out at least seven "drills" to test the RuNet's "resilience" in case of "unwanted external interference" by "unfriendly countries." During such drills, internet users in Russia reported difficulties with internet access, as they have when the state has blocked websites and online services.

For instance, in December 2024, users in Dagestan, Chechnya, and Ingushetia reported being unable to access foreign websites, apps, and messengers such as Telegram, YouTube, and Google. Also, most VPNs did not work. Some users were unable to order taxis via the Yandex Taxi app.

Questions:

5. Has Yandex recorded disruptions in the functioning of its services during state "drills" or other instances of state blockings? If so, can Yandex share this data with Human Rights Watch (i.e., what kind of services were affected, when, for how long, and why)?
6. Has Yandex received complaints from its users of such disruptions? If so, can Yandex share data about the number of such complaints it has received since January 2022?

Answer:

Yandex services are designed to maintain maximum possible availability under all network conditions. However, like all internet-dependent platforms, our services may be indirectly affected by broader network infrastructure disruptions outside our control.

Information on Data Sharing with State Agencies

Most Yandex services are listed as information dissemination organizers under Russian law and are thus obliged to store and pass on their users' data to law enforcement upon demand.

Questions:

7. With regard to user data that Yandex disclosed to Russian authorities after January 2022, can you share:

a. the number of government requests for user data or other surveillance assistance (e.g., interceptions) Yandex received

b. the number of accounts affected by such requests

c. the number of requests Yandex complied with, in whole or in part

Answer:

As reflected in our publicly available Transparency Report (https://yandex.ru/company/privacy/transparencyreport), Yandex maintains clear disclosure practices while complying with applicable laws. At Yandex, we handle all government requests for user data with strict adherence to both the law and our principles of user protection. We implement a multi-layered review process that:

1. Absolutely prohibits any form of backdoor access to our systems, ensuring all data disclosures occur through documented processes as obliged by the federal law

2. Rigorously assesses each request for legal validity, examining the basis, scope, and necessity of the demand. We only consider those requests that have been submitted in accordance with all formal law requirements. All requests are checked carefully to ensure their legitimacy. Yandex only provides the amount of information that is strictly required in order to fulfil the request.

3. Actively challenges overbroad and insufficient demands through legal channels. In H2 2024 Yandex received 41 439 requests and declined 13 384 requests (32% declined). Any requests that fail to comply with all relevant procedural and legal

requirements are turned down. Yandex does not provide responses to requests that do not comply with such requirements.

4. Maintains transparency through our biannual Transparency Report, which provides granular statistics about request volumes.

For complete information including year-to-year comparisons and detailed breakdowns by services, we invite you to review the Government Requests section of our latest Transparency Report available at https://yandex.ru/company/privacy/transparencyreport This disclosure reflects our commitment to transparency and is conducted entirely at our own initiative.

d. the type of information requested and disclosed, from which government agencies, and under which articles of the criminal code.

Answer:

Government agencies can legally request certain data and information about Yandex users. Several laws, such as "On Police", "On Operational and Investigative Activities", "Criminal Procedure Code" and others, clearly define the grounds for requesting data, as well as the types of data that can be requested and deadlines for responses. Failure to provide information in response to a legitimate request, which has been officially submitted and received, may result in penalties, and in some cases, the suspension of the company's activities and criminal liability for the CEO. Government agencies are not required to specify the relevant Articles of the Criminal Code in their requests.

Content Moderation and Censorship

According to Yandex's transparency report, the Yandex search engine automatically deletes from its search results links to websites listed by the authorities as banned. For instance, following law enforcement's request, Yandex Music deleted thousands of music tracks because they allegedly contained "fake information about the Russian army" or LGBT-friendly content. Yandex Music also labeled the music of "foreign agents," in compliance with the labeling requirement under the "foreign agents" law, which the United Nations Human Rights Committee has urged the Russian government to repeal due to its unjustifiable restrictions on freedom of association.

Independent internet censorship researchers documented Yandex browser algorithms to have a reference and source bias as they forward users to fewer websites that regularly featured criticism of Russia's leadership.

