RKS Global

June, 2026 · rks.global

Runet 2025: Sovereignization and Degradation

An Overview of Internet Censorship in Russia in 2025

Table of contents

1. Runet 2025: A Shift in the Internet Control Model..... 3

2. TSPU and DPI..... 7

How it works..... 7

Liability for telecom operators..... 8

3. Registry-Based Blocking..... 9

Roskomnadzor's Blocklist..... 9

Blocks Motivated by Military Censorship..... 10

Blocking Information About Circumvention..... 12

4. From IP Blocking to Protocol Control..... 13

5. Blocking Global Services and Promoting Local Alternatives..... 14

Communication Control..... 14

Pressure on Gamers..... 16

Promoting National Services..... 17

6. Pressure on App Stores, Media Platforms, and Content Censorship..... 17

Targeting App Stores..... 18

Pressure on Social Media and Content Creators..... 19

Censorship of Content Platforms..... 19

The Degradation of YouTube..... 21

7. Telecommunications as a Control Instrument..... 22

8. Regional Shutdowns in Russia..... 23

9. Whitelists and Greylists..... 27

10. Roskomnadzor vs. VPN: A Game of Cat and Mouse..... 29

Shifts in the Anti-Censorship Market..... 29

Unsafe VPNs..... 31

VPN as an Aggravating Circumstance..... 32

Blocking VPN Protocols..... 33

11. Alternative Circumvention Tools..... 34

12. Expanding Prohibitive Legislation..... 36

Banning the Search for Extremist Materials Online..... 36

Banning Advertising with "Undesirable" and "Extremist" Organizations..... 37

13. Toward Runet Isolation: Reducing Dependence on Global Infrastructure and Technology..... 38

14. Conclusions and Forecasts..... 39

1. Runet 2025: A Shift in the Internet Control Model

The work of Russia's censorship agencies changed qualitatively in 2025. If Roskomnadzor previously added websites, technical domains of apps, and other services to its registry and forced internet providers to block them, the agency now manages blocks at the architectural level.

The focus of censorship has shifted from "illegal" content to the transport and network layer: protocols, traffic types, mobile access, and infrastructure nodes. And with the introduction of shutdowns, connectivity itself came under attack. The internet in Russia now increasingly operates not on a principle of "allowed or prohibited," but on "working partially or unstable."

Throughout the previous decade, the regulatory system was built around registries of banned sites and the steady expansion of the regulator's powers. Domains and IP addresses were added to the lists, specific services were blocked, individual apps were restricted. Laws on blocking, on the "sovereign internet," and on the localization of foreign IT companies provided the legal framework, while TSPU hardware with deep packet inspection (DPI[1]) built out the technical capacity to enforce it. But in 2024, the situation changed.

In March 2024, a ban on the "promotion" of circumvention tools came into force. Throughout 2025, websites and individual pages containing information about bypassing blocks continued to be actively blocked, and a law introducing fines for VPN advertising was adopted. By year's end, the list of materials blocked by Roskomnadzor for "propaganda" of censorship circumvention stood at around 3,000 sources.

[1] TSPU (Technical Means for Countering Threats) — hardware devices installed at internet providers that filter internet traffic according to instructions passed down from above.

DPI (Deep Packet Inspection) — the technology used by censors to detect and block VPN connections and other circumvention tools.

Mass blocking of popular VPN protocols via TSPU — OpenVPN, WireGuard, Shadowsocks — also continued in 2025, but with more selective methods, including active probing[2].

In other words, the object of regulation is no longer specific websites, but connection methods. Not resources, but traffic types.

This is evidenced by restrictions on UDP traffic (affecting video streaming and online gaming) even when the platforms themselves remained accessible, by disruptions to voice calls in messaging apps before those apps were blocked outright, and by attempts to filter advanced VPN protocols such as VLESS with Reality.

In 2025, regional mobile internet shutdowns became routine practice rather than an emergency measure. While counter-drone operations were cited as the official justification, the shutdowns affected not only border regions but also areas in Siberia and the Far East.

A "whitelist model" was actively tested, in which only a limited set of government-approved services functioned reliably, while others worked intermittently or not at all — without any formal ban. In some cases this shaded into a "greylist" dynamic: certain non-banned services worked normally, others experienced outages, and others were inaccessible altogether.

At the same time, the infrastructure layer came under attack — CDN providers, DNS services, cloud platforms, and DDoS protection systems. Targeting these nodes allows authorities to affect thousands of resources simultaneously rather than issuing individual takedowns. A high-profile example was the blocking of Cloudflare, a company underpinning the server ecosystem of millions of websites. The incident knocked out not only VPN services but also the websites of Rostelecom, Beeline, Twitch, Miro, SoundCloud, Aviasales, and others — reminiscent of the Telegram block in 2018. Roskomnadzor denied any intentional restriction.

[2] Active Probing — a method for detecting VPN services. The censor sends probe requests to addresses or servers it considers suspicious and analyzes how they respond. VPN services have a characteristic response pattern, on the basis of which the address is blocked.

Now as authorities perceive the internet as a security threat, collateral damage is no longer a concern.

Another dimension of 2025 censorship was the transformation of telecommunications into an access-control instrument: tighter SIM card verification requirements, roaming restrictions, and more burdensome procedures for obtaining virtual numbers. Strict SIM card oversight also became part of a parallel process — the gradual erosion of Russians' right to privacy and anonymity — though the stated reason was combating fraud.

In late 2024, the Ministry of Digital Development amended the Law on Communications and required foreign nationals to link their SIM cards to biometric data. Starting July 1, 2025, subscribers who failed to comply began losing service.

For Russian citizens, it was hardly better. In April 2025, new rules for verifying individual subscriber data came into force. By November, users were required to complete personal data submission to their network providers and to cap the number of SIM cards registered in their name at twenty. A SIM card "cooling" procedure was also introduced, triggered after 72 hours of inactivity or upon a subscriber's return from abroad. The official reason: drone threats again.

Article 13.29.1 of the Code of Administrative Offences established penalties for subscribers who hand over their numbers to third parties, with fines ranging from 30,000 to 50,000 rubles for individuals, up to 100,000 for individual entrepreneurs, and up to 200,000 for legal entities.

Pressure on global platforms intensified in 2025. As in 2024, Russian authorities sent requests to app stores demanding the removal of VPN applications and apps belonging to independent media outlets. Simultaneously, censors successfully blocked popular messaging apps while promoting domestically developed Russian alternatives.

This represents a significant shift in the censorship model: a system is taking shape in which internet access is no longer a constantly available public good, but an option that can be switched off from above.

In 2025, not only censorship practices changed, but also how those practices are framed publicly. Officials now speak less and less about bans and blocks as such,

and increasingly describe their actions as protective measures — against fraudsters, "extremism," military threats, or "harmful content" for children.

Specifically, blocks, throttling, and regional shutdowns are called temporary measures for the sake of security. Using VPN tools and other circumvention technologies is being reclassified as suspect — even criminal — activity, and is therefore, by the authorities' logic, subject to strict regulation or outright prohibition. Malfunctions in the filtering equipment itself are contributing to the broader sense of internet degradation as well.

In 2025, censors largely stopped seeking legal justifications that framed restrictions as responses to violations of Russian law. Instead, authorities began relying on cliches about the need to ensure citizens' safety.

Taken together, these developments mark a new stage in Russian censorship — one defined not by the volume of blocks, but by a change in the nature of intervention:

- Outright blocking is increasingly replaced by managed degradation — deliberate deterioration of data transmission quality;
- Filtering now extends to traffic types and protocols, not just specific online resources;
- Internet access is no longer uniform across the country: the same services and features may function in one region while being unavailable in another, depending on the local operator's current network "mode";
- A user's access to connectivity can now be restricted at the telecommunications level itself, through SIM card controls.
- In 2024, RKS Global experts made forecasts about how censorship in Russia would develop. Among the likely scenarios were:
- the use of statistical blocking methods;
- the banning of popular international services and promotion of domestic alternatives;
- the introduction of whitelists;
- the expectation that circumvention would remain possible under tightening censorship only through tools capable of disguising themselves as innocuous services and thus evading DPI.

2025 bore out RKS Global experts' worst expectations. WhatsApp and Telegram were blocked amid the push to adopt the national messenger MAX; regions began transitioning to white lists; and VPN services lacking traffic obfuscation and split

tunneling capabilities almost entirely stopped working. Yet despite tighter censorship legislation and the deployment of new blocking methods — including statistical approaches that flag traffic as suspicious when large volumes are directed at an unknown resource — VPN services with obfuscation features continued to perform well.

2. TSPU and DPI

By 2025, the technological infrastructure of censorship in Russia had definitively become an independent connectivity-management system.

How it works

The core component of this infrastructure is the TSPU system (Technical Means for Countering Threats) — specialized hardware-software complexes that all internet providers are legally required to install on their networks, giving authorities full control over internet traffic within the country.

