FORUM 18 NEWS SERVICE, Oslo, Norway
https://www.forum18.org/
The right to believe, to worship and witness
The right to change one's belief or religion
The right to join together and express one's belief

3 October 2024

RUSSIA: Internet censorship and freedom of religion or belief

By Victoria Arnold, Forum 18 (https://www.forum18.org)

Ever-increasing internet censorship has seen religious websites and materials blocked for: "extremist" content; opposition to Russia's war against Ukraine from a religious perspective; material supporting LGBT+ people in religious communities; Ukraine-based religious websites; social media of prosecuted individuals; and news and NGO sites which include coverage of freedom of religion or belief violations. This also denies local people freedom of expression and the opportunity freely to seek information and views on religious issues. It also has a chilling effect on those considering publishing their views on issues related to religion which the regime dislikes.

Russia's ever-increasing internet censorship continues to affect the exercise of freedom of religion or belief in the country. The censorship denies local people freedom of expression in various matters related to religion and the opportunity freely to seek information and views on religious issues. It also has a chilling effect on those considering publishing their views on issues related to religion which the regime dislikes.

Communications regulator Roskomnadzor blocks access to websites, demands that even foreign sites remove information deemed to threaten state security or public order in Russia, monitors (with the security services) the use of social media, and is exploring the use of artificial intelligence to make all these processes more efficient (see below).

Websites may be blocked specifically for their religious content (https://www.forum18.org/archive.php?article_id=2935), if this is associated with material or religious organisations which courts have already outlawed as "extremist", as in the case of Jehovah's Witnesses' sites and even Wikipedia pages about them. This also includes material supporting LGBT+ people in religious communities.

The majority of religious sites, however, have become subject to "military" censorship since Russia's full-scale invasion of Ukraine in February 2022, with any opposition to the war being taken as grounds for preventing access (https://www.forum18.org/archive.php?article_id=2935). Similarly, several individuals who have been prosecuted for protesting against the war in religious terms or from a religious perspective have found their social media profiles blocked by order of Roskomnadzor.

Roskomnadzor has also blocked a large number of websites of media outlets, civil society organisations, and human rights groups (https://www.forum18.org/archive.php?article_id=2935) which have reported on violations of freedom of religion or belief. While their coverage of such issues is not typically the reason for the blocking, restricting access to their work on freedom of religion or belief further reduces the space for discussion of the topic inside Russia.

Internet users in parts of Ukraine Russia has illegally occupied face the same Roskomnadzor blocking that users face within Russia's internationally recognised boundaries.

Beyond their immediate impact, the concrete measures state agencies take to restrict access to online information also has a chilling effect on freedom of expression in general, with Freedom House noting in its 2023 report on Russia an increase in self-censorship when writing about "controversial" topics (see below).

While there is no explicit ban on sharing links to or quoting material from blocked websites, doing so may still incur penalties, depending on the reason a site was blocked. If a publication or internet user quotes from the blocked site of an "undesirable organisation", they may be prosecuted for "participation in the activities of an undesirable organisation". Linking to a site belonging to an "extremist organisation", or citing its materials, could lead to administrative or even criminal prosecution under the Extremism Law (see below).

The majority of religious websites now inaccessible in Russia (without a VPN) appear to have been blocked "openly" – that is, Roskomnadzor has added them to the publicly searchable registry of sites which Russian internet providers are obliged to prevent their customers from seeing (see below).

A few, however, are not in the registry, yet still appear to be inaccessible to some or all internet users inside Russia. It is unclear why this might be – it is possible that such sites have fallen victim to the filtering of internet traffic through Roskomnadzor's "technical means of countering threats" (TSPUs – see below), that smaller, local internet providers may be blocking access or having technical problems, or in the case of sites hosted abroad, the websites' servers may be blocking access requests from Russia (see below).

Forum 18 wrote to Roskomnadzor and its subsidiary, the Main Radio Frequency Centre, on 25 September, to ask:

- why sites are blocked for the expression of religious opinions, including on war in general or the war in Ukraine;

- why sites are being blocked without being added to the publicly searchable registry;

- for clarification of technical details of blocking.