Questions:

8. Has Yandex received requests from the authorities to adjust search results in its search engine other than deleting links to the list of state-banned websites? If so, what type of changes the authorities requested? Has Yandex complied?
9. Has Yandex changed its browser search results in any ways that filter information that is not directly listed by the authorities as banned? Are there keywords that the browser filters out from search results, and if so, what are they?
10. Has Yandex received requests or demands by the authorities to moderate its content in any other ways, apart from deleting or filtering content across its platforms? Has Yandex, for example, received a request or demand by the authorities to downrank content in search results?
11. Has Yandex taken steps to proactively moderate, label, or filter out content across its platforms, seeking to comply with Russia's legislation on internet censorship which were not at a direct request from the authorities? If so, what were those steps?
12. Has Yandex ever challenged or appealed any requests from the authorities to adjust search results or to moderate its content in other ways? If so, could you please provide details of to whom the challenge or appeal was made and the outcome?

Answer:

The fundamental principle of Yandex Search is to provide users with comprehensive, useful, and relevant information in an impartial manner, presented in a format that enables them to conveniently and efficiently accomplish their tasks. Like all search engines, Yandex indexes all content available on the internet.

Search results are generated exclusively through machine learning algorithms, ensuring unbiased ranking and presentation of information. The ordering of search results cannot be manually altered.

To identify the most appropriate web pages, Yandex Search automatically analyzes multiple factors including: the search query itself, page content quality, user interaction history with specific pages, interconnections between various web pages, language preferences, geographical location, and numerous other ranking signals. The performance of our machine learning ranking algorithms is continuously monitored through automatically calculated metrics.

All modifications to the ranking system are implemented exclusively through algorithmic updates, completely eliminating any possibility of manual interference.

Yandex strictly adheres to local legislation and removes links from search results when legally required to do so. In compliance with Russian regulations, Yandex — like all search engines operating in Russia — is legally obligated to remove from search results any websites included in Roskomnadzor's registry of prohibited sites. The service is also required to delist links in accordance with the "Right to Be Forgotten" law when information is found to be unlawful, outdated, or inaccurate — such actions are only taken upon submission of proper supporting documentation (such as court rulings). The company regularly publishes statistics regarding the processing of such requests in its Transparency Report available here: https://yandex.ru/company/privacy/transparencyreport

As for Yandex Music, the streaming service must comply with the legislation that applies in any country where Yandex Music operates. So, when the service receives an official request from the state authorities of the, e.g., Russian Federation that demands to remove some content, in accordance with Federal Law Yandex Music is obliged to meet the demand, but only if all the procedures required by the law are followed. We voluntarily disclose the statistics on removals requested by government authorities in our Transparency report every six months.

There are also public platform rules in Yandex Music that help to provide a safe environment for our users within the service. We use a hybrid model to determine potential violations, employing both ML models and manual review by the content moderation team alongside a committee of impartial linguistics experts. They consider the genre, the artist's right of self-expression, and the context. If content violates the platform rules, various actions can be taken. Depending on the severity of the violation, the content may be marked with special signs indicating an age restriction, excluded from recommendations, or removed from the service.

Social Advertisement

We are seeking to understand what proportion of social advertisement on Yandex's platforms is comprised of messaging to promote several sets of state interests. We understand that in accordance with December 2024 amendment into the Law on Advertisement FZ N38, the owners of websites that place advertisements should dedicate 5 percent of all annual advertisements to "social advertisement." The law defines such advertisements as aiming at "charity or other socially valuable goals, as well as ensuring state interests." We understand social advertisements to be state-procured and managed and can be placed by physical persons, legal entities, or state and municipal bodies.

According to Yandex's 2024 annual social advertisements report, among the social advertisements Yandex showed were those placed by organizations promoting and supporting the Russian army (for instance, by "Zashitnik Otechestva," and Association of SVO Veterans), and promoting state interests, the Russian authorities and Putin personally (Narodny Front, Dvizheniye pervykh) hundreds of millions of times.