TSPU operates independently of Roskomnadzor's registry: it blocks individual internet resources, hosting services outside state control, VPN protocols, and more — all without reference to the official banned-sites list. Internet providers and telecom operators have no ability to influence how TSPU functions.

The system can also throttle traffic or shut down internet access entirely in specific regions.This can be passed off as a technical fault rather than a deliberate ban.

By 2025, the TSPU infrastructure was fully deployed. Experts report near-complete coverage of key network nodes, including broadband access points (the infrastructure nodes through which subscribers connect to an operator's network), mobile networks, cross-border nodes, and even satellite operators. The regulatory framework for it had been put in place the year before.

In January 2026, it emerged that GRFC — the agency subordinate to Roskomnadzor — has a KPI target of filtering 98% of Russian internet traffic and blocking 92% of VPN connections by 2030. After this was reported in the press, the documents disappeared from Roskomnadzor's website.

According to sources cited by RBC, in December 2025 Roskomnadzor updated TSPU settings, causing significant disruptions to VPN services. In particular, three protocols were blocked: SOCKS5, VLESS, and L2TP. The VLESS protocol leaves

minimal technical traces and had previously evaded detection — but in December it became clear that TSPU had learned to identify it through indirect indicators.

Liability for telecom operators

In late 2025, amendments to the Russian Code of Administrative Offences were adopted tightening liability for telecom operators. These cover rules for internet operation, subscriber data verification, and interaction with regulatory authorities. Most of the new provisions came into force on January 1, 2026, and within days Roskomnadzor announced it had identified 35 violations related to TSPU installation.

In one case from December 2025, the Center for Monitoring and Management of the Public Communications Network audited traffic passing through the TSPU on the Tinko provider's network. The provider had failed to route traffic to its connected network through the TSPU, with the result that YouTube remained accessible to its subscribers. An administrative violation report was filed and a fine of 250,000 rubles was imposed.

In April 2026, further fines against telecom operators for violations of TSPU installation and usage rules became public. According to media reports, courts issued fines totaling 4 million rubles across 15 violations, with warnings issued in five additional cases.

The censorship infrastructure in 2025 operates across two interlocking layers:

1. The DPI/TSPU infrastructure enables blocking not only by lists of banned addresses, but by intervening in the connection itself — filtering, throttling, or severing traffic based on its characteristics and behavior. As a result, restrictions manifest as instability or degradation of specific functions rather than formal blocks.

2. Action against a single infrastructure layer scales across thousands of resources simultaneously by targeting the largest nodes in the ecosystem — such as Cloudflare

3. Registry-Based Blocking

Despite the evolution of TSPU, the state continues to expand registry-based blocking in parallel. Authorized agencies and courts issue rulings designating information as prohibited; Roskomnadzor adds the site or page to a dedicated registry, which internet providers are then required to enforce.

Roskomnadzor's Blocklist

Roskomnadzor reported restricting access to 1,289,000 items in 2025 — a 59% increase on 2024. These figures refer to individual pieces of content, not distinct websites or domains. Blocks on VPN-related materials surged to 93,000 (up 1,235%), while "LGBT content" reached 170,300 items (up 269%).

Under the banner of "countering threats to the stability, security, and integrity of Runet," 2025 also saw the blocking of 252 anonymous email services (up 20% year-on-year), 173 applications (up 28%), 410 malware distribution centers, more than 1.2 million resources (up 50%), and 119,000 phishing sites (up 441%).

For nearly 13 years, until October 2025, Roskomsvoboda, a digital rights protection public organization, operated a public monitoring service for the banned-sites registry, which also included a registry of bloggers and information distributors. Following the organization's suspension, a new aggregator tracking blocking data emerged at blockedin.org.

Drawing on data from both projects, experts calculated that 570,439 pages and websites were added to Roskomnadzor's registry in 2025, of which approximately 46,000 were subsequently unblocked. The total number of blocks recorded since monitoring began stands at 1.7 million.

Blocks Motivated by Military Censorship

Roskomsvoboda documented that by August 2025, around 25,000 entries in the registry had been added on grounds of military censorship — blocks initiated by an "unspecified government body" (which experts believe was a cover for the Prosecutor General's Office). According to experts analyzing the banned-sites registry, by spring 2026 the number of sites and links blocked under the pretext of combating "discreditation" and "fake news" about the military had exceeded 30,000.

Military censorship in Russia began on February 24, 2022. Within the first days, the Prosecutor General's Office began issuing blocking orders, which immediately took on a mass character. In a short period, bans were imposed on Facebook and the Messenger, Instagram, Twitter, BBC, Voice of America, Deutsche Welle, the student journal DOXA, the investigative outlet Bellingcat, Kavkazsky Uzel, TJ, a large number of Ukrainian publications — UNIAN, TSN, Zerkalo Nedeli, Channel 24, Hromadske — as well as Ukrainian government websites, including those of the Ministry of Health and the anti-corruption bureau NABU.

In the days and weeks that followed, the list grew at an avalanche pace: Meduza, Mediazona, Echo of Moscow and TV channel Dozhd, Republic, The Village, Bumaga, Radio Svoboda, Colta.ru, Amnesty International, Golos, 7×7, Instagram, Euronews, The New Times, the independent Belarusian broadcaster Belsat, and many others.

Some orders were progressively expanded: where late February and early March rulings covered dozens of sites, by April a single order could encompassed several hundred.

The legislative basis for military censorship was established only afterward. Laws on "discrediting" the army and on "fake news" about it granted the Prosecutor Office expanded powers to block resources without a court order. Subsequently, an ever-growing share of blocking orders began to be attributed to a so-called "unspecified government body". This "unspecified body" is today the primary censor of any material presenting information that diverges from the Russian authorities' official narrative about the "special military operation."

108.138.7.128 and 3 more IP-addresses

Status	Blocked
Domain	*.de44d3365da6.click
IP-address	108.138.7.57 108.138.7.92 108.138.7.97 108.138.7.128
Authority	—
Number of decision	Решение не указано
Decision date	25.08.2022
Date of first blocking	16.12.2022
Date of the last update	16.12.2022

https://blockedin.org/

Ban of one of the True Story news portal mirrors.

The trajectory of military censorship blocks tells its own story: by July 2022 the count had exceeded 5,000; by February 2023, 10,000; by November 2023, more than 15,000; by summer 2024, 20,000; by summer 2025, 25,000.

By the end of 2025 and into early 2026, the number of blocks motivated by military censorship stands at over 30,000.

Among the sites blocked in 2025 on military censorship grounds was the official website of football club Dynamo Kyiv. Songs by rapper Noize MC and singer Monetochka are also among the blocked content. Notably, because blocks are often applied at the HTTPS level, they frequently cut off access not just to a single page containing "prohibited content" but to an entire website. This is what happened when a piece by Spanish sports outlet Marca — debunking a fabricated story about Vladimir Putin — was blocked, taking the entire domain offline.

Blocking Information About Circumvention

According to experts, the number of entries in the registry blocked for containing information about bypassing censorship approached 3,000 by the start of 2026. This encompasses not only VPN service websites themselves, but also guides, mirrors, documentation pages, reviews, and any other material relating to circumvention.

Since March 2024, Roskomnadzor has had the authority to block, without a court order, any resource containing information about methods of bypassing internet censorship. One likely driver of this legislation was the mass surge in VPN, proxy, and other anti-censorship tool usage following the 2022 wave of blocks — when Russians found themselves cut off from Facebook, Instagram, Twitter, and dozens of independent media outlets, and rapidly adopted tools to restore access to blocked content.

From the very first days the law was in effect, Roskomnadzor began mass-adding circumvention-related resources to the registry. Between March 1 and 6, 2024, alone, 1,700 sites and links were blocked. A characteristic feature of these blocks is the use of so-called "elastic" orders: new links continue to be added to the registry on the basis of a single Roskomnadzor ruling issued back in March 2024.

VPN service websites and their mirrors were the primary targets. Among those added to the registry: ExpressVPN, Tesla VPN, Pingle VPN, Gen VPN, Happ VPN, Ded VPN, Octohide VPN, PaperVPN, and Amnezia VPN. The blocks extend beyond the services themselves to any mention of them.

In 2025, the VPN Guild's website was banned. A site selling the Deeper Connect router — which has a built-in VPN — was also blocked. The "Yuboost" service for improving YouTube performance was banned, with authorities for a time hunting down every variation of its domain name. A page on the gaming platform Fandom containing circumvention information was blocked. A mirror of AdGuard VPN (among others) hosted on Amazon Web Services was taken down. Links containing information about the VLESS protocol and the XRay core were blocked.