Roskomnadzor Press Service's response of 26 September did not answer Forum 18's questions and asked which sites Forum 18 was referring to.

Self-censorship to try to avoid possible prosecution

On 4 March 2022, specific Criminal Code and Administrative Code penalties for "discrediting" the Russian Armed Forces (https://www.forum18.org/archive.php?article_id=2897) came into force, alongside Criminal Code penalties for spreading "false information" about the Armed Forces' actions. Some of the criminal penalties were increased on 28 March 2023 (https://www.forum18.org/archive.php?article_id=2897). If individuals commit an offence covered by Administrative Code Article 20.3.3 ("Public actions aimed at discrediting the use of the Armed Forces of the Russian Federation") more than once in a year, they may be prosecuted under Criminal Code Article 280.3.3, they may be prosecuted under Criminal Code Article 280.3 ("Public actions aimed at discrediting the use of the Armed Forces of the Russian Federation in order to protect the interests of the Russian Federation and its citizens, [and] maintain international peace and security").

Alongside blocking of websites and online materials, these Administrative and Criminal articles have led to individuals such as Christian preacher Eduard Charov being prosecuted and fined for what they post online (https://www.forum18.org/archive.php?article_id=2925). He is currently banned from leaving his home district and using the telephone or internet, and is also awaiting criminal trial on charges of repeatedly "discrediting" the Russian armed forces and state bodies. "Most likely, it will all end with a prison term for me," Charov noted.

In March 2023, a court fined 87-year-old Archbishop Viktor Pivovarov of a small independent Orthodox community one month's average local wage or more than two months' average local pension (https://www.forum18.org/archive.php?article_id=2822) under Administrative Code Article 20.3.3, Part 1 (https://www.forum18.org/archive.php?article_id=2897) ("Public actions aimed at discrediting the use of the Armed Forces of the Russian Federation") for an anti-war sermon he had given in church.

Subsequently, the Archbishop continued to openly oppose Russia's war in Ukraine in his articles, his sermons (many of which are available on his YouTube channel), and in a video made by independent Russian media outlet Novaya Gazeta Europe (which Roskomnadzor has also blocked). In April 2024, under Criminal Code Article 280.3, Part 1 (https://www.forum18.org/archive.php?article_id=2897), Archbishop Pivovarov was fined nearly eight times the local average monthly pension for allegedly "discrediting" the Russian Armed Force by condemning Russia's invasion of Ukraine (https://www.forum18.org/archive.php?article_id=2904) and the conduct of the war in his sermons, articles and video interviews posted online.

On 30 March 2023, a Moscow court jailed 63-year-old Orthodox Christian Mikhail Simonov for 7 years for disseminating "false information" about the Russian armed forces on the basis of "political hatred". He had made two short social media posts condemning Russia's war against Ukraine (https://www.forum18.org/archive.php?article_id=2822), including: "We, Russia, have become godless. Forgive us, Lord!"

Such cases have led individuals to self-censor and to remove material from the internet to try to avoid possible prosecution.

Portal Credo, a religious news website, went offline of its own accord after receiving a warning from Roskomnadzor (https://www.forum18.org/archive.php?article_id=2763) on 22 March 2022, apparently for its coverage of the war in Ukraine. "It remains unclear how it is technically possible to bring the content of the Portal in line with the requirements of [the law on disseminating 'false information']," editor Aleksandr Soldatov wrote on Facebook on 23 March 2022.

After being denounced by a reader and fined under Administrative Code Article 20.3.3 (https://www.forum18.org/archive.php?article_id=2897), Part 1 for "discrediting" the Russian Armed Forces, Orthodox commentator and former deacon Andrey Kurayev deleted all posts on his LiveJournal blog (https://www.forum18.org/archive.php?article_id=2787) dating from 23 February to 1 April 2022, "to make it difficult for future informers to do their noble work".

Similarly, Fr Nikandr Pinchuk (the first person to receive a criminal conviction – in his case a large fine - for opposing the war in Ukraine on religious grounds) deleted his profile on the VKontakte social media site (https://www.forum18.org/archive.php?article_id=2783) after learning of his initial (administrative) prosecution for calling the Russian army "the horde of the Antichrist".