Questions:

13. Can Yandex provide a breakdown of social advertisements placed by the Russian authorities and state-affiliated entities, including the content, the number of times they were displayed to users across its platforms, and cost of such advertisements?
14. Does Yandex have a say over which social advertisements are displayed as per the FZ N38 requirements?

Answer:

Since 2021, Russia's advertising legislation requires Yandex — like other major digital platforms in the country — to allocate mandated space for social advertising.

The majority of these social ads promote domestic tourism, museum initiatives, and urban development projects. A significant portion also features foundations supporting people with disabilities and chronic illnesses, orphaned children, and environmental causes.

Every social ad in our system carries a special badge linking to our transparency report at https://yandex.ru/socialads-transparency-report

Our platform strictly prohibits political advertising content in any countries of operation. This includes any materials referencing politicians, political parties, candidates, electoral associations, public figures, or containing commentary (whether critical or supportive) about such entities.

Question:

15. We understand that Yandex also places social advertisements as a part of its own "Help is Near" (Помощь рядом) grants for social advertising campaign. What proportion of such advertisements are run by state and state-affiliated entities, and what is the content of these in state or state-affiliated advertisements?

Answer:

The Help Nearby Foundation offers grants for social advertising exclusively to non-profit organizations that have undergone strict verification. To qualify, an NGO must have been active for at least one year and demonstrate transparent financial reporting. Government agencies, political parties, and commercial entities are explicitly excluded from eligibility. Currently, the foundation works with 671 verified nonprofits, all meeting the criteria detailed here: https://yandex.ru/legal/ngo_verification/.
Last year, 402 nonprofits — spanning causes like disability support, orphan care and animal welfare — received funding to run social ads, helping them raise awareness, attract volunteers, and increase donations.

All grant-funded social advertising must promote systemic charity work, whether by spotlighting social issues, sharing solutions, guiding people to assistance, or showcasing related projects. The primary focus of these advertisements revolves around the core activities of charitable foundations and non-profits in order to promote systematic charity work — particularly initiatives related to illnesses and disabilities, orphan care, and environmental causes.

Corporate Structure

We cannot find detailed publicly available information on Yandex's official sources on Yandex's shareholders and ownership structure.

Question:

16. Can you please provide information about the shareholders of Yandex?

Answer:

Yandex is privately owned company and listed on Moscow exchange. Yandex's principal shareholders include management team and other financial private investors. Free-float is 17,2%. The detailed shareholder structure as of January 31, 2025 is available here: https://ir.yandex/shareholder-structure

“Disrupted, Throttled, and Blocked”

State Censorship, Control, and Increasing Isolation of Internet Users in Russia

The Russian authorities have been meticulously building a “sovereign internet”, aiming to turn Russia’s section of the internet into a state controlled and isolated forum, subject to non-transparent state censorship and manipulation of internet traffic without independent oversight or accountability.

In today’s Russia, internet users are cut off from independent media outlets, human rights organizations’ websites, opposition politicians’ web pages, and foreign social media platforms because authorities have blocked access to those sites for not complying with the country’s draconian laws on internet regulation. Russia’s authorities are also increasingly blocking use of censorship circumvention tools that many users utilize to overcome denial of access to sites.

Internet shutdowns around peaceful protests, elections, or other political events have become the new norm, along with occasional and unpredictable internet disruptions attributed to the authorities’ experiments with internet censorship technology.

Russian authorities also increasingly pressure foreign tech companies such as Apple, Google, and Mozilla, to remove censorship circumvention tools, independent media applications, and other resources that the government considers subversive, threatening to fine and/or block companies that do not comply. Simultaneously, a growing number of users are forced to switch to Russian browsers and social media that direct users to state approved interpretations of current and historic events and pose high risks that users’ personal data will be passed on to the law enforcement.

“Disrupted, Throttled, and Blocked” documents the technological aspect of state censorship, which is largely invisible to the majority of the Russia’s internet users, and shows the serious risks they carry for users’ rights and freedoms. Human Rights Watch calls on Russia to end all censorship of internationally protected expression on the internet. It also urges Russian and foreign technology companies to resist the state pressure to censor content and disclose user data in violation of international law using all available legal means and technological solutions.