Services with only an indirect connection to the topic have also been caught in the net. For example, links with instructions on restoring access to Facebook and Instagram, published on entirely unrelated third-party websites, have been blocked. The entertainment platform Pikabu is regularly compelled to remove content about circumvention tools to avoid being added to the registry itself — in 2025 it received nearly 30 government takedown requests for "instructions on bypassing blocks."

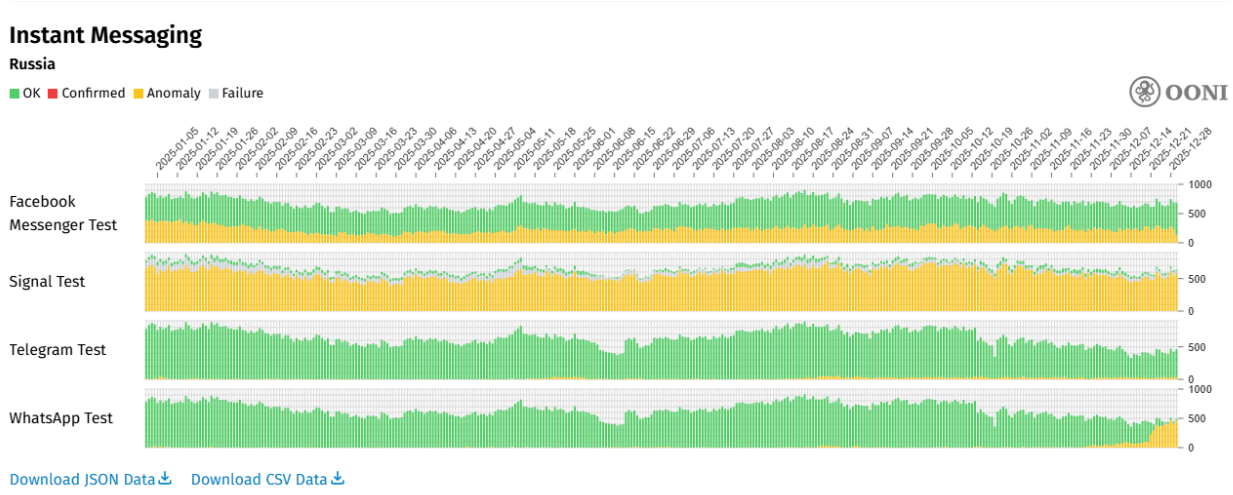
4. From IP Blocking to Protocol Control

Beyond blocking specific IP addresses and domains, censors have increasingly turned to blocking protocols and specific traffic types — meaning that censorship now intervenes in the connection method itself. For users, this manifests not as a specific website being unavailable, but as certain functions becoming unstable: voice calls in messaging apps, certain VPN services, and services using the data transmission protocol known as User Datagram Protocol (UDP).

Throughout the year, numerous reports were recorded of VPN failures on WireGuard-based protocols, problems with gaming services, and VoIP call disruptions. These failures occur when the censor rather bluntly filters or restricts UDP while leaving TCP (Transmission Control Protocol) functional. UDP is generally more sensitive than TCP: it is used for real-time media transmission, and it is relatively easy for authorities to disrupt a dense, steady media stream.

A characteristic example of protocol-level interference was the degradation of VoIP and messaging app calls. Users reported failures during voice calls in Telegram and WhatsApp, even as text messages continued to go through.

In August 2025, Roskomnadzor officially confirmed "partial restrictions" on calls in Telegram and WhatsApp, while the public statement emphasized that "no other functional restrictions" had been introduced. Reports of problems in other similarly structured VoIP services (video conferencing and calls) followed shortly after. Roskomsvoboda documented complaints about Google Meet failures in Russia in the absence of any global Google outage, while Roskomnadzor publicly denied having taken any restrictive measures.



5. Blocking Global Services and Promoting Local Alternatives

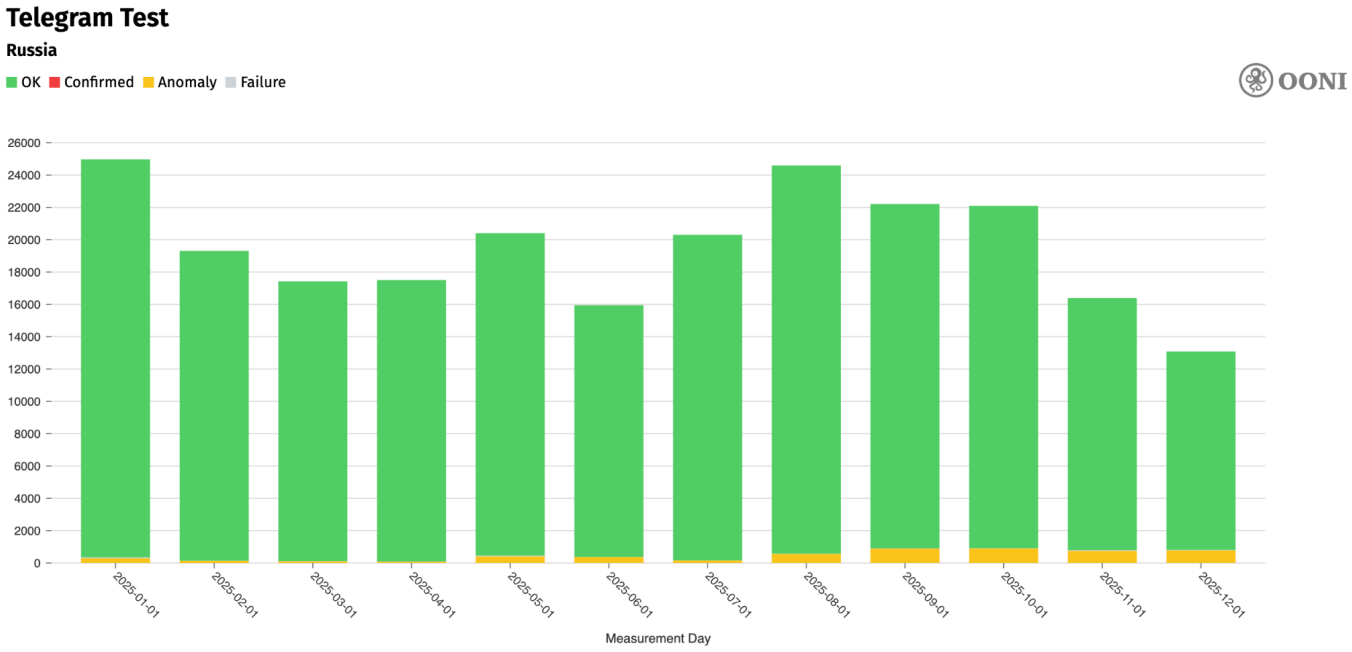
The dynamics of 2025 in the blocking of global services are best illustrated by the war on popular messaging and communication apps. While 2024 saw blocks imposed on relatively niche services — Viber, Discord, Signal, Session, SimpleX Chat — in 2025 authorities went after the most widely used platforms. Against this backdrop of pressure on global services, import substitution ceased to be merely a slogan and became a concrete restrictive measure.