Baptist preacher Sergey Stepanov deleted his VKontakte profile "immediately after the 'law' persecuting people for anti-war statements came into force", he told a local news website on 30 April 2022, "because I have a firm anti-war position, which I do not hesitate to express openly". He was nevertheless still prosecuted and fined (https://www.forum18.org/archive.php?article_id=2738) under Administrative Article 20.3.3 (https://www.forum18.org/archive.php?article_id=2897), Part 1 for anti-war statements he had made on the page before 4 March 2022, when the law was adopted.

Sharing blocked material could risk prosecution

While there is no explicit ban on sharing links to or quoting material from blocked websites, doing so may still incur penalties, depending on the reason a site was blocked in the first place, the Centre for the Protection of Media Rights warned in its blog on 5 September 2023 (https://mmdc.ru/blog/2023/09/05/mozhno-li-stavit-giperssylki-na-zablokirovannye-sajty/).

If a publication or internet user quotes from the blocked site of an "undesirable organisation" (https://www.forum18.org/archive.php?article_id=2707), for example, they may be prosecuted for "participation in the activities of an undesirable organisation" (Administrative Code Article 20.33). Linking to a site belonging to an "extremist organisation", or citing its materials, could lead to administrative or even criminal prosecution under the Extremism Law.

Long history of internet censorship

According to Freedom House's 2023 Freedom on the Net report (https://freedomhouse.org/country/russia/freedom-net/2023), Russia scores badly on: blocking and filtering internet content, "particularly material that is protected by international human rights standards"; using "legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards"; and "restrictions on the internet and digital content [which] lack transparency, proportionality to the stated aims, or an independent appeals process".

Religious material which does not violate the human rights of others has been routinely blocked over the last ten years, and added to Roskomnadzor's registry of blocked sites alongside violent terrorist and extremist content, child pornography, and information on illegal narcotics production.

Blocking accelerated after the beginning of Russia's full-scale invasion of Ukraine. Between February 2022 and August 2024, Roskomnadzor blocked over 20,000 websites and webpages (https://roskomsvoboda.org/ru/post/20000-saytov-pod-voennoy-cenzuroy/) for disseminating "false information" about the Russian Armed Forces. These include the sites of religious organisations and news outlets and the social media profiles of individual believers who have opposed Russia's war in Ukraine on religious grounds.

Laws on prohibited internet content have become ever more restrictive in recent years, and Roskomnadzor's blocking efficiency appears to be increasing (see below).

"Now the authorities block according to 'black lists', that is, everything is allowed except what is prohibited. But I see preparations for transition to a 'white list', when everything is prohibited except what is permitted", Mikhail Klimarev of the Society for the Defence of the Internet commented to the independent media project Okno on 15 March 2024 (https://okno.group/blokirovki-runet/).

"Over 10 years of censorship, Roskomnadzor has blocked millions of websites and individual materials. In the first half of 2023 alone, the agency restricted access to 885 thousand websites", Klimarev observed. "Previously, it seemed that [Roskomnadzor] would only hunt for opposition media. But in 2024, they are coming for everyone".

Who blocks websites and webpages?

The Federal Service for Supervision of Communications, Information Technologies, and Mass Media (Roskomnadzor) is the Russian government agency with primary responsibility for monitoring the Russian internet and online communications (as well as offline media). It initiates the blocking of websites and specific webpages according to its own decisions, court rulings, and requests from certain other government bodies.

The General Prosecutor's Office, the Interior Ministry, the Federal Service for Oversight of Consumer Protection and Welfare (Rospotrebnadzor), The Federal Service for Oversight in Healthcare (Roszdravnadzor), Federal Service for Veterinary and Phytosanitary Oversight, the Federal Drug Control Service (before this was subsumed into the Interior Ministry), the Ministry of Digital Development, the Federal Service for Alcohol Market Regulation, the Federal Tax Service, and the Federal Agency for

Youth Affairs (Rosmolodezh) are entitled to demand the blocking of particular categories of online material without any court order.

For example, on the basis of 2014 amendments to the Federal Law on Information, Information Technologies and the Protection of Information, the General Prosecutor's Office can demand the blocking of websites which contain "calls for mass disorder, extremist activities, incitement of interethnic and/or interfaith hatred, participation in terrorist activities".