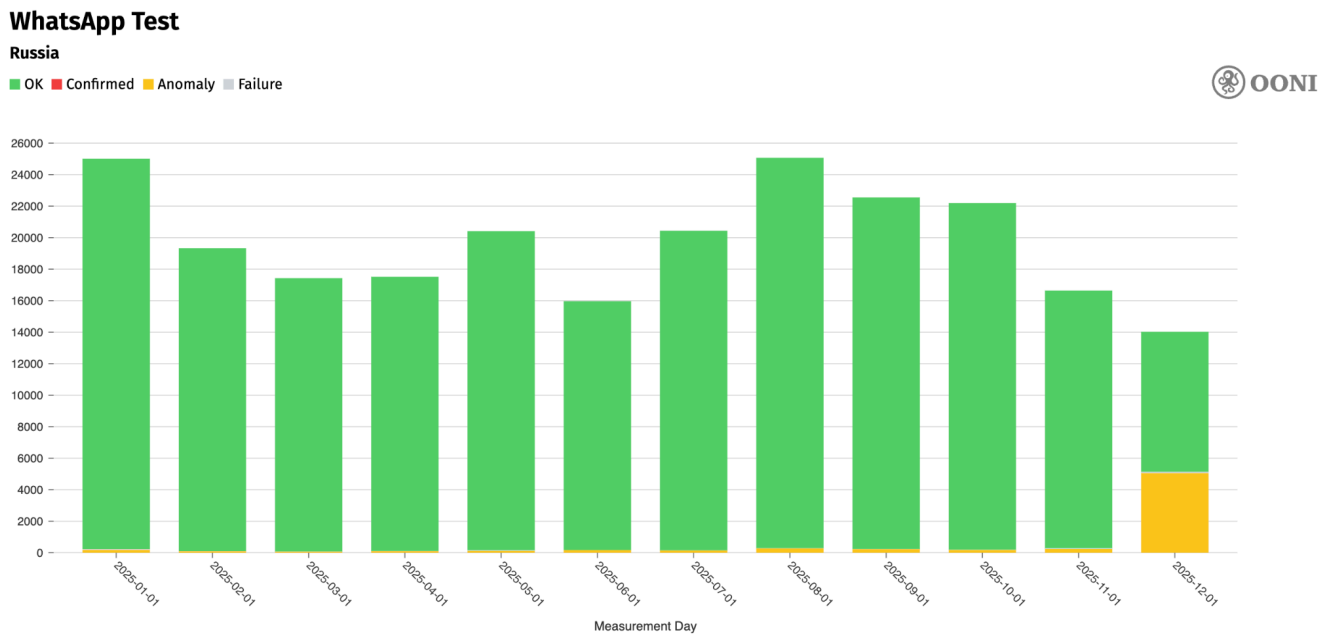
Communication Control

In August 2025, Roskomnadzor announced it would introduce "gradual restrictions for services that systematically ignore Russian legislation, with the possibility of lifting them once violations are remedied." The stated requirements included hosting servers on Russian territory, ensuring personal data protection, protecting citizens from fraud, and creating conditions for suppressing extremism and terrorism. The requirements around fraud protection and extremism suppression have no quantitative benchmarks: Roskomnadzor itself decides how well services comply.

From that same August, authorities began restricting voice and video calls in the two most popular messaging apps in Russia — WhatsApp and Telegram. Roskomnadzor stated that the restrictions had been imposed "to counter criminals." Telegram was accused of "systematically creating" infrastructure for leaking Russians' personal data — though in reality the platform had been regularly removing data-harvesting bots.

According to some media reports, Russian telecom operators had already been pushing to block calls in foreign messaging apps as early as spring 2025. The companies openly explained this as a need for additional revenue to maintain their infrastructure.





Measurements of Telegram and WhatsApp performance in Russia in 2025 (the presence of anomalies indicates potential blocking, in cases where no definitive signals such as block pages are present)

Pressure on Gamers

Alongside messaging apps, global gaming platforms came under censors' attention. In spring 2025, against the backdrop of access problems affecting resources behind Cloudflare, complaints emerged about disruptions to gaming services and game developers (Steam, Ubisoft, Epic Games), the streaming platform Twitch, the game Genshin Impact, and Discord.

The user-generated content platform for children and teenagers, Roblox, was also affected. On December 3, 2025, Roskomnadzor restricted access to it, and on December 17 published an official statement about having contacted the platform's leadership "after restricting its operation in Russia" and about Roblox's readiness to gradually bring its operations into compliance with Russian law.

Child protection from harmful or illegal online content is always more publicly palatable than abstract measures against fraudsters and terrorists, so the public reaction on blocking Roblox was predictably muted. User-generated content platforms will always contain material that can be deemed problematic — meaning there will never be a shortage of pretexts for blocking.

Promoting National Services

In March 2025, VK announced the launch of a beta version of the Russian "super-app" MAX, and by mid-August 2025 the MAX press office reported 18 million users. Even if true, that figure came nowhere near the numbers of WhatsApp and Telegram. At the height of the voice call blocks on those platforms — amid administrative pressure and aggressive media promotion of MAX — the national messenger's average daily reach stood at 5.7% of the population. Telegram and WhatsApp reached 55.2% and 66.7% respectively.

The low usage figures for MAX may reflect not only privacy concerns: the messenger simply appears unpolished and less convenient than the foreign alternatives people are accustomed to. Nevertheless, the Russian super-app comes pre-installed on new phones sold in Russia, and employees of public-sector institutions, as well as parents of schoolchildren and kindergarteners, are being pressured to use it under threat of professional or educational consequences. Either way, its user base is growing.

In September 2025, RKS Global experts tested MAX for continuous user surveillance and disproved the hypothesis that it behaves as spyware. However, within a few months, new tests showed that extended surveillance functionality had appeared in the app — it could request more permissions or attempt to obtain them without asking, and could transmit more information than it had been granted access to, among other things. The behavior of a state-affiliated messenger can change at any moment, while Russians are left with virtually no choice but to use state-controlled services.

6. Pressure on App Stores, Media Platforms, and Content Censorship

In 2025, Roskomnadzor continued its offensive against platforms hosting various types of content. Every channel through which Russians access information and useful tools came under fire.

Targeting App Stores

In 2025, deplatforming — pushing circumvention tools out of the places where they are distributed — took on a mass character. In March 2025, Roskomnadzor sent 47 requests to Google to remove VPN applications, whereas previously such requests had been isolated incidents.

According to the App Censorship project, which studies internet censorship, between March 12 and April 1, 2025, Russia submitted 214 app removal requests to Google Play, targeting 212 VPN and similar services — more than 90% of all requests to Google during that period. Beyond app removals, Roskomnadzor demanded the delisting of more than 80,000 URLs from Google Search under the law banning information about bypassing blocks, but the company ignored the requests.

Apple has been quicker and more compliant in accommodating Russian authorities. As early as September 2024, 98 VPNs were already unavailable in the Russian App Store — in addition to independent media apps and podcasts. Calls for transparency and respect for human rights were met with no response then, and continue to be ignored.

In early 2025, Apple blocked Russian developers' access to the Apple Developer Enterprise Program (ADEP) — a tool previously widely used by large companies and developers to distribute corporate business apps, chatbots, CRM systems, and logistics solutions without going through the App Store.

Company representatives explained their compliance as necessary to continue operating in Russia. As 2026 is showing, however, a "nothing personal, just business" position doesn’t protect that business from subsequent state demands.

Removing VPN apps from stores complicates the user journey. Some users simply give up on installing proven services when they are unavailable in the App Store. VPN developers and experts publish guides to help users install services through alternative means, but the problem remains acute. In 2025, Apple continued to hide VPN apps from Russian users.

By spring 2026, it emerged that Apple had removed a number of proxy and V2Ray clients from its store, including Streisand, V2Box, v2RayTun, and Happ Proxy Utility — apps frequently used to access independent media and Telegram under DPI-based blocking.

Pressure on Social Media and Content Creators

In November 2024, a law requiring bloggers to register in Roskomnadzor's ocial media registry came into force. All bloggers with more than 10,000 subscribers on any social network were required to submit an application through the Gosuslugi portal and provide personal data, or face a ban on posting advertising and sponsorship content, with users unable to share their posts.

In spring 2025, authorities added the Trustchannelbot to Telegram to cross-reference application numbers on Gosuslugi with channel owner data and mark verified channels with an A+ badge. To participate, bloggers had to add the bot to their channel — giving it access to channel management and content. Trustchannelbot could view posts, edits and removals, change the channel name, description, and username, and add or remove members.

This practice created real risks of mass audience data collection in the event of hacks or leaks; early versions of the mechanism allowed users to be linked to their phone numbers and Gosuslugi profiles. Roskomnadzor's requirement to verify Telegram channels through a dedicated bot turned bureaucratic registration into a technical lever of control.

Censorship of Content Platforms

In 2025, a new wave of censorship swept digital content platforms. Music, films, and books began disappearing not only through registry-based blocking, but also through systematic removals from streaming services and online libraries.

Yandex Music, for instance, removed 1,576 units of content (songs, music videos, podcasts) at government agencies' request during Q4 2024 and Q1 2025, and received dozens of additional URL-specific takedown requests. This included content deemed "aimed at destabilizing the socio-political situation in Russia" — a category that subsequently appeared as a distinct entry in Yandex Music's Transparency Report. A further 2,068 items were removed over Q2–Q4 2025.

The online cinema Kinopoisk (owned by Yandex) removed nine films and series in 2025 at Roskomnadzor's request. The grounds were: "propaganda of non-traditional relationships" (five titles) and scenes depicting suicide (four titles). The platform also preventively removed around two thirds of all the movies containing LGBTQ+ scenes and characters. The company's director noted that no removal requests had been received from other government bodies.

According to media reports, in August 2025 Moscow's Tagansky District Court ordered Kinopoisk to pay a fine of 3 million rubles for displaying content deemed "propaganda of non-traditional sexual relationships." Kinopoisk had already been fined 10 million rubles on a similar charge in 2024.

Other Russian online cinemas and streaming platforms — Okko, Ivi, and Beeline TV — also faced fines and sanctions for hosting prohibited content. Streaming services removed the Spanish series Galgos, in which signs of “LGBTQ propaganda” were identified. Apple was fined 7.5 million rubles in connection with distributing a series containing scenes of "propaganda of non-traditional sexual relationships" through its streaming service.

Alongside top-down censorship, self-censorship is spreading. Popular streaming services are mass-editing out scenes deemed sensitive — particularly LGBT storylines — and in some cases, where too much must be cut, blocking access to individual episodes entirely. Scenes involving erotica, smoking, alcohol, and profanity are also being excised. Users complained that streaming services were not labeling content that had been edited, passing modified versions off as originals. By early 2026, reports emerged that some services had begun adding such labels.