Regional courts consider blocking requests from other state agencies and lower-level prosecutor's offices. Private individuals can also submit online requests for Roskomnadzor to consider particular websites for blocking.

The Federal Security Service (FSB), meanwhile, has the right to make blocking demands directly to domain registrars, thus bypassing both the courts and Roskomnadzor.

Roskomnadzor maintains the "Unified Registry of Domain Names, URLs, and Network Addresses which allow the identification of information banned from distribution in the Russian Federation", to which it adds the sites and webpages government agencies and courts have decided should be blocked. Russian internet service providers are obliged to monitor the registry and block their customers' access to all these links.

The registry has existed since 2012 but was not initially accessible to the public. Originally, it listed websites blocked for content including child pornography, illegal gambling, suicide methods, and illegal narcotics sales. This has since been expanded – on the basis of various increasingly restrictive laws – to incorporate more and more categories of information deemed to threaten the security and stability of the Russian state.

Most recently, these have included "false information" about the Russian Armed Forces (a broad category which covers virtually anything about Russia's war in Ukraine which contradicts official sources) and "propaganda of non-traditional sexual relations".

It is not possible to view the full registry on Roskomnadzor's website, only to search it for specific domain names or website addresses, which must be precisely entered. Internet freedom monitoring group Roskomsvoboda maintains its own mirror of the registry which permits a broader range of searches.

From November 2022, Roskomnadzor has entered many sites in the registry with the label "State agency not given" ("Gosorgan ne ukazan"). Roskomsvoboda believes these blocks to have been requested by the General Prosecutor's Office, which has since largely disappeared from the registry as a block-requesting agency. Some sites appear in the registry without even the "State agency not given" designation, Forum 18 has observed.

"Concealing the body that makes the decision to block a resource leads to a decrease in transparency", Artyom Kozlyuk, head of Roskomsvboda, noted in comments to Forbes Russia on 5 January 2024 (https://www.forbes.ru/tekhnologii/503386-blok-shema-kak-roskomnadzor-ogranicival-dostup-k-internet-resursam). "There is no one [from whom] to request information about what demands were made on the resource [and] why it was blocked, and it is difficult to challenge the blocking".

In June 2023, the Justice Ministry also began appearing in the registry as an agency requesting blocks on websites, even though nothing in the legislation explicitly allows it to do so without a court order, Freedom House noted in its 2023 Freedom on the Net report on Russia (https://freedomhouse.org/country/russia/freedom-net/2023). So far, this appears to have been confined to blocks on websites associated with so-called "foreign agents".

In addition to internet service providers/telecoms operators, Russian social media and other tech companies must also cooperate with Roskomnadzor. Since February 2021, if a user complains about "prohibited content" (a definition which covers illegal gambling, child pornography, illicit drug sales, etc., but also material deemed to disrespect society or the state), the social network must block this immediately, pending review by Roskomnadzor. Social networks must also block users' profiles if ordered to do so by Roskomnadzor or the General Prosecutor's Office.

A July 2023 report by the University of Toronto's CitizenLab concluded that the number of such orders blocking VKontakte pages had risen by 3,000 per cent since the start of Russia's full-scale war against Ukraine.

Since 2020, VKontakte has also used an algorithm to detect images included in the Justice Ministry's Federal List of Extremist Materials (https://www.forum18.org/archive.php?article_id=2897) and remove them automatically from users' posts, Freedom House noted in its report. The Russian search engine Yandex has also confirmed that it removes links to blocked materials from its search results as soon as they are added to the Unified Registry.

Beyond the concrete actions of Roskomnadzor and other state agencies, it is clear that Russia's adoption of increasingly repressive laws (on extremism, on "foreign agents" and "undesirable organisations", on "discreditation" of and "false information" about the Armed Forces) is leading to a degree of self-censorship, including among religious websites and individual believers. The laws' "vague wording" and "arbitrary enforcement" and the "general ineffectiveness of judicial remedies" also contribute to this, according

to Freedom House (https://freedomhouse.org/country/russia/freedom-net/2023).

Why are websites blocked?

There are "few clear legal criteria" by which courts and government agencies, including Roskomnadzor, decide whether or not internet content is lawful, Freedom House notes in its 2023 report (https://freedomhouse.org/country/russia/freedom-net/2023). These authorities usually give no detailed explanations.

The blocking of websites is largely governed by the Federal Law "On Information, Information Technologies, and Information Protection" (https://www.consultant.ru/document/cons_doc_LAW_61798/). This sets out grounds for restricting access to internet resources. These include the presence of information relating to child pornography, illegal drugs, gambling, illegal alcohol sales, the unlicensed sale of restricted medications, the manufacture of explosives, and the confidential details of victims and witnesses of crime – but also (non-exhaustively):

- "information expressed in an indecent form, which offends human dignity and public morality, [or shows] obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation or bodies exercising state power in the Russian Federation";

- "information containing calls for mass disorder, extremist activities, participation in mass (public) events held in violation of established procedures";

- "false information disseminated under the guise of reliable reports" on the use of the Armed Forces (added in July 2022);

- "information containing an offer to finance the enemy in the context of an armed conflict, military actions, counter-terrorist operations or other actions involving the use of weapons and military equipment in which the Russian Federation is participating, as well as information on possible methods of implementing such financing";

- calls for sanctions against Russia (added in July 2022);

- "information containing a rationale and/or justification for the implementation of extremist activity, including terrorist activity" (added in December 2021);

- information "promoting non-traditional sexual relations and/or preferences" and gender reassignment (these are placed in the same category as paedophilia) (added in December 2022);

- "information that offends human dignity and public morality, expresses obvious disrespect for society, contains images of actions with signs of illegality, including violence, and is disseminated out of hooliganism, selfishness or other base motives";

- informational materials of an "undesirable", extremist, or terrorist organisation (added in December 2021);

- information on the collection of donations in connection with the performance by centralised religious organisations, and by religious organisations included in their structure, of religious rites and ceremonies in violation of the requirements of [the Religion Law];

(Materials in all of these categories may be blocked extrajudicially.)

- an administrative conviction for violating the "foreign agent" law (ie. for failing to label a webpage or blog post with the obligatory "foreign agent" disclaimer);

- a court decision stating that a site contains information banned from distribution in the Russian Federation.

Several of these categories, including court orders (usually for already-banned "extremist" content), information about "extremist" organisations, and most recently, "false information" about the Russian Armed Forces, have been used to block religious materials. The precise grounds for many blocks, however, remain unclear.

Although some "military censorship" blocks (ie. of anything criticising the war, often even if it does not mention the armed forces) are the result of court orders, most are requested by the General Prosecutor's Office, as these do not need to go to court, the Open Observatory of Network Interference (OONI) pointed out in a February 2023 report (https://ooni.org/post/2023-russia-a-year-after-the-conflict/).

OONI also notes that Roskomnadzor blocked more than 6,000 websites in the first nine months following Russia's full-scale invasion of Ukraine in February 2022 on the basis of a single decision taken by the General Prosecutor's Office before the "military censorship" laws were even enacted.

How are websites blocked?

Roskomnadzor's subsidiary, the Main Radio Frequency Centre (Glavniy Radiochastotniy Tsentr, GRChTs), carries out active surveillance of online content for prohibited information – this is increasingly an automated process, and in recent years has begun to incorporate artificial intelligence.

According to leaked documents from Roskomnadzor's Bashkortostan branch, reported on by the New York Times in September 2022 (https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html), the Main Radio Frequency Centre analyses text, images, and video on websites, social media, and messaging services to identify individuals with critical views, track the likelihood of protests, and find material which should be blocked.

Belarusian hacking group Cyberpartisans leaked more Roskomnadzor documents in November 2022 (https://www.rferl.org/a/russia-agency-internet-censorship/32262102.htm), which showed that GRChTs also uses bots to enter closed groups and chats.

In February 2023, GRChTs launched a system called "Oculus", which, Radio Liberty notes, "can allegedly identify information in images or videos that violates Russian law". Also in 2023, Roskomnadzor announced a tender for the integration of Oculus with its various other monitoring systems, Russian news outlet Kommersant reported on 10 April 2024 (https://www.kommersant.ru/doc/6635402). These systems include IS MIR – the "information system for monitoring internet resources" – which identifies and categorises texts containing prohibited information.