From March 1, 2026, a law came into force in Russia banning the distribution and screening of films that discredit traditional Russian spiritual and moral values or promote their rejection. The law was signed by Vladimir Putin on July 31, 2025.

In the book market, beyond selective pressure on publishers and booksellers, by year's end the logic of preemptive self-censorship had reached large online catalogs: content disappears not only through direct prohibition, but out of fear of legal consequences for platforms and rights holders. Litres, the largest e-book and audiobook service in Russia and the CIS, reported removing approximately 4,500 books due to the risk of sanctions for "drug propaganda". In total, it removed roughly 0.5% of its catalog.

Russian publishing houses spent the year hastily pulling titles from shelves that might be considered dangerous by censors. With no official lists of banned books, the burden of selection falls on booksellers themselves. The purge extends beyond LGBT-themed titles to books touching on drugs, feminism, religion, and more.

On May 14, 2025, staff at the publishers Popcorn Books and Individuum (both part of the Eksmo-AST group) were charged with extremism. The Investigative Committee alleged the publishers had engaged in “LGBTQ propaganda”, including targeting minors. Following the charges, all books from both imprints were pulled from sale and destroyed, and the publishers ceased operations. In spring 2026, offices of Eksmo were raided by the police, with equipment and documents seized.

The Degradation of YouTube

Throttling — the deliberate slowing of connection speeds by internet providers — of YouTube has its own long history in Russia. Users continue to experience slowdowns and partial inaccessibility severe enough to make using the service without a VPN practically impossible. Rather than an outright ban, authorities have degraded connection quality to the point of total unusability. This approach allows the platform's audience to be reduced without a formal prohibition — and with it, the risk of negative public backlash.

When YouTube throttling began in 2024, Russian authorities initially blamed Google's equipment degradation. Later, official statements acknowledged the actions were deliberate. In 2025, the State Duma set out the conditions under which YouTube could resume normal operation in Russia: Google would need to pay fines (which constitute around $1.2 quintillion by February 2026 — a million times more than world GDP) , restore access to Russian media accounts blocked without a court order, and "handle its abandoned equipment."

In December 2025, Google notified Russian providers that it planned to retrieve its Google Global Cache (GGC) equipment — specifically Dell R720 caching servers — as no longer in service. And in early 2026, it emerged that the domain name www.youtube.com had been removed by Roskomnadzor from Russia's National Domain Name System (NDNS).

7. Telecommunications as a Control Instrument

One of 2025's defining innovations was the introduction of total SIM card surveillance. The state began determining who has the right to connect, on what terms, and when a user gains access to mobile internet.

From January 1, 2025, purchasing a SIM card became significantly harder for foreigners. To obtain a phone number, foreign nationals and persons without citizenship were required to have a SNILS number (Russia's national insurance number), a Gosuslugi account, and biometric identity verification. Registration of the device's unique IMEI number also became mandatory. Authorities justified the tightened procedure as "measures aimed at combating fraudsters and grey SIM cards."

The new SIM card regime introduced restrictions for Russian citizens as well. Russian nationals could register a maximum of 20 SIM cards per passport (10 for foreign nationals). Telecom operators audited how many phone numbers were registered to each subscriber and disconnected those who failed to meet the new requirements — resulting in 14 million phone numbers being blocked over the course of the year.

In 2025, a new term entered everyday use: SIM card "cooling." Upon returning from abroad, a mobile subscriber would receive an SMS informing them that network services were unavailable and that they needed to complete verification — or wait 24 hours for connectivity to be restored. The same applied if a SIM card had been inactive for more than 72 hours. Once verification was completed (via a hotline call, a carrier app, or other means), mobile internet and SMS functions were unblocked.

Authorities claimed that "cooling" was intended to disconnect SIM cards being used in Ukrainian drones, causing them to lose control. The Kremlin stated that the procedure causes citizens "no discomfort whatsoever."

A significant new development was the liability imposed on subscribers for transferring their personal SIM cards to third parties. Article 13.29.1 of the Code of Administrative Offences introduced fines of up to 50,000 rubles for individuals and up to 200,000 for organizations for allowing others to use their mobile number. This measure was also framed as anti-fraud.

In this way, authorities once again legitimized mobile internet disconnection in their own interests — no longer as a one-off security measure, but as a formalized procedure with access restored only after identity verification.

8. Regional Shutdowns in Russia

In most regions, restrictions affected not only messaging apps and social networks but also services that had long simplified daily life: banking apps, online payment systems, ride-hailing and delivery services.

Mobile internet outages were recorded across almost every region of Russia in 2025. The first major disruptions came in May: on the eve of Victory Day celebrations, mobile internet disappeared across all major operators in dozens of regions. Authorities officially attributed this to security measures at mass events and urged citizens to be "understanding" about the restrictions given the "dangerous proximity" of threats. At the time it was presented as an exceptional measure, but similar shutdowns soon became routine.

In Moscow, May 2025 outages lasted several days and covered at least the city center, where parade rehearsals and then the holiday events were taking place. By March 2026, a mobile shutdown in Moscow lasted nearly two weeks, causing serious economic damage. Authorities stated that such disconnections could last "as long as necessary to ensure citizens' safety."

From June 2025, the frequency of internet outages grew dramatically. According to the Na Svyazi project, the number of days with connectivity disruptions (defined as outages recorded on at least two operators' networks simultaneously) rose from 69 in May to 662 in June, and reached 2,099 in July.

Mobile internet shutdowns spread far beyond border zones. Connectivity disruptions were recorded in central, southern, Siberian, and Far Eastern regions, including major cities and areas far removed from active combat, where the likelihood of drone strikes or immediate threats was minimal.

Authorities justified the restrictions as necessary to ensure citizens' safety and protect critical infrastructure. Official statements and regional press releases cited drone-related threats — this language repeated across relevant ministries, the Ministry of Emergency Situations, and Roskomnadzor, framing the shutdowns as temporary preventive measures in the public interest rather than access-restriction tools. Whether internet shutdowns actually improve counter-drone effectiveness remains a matter of expert debate.

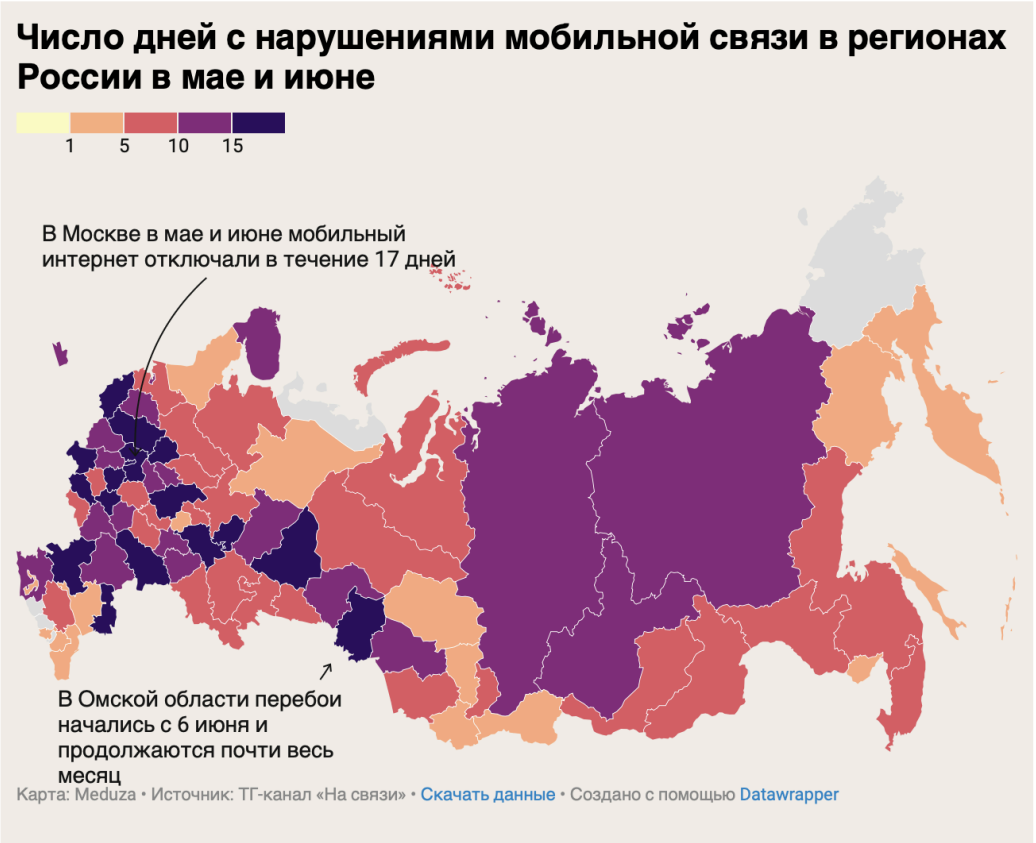
In practice, shutdown patterns varied widely: in some areas the internet disappeared entirely for hours or days; in others only Wi-Fi remained; in others access was preserved only to state-approved services (Russian banks, marketplaces, etc.) via whitelists. The logic governing which restrictions were applied was often absent. It is difficult to assess how far telecom operators' technical capabilities were coordinated with federal instructions or with any desire on the part of local administrations to minimize the harm from shutdowns — if such desire existed at all.