Roskomnadzor also intended to start using artificial intelligence in 2024, to improve its analysis of online texts and speed up the identification of prohibited content, Kommersant added. "In 2023, Roskomnadzor detected illegal content on the Internet three hours after publication", Kommersant noted. "In 2024, the figure is planned to be reduced to two hours, and by the end of 2026 - to one".

Russia's security agencies also carry out monitoring of internet activity. To obtain an operating licence, an internet service provider must install equipment which enables this (known as the System for Operational Investigative Measures, Sistema operativno-rozysknykh meropriyatiy – SORM). In May 2023, the Ministry of Digital Development had fines introduced for operators who fail to install SORM, as well as an obligation for operators to obtain FSB approval before they can apply for a licence from Roskomnadzor. Telecoms operators must work with the FSB to implement SORM within 6 months of gaining a licence.

Legal and bureaucratic procedures

Roskomnadzor adds domain names, websites, and webpages to its Unified Registry based on a) orders from government agencies and the General Prosecutor's Office (see above); b) court orders; c) its own decisions.

(Private individuals can report internet content they believe to be unlawful through the Roskomnadzor website. Roskomnadzor sends these reports on to the relevant government agency, which then communicates its decision to Roskomnadzor.)

Russian internet service providers automatically download updates to the Roskomnadzor registry every 2-3 hours and the complete list once a day. They must then use their own filtering systems to block access to everything in the registry.

Access to users in Russia is sometimes restricted not just by Roskomnadzor and the telecoms operators, but also by hosting services and social media companies at Roskomnadzor's request – for example, the VKontakte social network will prevent Russian users from seeing a blocked profile, although the account itself still exists and its contents remain visible from abroad.

Roskomnadzor should contact a website's hosting provider with a demand to contact the site owner immediately, and have them remove the material which has been deemed to violate Russian law within 24 hours. They must then notify Roskomnadzor that this has been done. If the hosting provider does not do this, the site is added to the registry and blocked. If hosting providers and site owners can show that they have removed the material, Roskomnadzor will allow access to resume.

In practice, however, some organisations find that their websites have been blocked without any notification from Roskomnadzor.

Site owners are not involved in extrajudicial decisions to block websites (and are often not involved in court cases). While they may subsequently go to court to challenge a block within three months, this can be a lengthy and potentially expensive process.

"It is quite possible to overturn blockings based on a court decision", Yekaterina Abashina, lawyer at DBA and Partners in Moscow, commented to Kommersant on 27 March 2024 (https://www.kommersant.ru/doc/6553293). "At the same time, it is much more difficult to achieve the cancellation of a decision by a state body. In such cases, the courts deem compliance with the procedure for making a blocking decision to be the most important thing, and [the procedure] is almost always followed. At the same time, the nature of the content and the fairness of its classification as prohibited information are very rarely assessed".

Technical means

After Roskomnadzor has added a website to the Unified Registry, internet service providers/telecoms operators must then block it using their own systems for filtering internet traffic. The Open Observatory of Network Interference (OONI) found that operators use a number of different techniques (https://ooni.org/post/2023-russia-a-year-after-the-conflict/), including tls.connection_reset, tls.generic_timeout_error, tls.certificate_error, dns.dns_temporary_failure, tcp.connection_refused.

OONI also noted that blocks ordered through the registry are not always put into practice on all networks.

On 1 November 2019, the so-called "sovereign Runet" law came into force. This is a set of amendments to the Federal Law on Information aimed at "suppressing the dissemination of unreliable socially significant information under the guise of reliable messages that creates a threat of harm to the life and/or health of citizens [or to] property, a threat of massive disruption of public order and/or public safety, or a threat of interfering with the functioning [of critical infrastructure]", according to a Kremlin statement of 18 March 2019.

As well as creating domestic equivalents to international internet infrastructure – for example, a Russian domain name system (DNS) as an alternative to the global domain name system – these amendments oblige telecoms operators to install state-provided equipment at key internet nodes, both within and at the borders of the country, enabling Roskomnadzor both to block information it deems a threat to the state, and to isolate the Russian segment of the internet (the "Runet") from the rest of the world wide web in the event of "external threats".