In Nizhny Novgorod Oblast, mobile internet disruptions were so frequent that in some municipalities access to mobile data effectively disappeared for extended periods. The region was repeatedly cited in media coverage and monitoring reports as an example of mobile internet ceasing to be a guaranteed service.

The North Caucasus was among the earliest adopters of shutdown practices, back in late 2024, when large-scale disconnection from the "unfriendly" segment of the internet was recorded in Dagestan, Chechnya, and Ingushetia, lasting at least 24 hours — as documented in RKS Global's 2024 report. Throughout 2025, connectivity instability in the region persisted under the pretexts of counter-terrorism and national security.

Data and users testimony confirm that by year's end, local shutdowns had ceased to be episodic: regular mobile internet restrictions were recorded in 80% of Russian regions, and according to experts, by late December the number of documented regional outages ran into the thousands across the country.

Na Svyazi documents numerous accounts of connectivity failures across regions — among them: the hamlet of Krasivo in Belgorod Oblast, which has no fixed-line internet connection and whose residents found themselves completely cut off from the outside world during shutdowns; Izhevsk, where shutdowns failed to prevent drone strikes but did prevent residents from receiving emergency alerts and taking shelter; and Ulyanovsk Oblast, where authorities were considering making temporary connectivity restrictions permanent.



In early 2026, Russia's Federal Security Service (FSB) was granted the authority to block communications even outside situations of active security threat, streamlining the decision-making process for internet shutdowns. The conditions for such blocks were to be determined exclusively by the president. The new law established a legal basis for mass, immediate disconnection of any communications services — including mobile and fixed-line internet, phone calls, email, and more — and exempted telecom operators from liability for losses incurred by subscribers as a result.

According to experts, Russia ranked first globally in internet shutdowns in 2025. Over the year, the internet was unavailable in Russia for a combined total of 37,166 hours, costing the economy nearly $12 billion — given how heavily modern business depends on internet infrastructure. This represents the largest economic damage from internet shutdowns of any country in the world, and the third consecutive year Russia has led this ranking.

9. Whitelists and Greylists

If regional shutdowns were 2025's most visible internet phenomenon, whitelists make the situation even worse. When whitelists are activated, access is preserved only to a pre-approved set of services, while all other traffic is blocked. The logic of blocklists, or blacklists is "only what is prohibited gets blocked"; the logic of whitelists is "only what is permitted works."

The whitelist mode is technically the inverse of the familiar blocking model. In the standard registry-based scheme, traffic passes through by default, and connections to specific IPs or domains are cut via DPI or access control lists (ACL). In the allowlist model, all external traffic is blocked by default, except for a pre-defined set of domain names, IP subnets, or autonomous system numbers (ASNs).

This scheme does not require individually adding each prohibited resource to a registry. The operator simply receives a list of permitted addresses and applies a policy of rejecting all traffic outside that list. From an engineering standpoint, this is a standard traffic segmentation mechanism — the kind used in corporate networks or emergency operating modes. The difference is that what was once an emergency mode has now begun to be applied to mass civilian users.

The idea of whitelists was first publicly announced by Minister of Digital Development Maksut Shadayev in August 2025. He promised that the list would include "all resources necessary for daily life."

The Ministry of Digital Development published the first version of the whitelists on September 5. It included: Gosuslugi (the state services portal), digital platforms Yandex, VKontakte, Odnoklassniki, Dzen, Rutube, Mail.ru, the MAX messenger, marketplaces Ozon, Wildberries, and Avito, the Mir payment system website, government and presidential administration websites, the remote electronic voting platform, and the telecom operators Beeline, MegaFon, MTS, Rostelecom, and T2.

Media outlets and Telegram channels subsequently published their own versions of whitelists, but an official, definitive list of sites that remain accessible during shutdowns was never published. The absence of clear rules means that socially important services may be left off the list, while for commercial services — especially small ones — being inaccessible during internet outages can be financially ruinous.

In March 2026, whitelists were activated in Moscow, St. Petersburg, and surrounding regions, with reports of connectivity losses by district, restricting access to everything except approved sites.

Anticipating which resources — beyond basic information services — residents will need during a shutdown is no simple task. A company managing public toilets in Moscow requested that its payment system be added to whitelists, after users encountered problems during outages. In St. Petersburg, public transport temporarily became free because the fare payment system predictably stopped working when the internet went down.

Alongside whitelists, "greylists" emerged in the Russian internet in 2025. This term describes a state of internet restriction in which there are no formal hard blocks, but services work unreliably: connections drop, specific functions (such as calls) disappear, and speeds fall sharply. Such conditions were documented for messaging apps and video platforms and discussed as an example of managed degradation without an official ban.

For analytical tools, greylists look like selective filtering or throttling of specific traffic types rather than full domain blocking. It is precisely the combination of these two mechanisms — narrowly restricted connectivity through whitelists and degradation through greylists — that is gradually shaping a distinctly Russian model of internet censorship, different from those of China and Iran.

Predictions that Russia might shift toward a model of "only approved content works" were previously treated as an extreme scenario for the TSPU infrastructure. In 2025, that scenario began to materialize in practice — first and foremost in mobile networks during regional restrictions. The Russian internet is following the worst-case trajectory, becoming a controlled environment with strict access controls over both content and connectivity itself.

10. Roskomnadzor vs. VPN: A Game of Cat and Mouse

The official ban on distributing information about circumvention tools has not worked: demand for VPNs is growing in proportion to restrictions. In turn, the restrictions only tighten. Government officials periodically reassure citizens that "introducing fines for VPN use is not planned and not even under discussion." Experts, however, consider this a quite realistic scenario.