Creation of the "sovereign Runet" has included the installation of "technical means of countering threats" (tekhnicheskiye sredstva protivodeystviya ugroza, TSPUs), allowing Roskomnadzor to monitor and filter internet traffic and block apps and websites unilaterally, no longer having to rely on individual internet service providers to implement restrictions (although this still takes place on a large scale), and without adding these sites to the Unified Registry.

In October 2023, Roskomnadzor director Andrey Lipov said that mobile, broadband, and cross-border communication nodes in Russia were now "100% closed with the help of TSPUs", Forbes.ru noted on 9 September 2024 (https://www.forbes.ru/tekhnologii/520876-rkn-pletet-novye-seti-sluzba-obnovit-sistemu-blokirovki-sajtov-za-59-mlrd-rublej).

With the introduction of TSPUs, website blocking has become "increasingly opaque and unpredictable, and, to put it mildly, very dubious even from the point of view of the legal norms that regulate the blocking of sites", according to Roskomsvoboda (https://roskomsvoboda.org/en/post/suvenir-runet-obrastaet-cenzuroy/). "It is impossible to trace by what decision and on what grounds these blockings and slowdowns occur through the TSPU. And this, let us recall, affects our constitutional rights to access and disseminate information."

A TSPU consists of a set of hardware and software through which internet service providers are obliged to route all internet traffic, which analyses this traffic and directly blocks prohibited materials. It can also slow down access to certain sites – for example, Twitter in 2021 and YouTube in 2024 – block VPNs, and implement local-level shutdowns (as happened in Dagestan after rioters attacked a passenger plane from Israel in October 2023).

Roskomnadzor's Centre for Monitoring and Control of the Public Communications Network (CMU SSOP) installs this equipment on telecoms operators' premises and is responsible for all subsequent management; the operators have no access to it and cannot override any blocks. TSPUs are known as 'black boxes' because telecoms companies themselves "do not know what Roskomnadzor does with the traffic on their networks", Forbes.ru noted (https://www.forbes.ru/tekhnologii/520876-rkn-pletet-novye-seti-sluzba-obnovit-sistemu-blokirovki-sajtov-za-59-mlrd-rublej).

Although the blocking of internet resources without including them in the registry does not appear to take place on en masse, "there are and have been precedents", Artyom Kozlyuk of Roskomsvoboda told Forum 18 on 9 September.

For example, there appears to have been a surge in non-public blocking of websites in the lead-up to the Russian presidential elections in March 2024, Radio Liberty noted on 15 March (https://www.svoboda.org/a/roskomnadzor-veroyatno-nachal-napryamuyu-blokirovatj-sayty/32862918.html), when Roskomnadzor stopped updating the Unified Registry entirely. This hiatus lasted a few weeks, Kozlyuk told Forum 18.

It is not clear how exactly TSPUs work. In contrast to the registry-based blocks which internet service providers implement, which identify banned sites by IP address or URL, TSPUs are known to analyse the content of internet traffic (https://www.digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more) using Deep Packet Inspection technology. They identify sites to block by means of "signatures", or patterns in data, Kozlyuk of Roskomsvoboda explained to Forum 18. It is unclear whether Roskomnadzor's systems for analysing text and images are integrated with TSPUs. (END)

More reports on freedom of thought, conscience and belief in Russia (https://www.forum18.org/archive.php?country=10)

For background information see Forum 18's Russia religious freedom survey (https://www.forum18.org/archive.php?article_id=2897)

Forum 18's compilation of Organisation for Security and Co-operation in Europe (OSCE) freedom of religion or belief commitments (https://www.forum18.org/archive.php?article_id=1351)

Follow us on X/Twitter @Forum_18 (https://x.com/forum_18)

Follow us on Facebook @Forum18NewsService (https://www.facebook.com/Forum18NewsService)

Follow us on Telegram @Forum18NewsService (https://t.me/s/forum18newsservice)

If you need to contact F18News, please email us at:
f18news @ editor.forum18.org

Forum 18
Postboks 6603
Rodeløkka
N-0502 Oslo
NORWAY