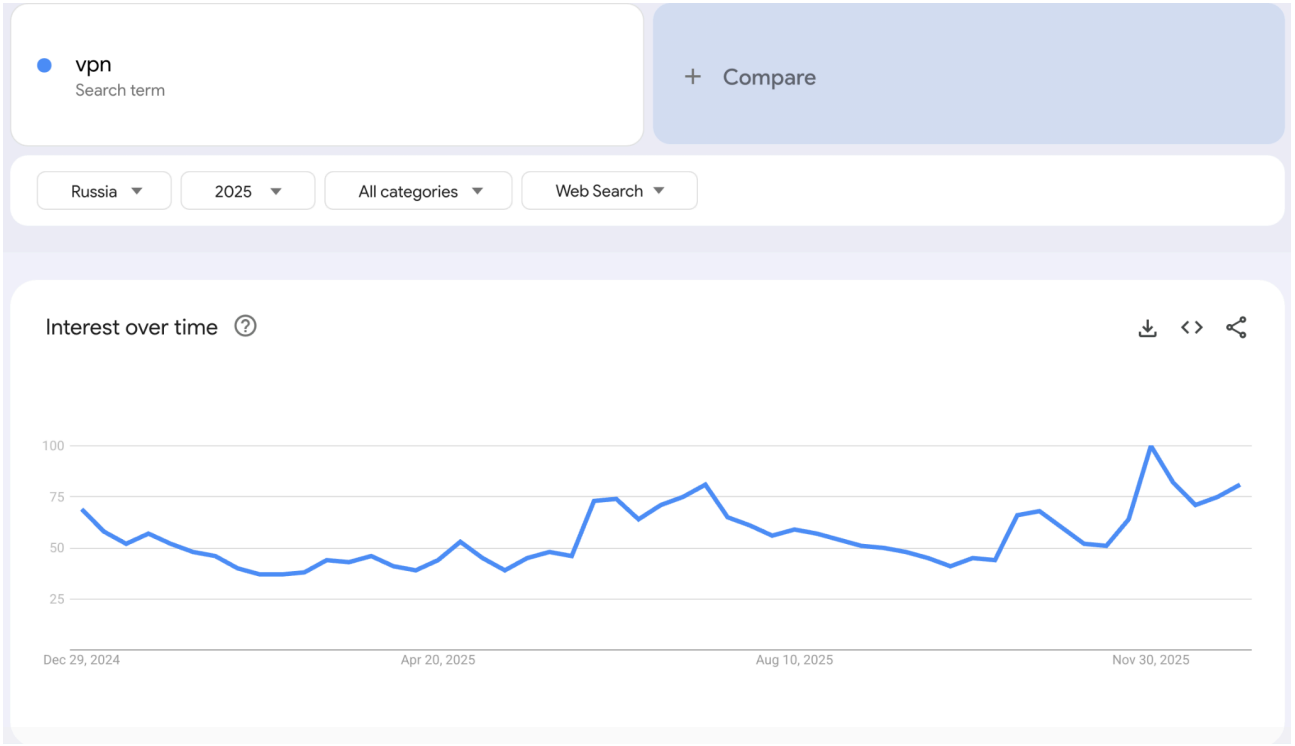
Shifts in the Anti-Censorship Market

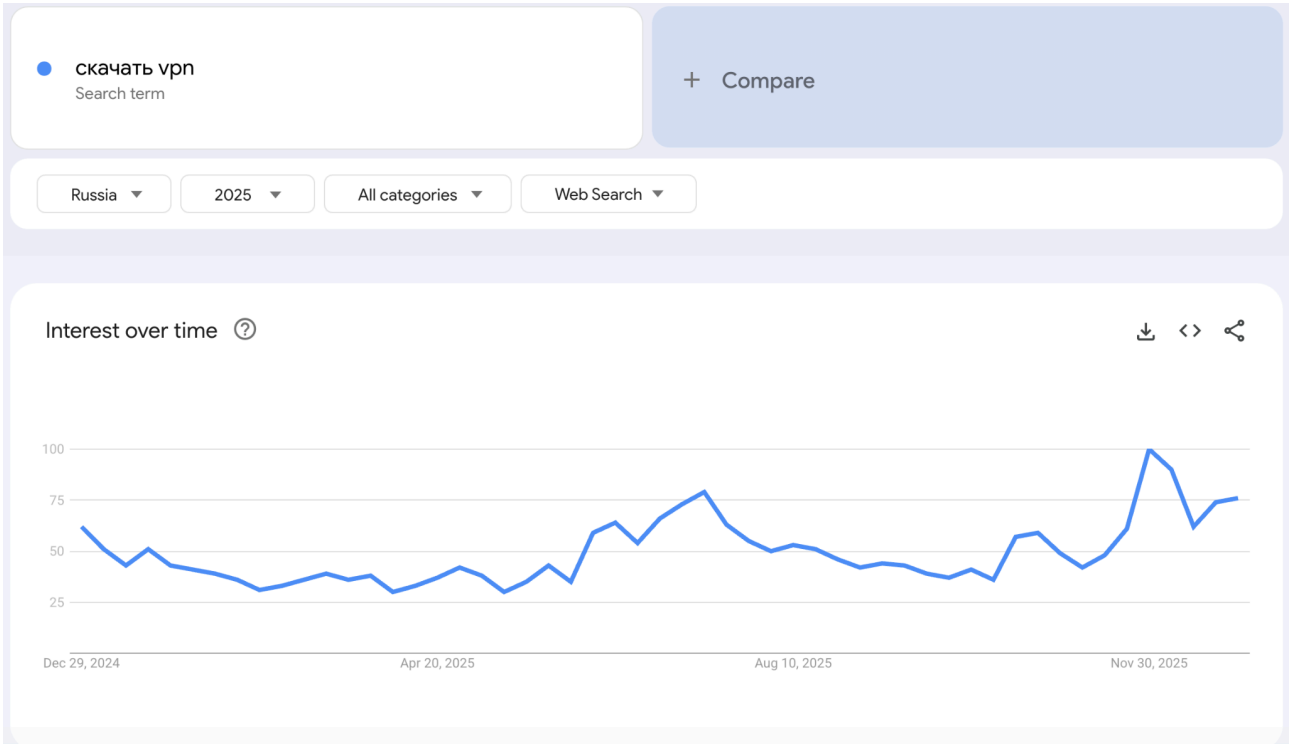
VPN services became the primary tool for restoring access to popular resources and messaging apps blocked by Russian authorities. The circumvention market grew rapidly throughout 2025. According to rough expert estimates, up to half of internet users in Russia use VPNs, with most opting for paid versions. Surveys paint a similar picture: two in five people actively use VPN services, and Russians' awareness of circumvention technologies rose to 74% between 2024 and 2026.

According to a Levada Center poll from March 2025, the most active VPN users were young people, more educated and financially secure respondents, and those with opposition political views. Kommersant cited Sensor Tower data showing that by late 2025, the active user base of the top five VPNs in Russia stood at 7.3 million, while over the 12 months from March 2025 to March 2026, total VPN installs reached 35.7 million, according to Digital Budget.

BlancVPN reported that more than 50 petabytes of traffic passed through its servers in 2025 — roughly equivalent to 10 billion high-resolution photos or 13 million 4K films.

Google search query frequency also rose throughout the year. Interest in the query "vpn" began climbing in the first days of May 2025 — precisely when the first local shutdowns, timed to Victory Day, occurred. Searches for "download vpn" and similar terms likewise spiked during periods of messenger blocks and other restrictions.





Google trends of the "vpn" and "download vpn" search terms in Russia in 2025

Unsafe VPNs

Against the backdrop of unprecedented VPN demand in 2025, a proliferation of scam services appeared — some impersonating well-known VPNs, others existing only briefly before disappearing. On one hand, each time Roskomnadzor blocks a VPN service or protocol, new services emerge relatively quickly; on the other, the quality of these products is often left to wonder.

Meanwhile, blocking in Russia is severe enough that any service — from a self-hosted VPN server for a small community to a major commercial product — can stop working at any moment. People download and install several VPNs at once, and among them are sometimes unvetted services that happen to be working.

Free VPNs carry elevated risk. Development and maintenance costs money, and creators may sell user data to advertisers. Sometimes a free VPN is simply a wrapper for malware or spyware.

In mid-2025 it emerged that in Iran — another country with severe internet censorship — a program distributed under the guise of a VPN was collecting users' messages, contacts, location, and other data and transmitting it to the Ministry of Intelligence and Security. No such cases have been documented in Russia so far, but there are indications that the two countries exchange censorship and surveillance practices with each other.

In July 2025, government officials proposed creating a "state VPN." According to them, such VPN would allow access to foreign resources that have themselves restricted access for Russian users — citing foreign medical journals as an example — along with services like Microsoft and Booking.com, though voluntary departures from the Russian market are actually fewer in number than outright bans. Furthermore, there is little reason to expect a state VPN to encrypt user traffic from the state itself, meaning all user activity would be visible to the authorities.

In a study conducted between October and December 2025, RKS Global experts found that nearly 20% of the most downloaded free VPN apps in Russia were linked to Russian internet infrastructure. Sixteen of 87 apps used Yandex Metrica, and one service was even sending data to its own servers in Russia. Under the Yarovaya Law, any data transmitted to Russia can be provided to law enforcement on demand at any time.

Constant VPN failures, services going down, the need to find replacements, pay again for access, or download risky free alternatives — all of this adds up to a deeply negative user experience. Which suits the authorities, who are intent on discrediting VPN technology as such.

VPN as an Aggravating Circumstance

A law making VPN use an aggravating factor in criminal offenses was signed in late July 2025 and came into force on September 1. Also, an amendment to Article 63 of the Criminal Code introduced enhanced penalties for crimes committed using "hardware-software means of accessing information resources and information-telecommunications networks to which access is restricted (VPN services)." Authorities claimed that personal VPN use was not being criminalized.

As it turned out, that was not entirely accurate. In December 2025, Tula Oblast saw the first conviction in which VPN use featured as an aggravating circumstance. The ruling stated that the defendant, "using hardware-software means of accessing information resources and information-telecommunications networks to which access is restricted, accessed the internet, where on a website he found a mixture containing a narcotic substance."

Also signed in July — and entering into force on September 1, 2025 — was a law introducing fines for advertising circumvention tools. Under it, advertising VPN services can result in fines of 50,000 to 80,000 rubles for individuals, 80,000 to 150,000 for officials, and 200,000 to 500,000 for legal entities.

But enforcement for VPN advertising began even before the law passed. In January 2025, Russia's Federal Antimonopoly Service declared an advertisement for a VPN service posted in a Telegram channel "improper" on the grounds that the channel owner had included links to online services.

In July 2025, Russian authorities required VPN service owners to cooperate with Roskomnadzor and created yet another registry for compliant providers. Cooperation presumed that services restrict access to resources banned in Russia — which would render VPNs essentially pointless for their primary use case (they would still offer privacy benefits, but circumvention of blocks is far more relevant to Russian users than privacy per se). Refusal to comply meant fines and subsequent blocking of the service itself.

The only VPNs for which such a registry might be useful are corporate ones, used for remote employee access. If they comply with the regulator's requirements, they can be relatively confident of avoiding blocks. When Roskomnadzor blocks VPNs at the protocol level, all services are affected because they operate on the same principles — but compliant corporate services are generally left untouched.

Earlier, Roskomnadzor's website published a recommendation for "owners of Russian private virtual networks" to abandon foreign encryption protocols "used, among other things, by applications providing access to prohibited information" — or, if that was not possible, to submit the IP addresses of their VPN servers for inclusion in a special exceptions list. Natalya Kasperskaya, president of InfoWatch Group — a company closely aligned with the state — noted that handing IP addresses to Roskomnadzor essentially means those addresses will likely be hacked or leaked, causing foreign services (GitHub and others that developers depend on) to see them and simply block access.

Blocking VPN Protocols

VPN service representatives describe working under conditions of constant pressure. Predicting what obstacles developers and users will face tomorrow is impossible: the situation changes very rapidly.

The logic of protocol-level blocking is described in Chapter 4.

According to DPI Detector data, throughout 2025 the popular protocols Shadowsocks, WireGuard, and OpenVPN were mass-blocked on mobile networks and partially on home broadband across almost all regions of the country. Intermittent problems with Cloak were also recorded.

From May 2025, attempts to block XRay (REALITY) and SOCKS5 on home internet were recorded across various operators in several regions. The peak came between June 4 and 16, when the majority of protocols were blocked on home broadband — partially coinciding with the onset of hosting provider blocks in Russia. In August, a major disruption affected OpenVPN, Shadowsocks, AnyConnect, and Cloak on home internet in St. Petersburg, Leningrad Oblast, and Pskov Oblast.

From autumn 2025, the functioning of most VPN protocols in Russia was significantly impaired by the active rollout of whitelists. Shadowsocks, WireGuard, and OpenVPN — still widely functional at the start of the year — had stopped working or were working intermittently. Experts noted that when other protocols experienced disruptions, connecting via XRay (VLESS+Reality) had previously served as a reliable fallback — but from November onward, it too came under partial blocking.

The distinctive feature of VLESS+Reality is that it conceals the very fact that a VPN is being used, disguising VPN traffic as ordinary HTTPS traffic. VPN Guild published

a statement urging VPN users and media not to panic over the VLESS blocks, since "censors can make access harder for certain user groups, but they cannot fully control these technologies." By early December, XRay functionality had gradually been restored.

In July 2025, the Amnezia team released a new version of its AmneziaWG protocol, designed specifically for use in the most censorship-hostile environments. In AmneziaWG version 1.5, traffic is disguised to resemble the most common UDP protocols (QUIC, DNS, and others). However, the developers themselves noted that "obfuscation dosn't always work": DPI systems have learned to identify even obfuscated protocols through statistical analysis and behavioral pattern recognition. In early 2026, AmneziaWG 2.0 was released, making traffic even harder to detect through constantly shifting packet headers and sizes.

The technological arms race demands resources that censorship agencies have in vastly greater supply. Even major providers such as NordVPN and Surfshark are not prepared to absorb the costs of this confrontation indefinitely. But state expenditure is rising too. According to calculations by The Moscow Times, since 2022 the Ministry of Digital Development, Roskomnadzor, and other government bodies have signed contracts worth 35 billion rubles for information restriction and blocking operations — 12 billion of that in 2025 alone.

Beyond the protocol-level blocking described above, Russian censors employ other methods. VPNs are blocked by signature — TSPU systems scan for any recognizable signs of VPN use, including traffic patterns, headers, encryption characteristics, and typical packet structures. Statistical methods are also used: if too much traffic passes through a single server, censors infer it is being used for VPN purposes and eventually block those IP addresses. Additionally, censors conduct "test purchases" from specific VPN services, analyze how they work, and proceed to block their servers.

11. Alternative Circumvention Tools

VPN is the most widely used censorship circumvention tool, but that popularity also makes it the primary target of surveillance agencies. There are, however, other ways to access the open internet, and many of them require no particular technical expertise.

Most independent media outlets launched email newsletters before Telegram was even blocked. Experts advise setting up additional email accounts with Google, Proton, or Tuta — Russian email clients like Yandex Mail and Mail.ru may block unwanted senders, meaning messages might not even reach the spam folder.

Since newsletters struggle to accommodate full-length articles, some media outlets have revisited RSS feeds — a file format resembling plain text but with website markup, which automatically delivers new content to subscribers as soon as it is published. Users can receive the feed by email or install an RSS reader app and subscribe to multiple outlets' feeds.

Switching to unblocked alternatives is a more short-term solution: Roskomnadzor can block any messaging app or video call service without much difficulty, as it did with Google Meet and FaceTime. And it is unlikely that a French, Korean, or American service will make significant efforts to restore access in a country where its audience is relatively small, or where the service has no built-in anti-blocking features. Furthermore, not all such services meet basic security standards.

Delta Chat, for instance — a messenger built on email protocols — is resistant to blocking and has undergone security audits, though some users in Russia have experienced slow message delivery. The decentralized Matrix protocol also continues to function; rather than relying on a single central server, it runs on a distributed infrastructure of many servers. The newly popular imo, however, is not recommended for private communication.

Among social networks, only the least popular in Russia — such as Reddit and Mastodon — remain unblocked, and Reddit occasionally bans Russian users of its own accord. Mastodon is a decentralized social network built around servers rather than pages and profiles. Servers are organized by theme (technology, activism, regional topics), and a user with an account on one server can follow and read posts from users on others. Servers can be self-hosted on personal infrastructure. Roskomnadzor cannot block the entire network — it would have to block each server individually, as with the Matrix-based Element messenger mentioned above.

Another circumvention method is purchasing a physical or eSIM from a foreign carrier and enabling roaming. When a user goes online with a German or Serbian SIM card, their device registers on the network via international roaming and routes traffic through the card's home operator. This does not always work — some foreign SIM cards still connect through Russian networks — so it is worth researching the carrier's services and traffic routing practices before purchasing.

From 2025, several well-known circumvention utilities — notably the free tools GoodbyeDPI and Zapret — largely stopped working. Unlike a VPN, which creates a tunnel from the device to its server and then onward to the target site while

concealing the user's location, GoodbyeDPI and Zapret simply modified traffic packets: altering certain header formats, injecting false requests, and fragmenting packets to confuse TSPU equipment. But unlike a VPN, these tools did not encrypt traffic, meaning censorship hardware could still determine which resource was being requested.

At the same time, Roskomnadzor continues applying "elastic" blocks: a single prohibition order is used to block new links, mirrors, and pages as they appear, allowing the registry to be expanded in batches without initiating a new procedure each time. Even so, mirrors allow access — at least for a limited period.

In practice, it is very difficult for Roskomnadzor to permanently cut off all means of communication. When necessary, people find remarkably creative workarounds: after WhatsApp and Telegram were blocked, users communicated through fitness app chats, mobile game chat functions, Apple photo comments, Yandex Maps traffic reports, and Google Sheets.

12. Expanding Prohibitive Legislation

Lawmakers have shifted from restricting publications and penalizing the distribution of "undesirable", or “extremist” information to punishing its search and consumption. As the risks of online surveillance grow, VPNs are returning to their original purpose — not only bypassing blocks, but concealing the content of users' online activity from their internet provider and the state.

Banning the Search for Extremist Materials Online

Article 13.53 was added to the Code of Administrative Offences, under which deliberately searching for materials recognized as extremist and accessing them — including through circumvention tools — is punishable by a fine of 3,000 to 5,000 rubles. This means that liability now extends not only to authors, distributors, and platform owners, but to users who search for or open prohibited material. Such users can be identified through physical device inspections, browser and search history, or

through telecom operators if the user visits unencrypted sites (HTTP rather than HTTPS).

Experts interviewed by Roskomsvoboda said that operators can see which applications a user runs and which sites they visit — for example, through DNS logs. These amendments resemble the Belarusian model: the criminalization of consuming prohibited content and software.

In November 2025, the first administrative case for deliberately searching extremist materials online was opened against a resident of Sverdlovsk Oblast, who was fined approximately 3,000 rubles. According to one account, information about the violation was passed to the FSB by an unnamed telecom operator.

Banning Advertising with "Undesirable" and "Extremist" Organizations

From September 1, 2025, existing advertising bans — covering ads with "foreign agents," ads for circumvention tools, and distribution of technical or statistical information about VPNs — were extended to include advertising on resources designated as "undesirable" or "extremist," as well as on any blocked resource. The law covers advertising on Instagram and Facebook, which belong to Meta — designated by Russian authorities as an "extremist organization" and banned in Russia. Penalties apply both to placing new advertising and to failing to remove existing ads.

Violations are subject to the general provision under Article 14.3(1) of the Administrative Code: fines of up to 2,500 rubles for individuals, up to 20,000 for officials, and up to 500,000 for legal entities.

Within a few months, lawmakers proposed increasing the fines, observing that "it is obvious that a fine of 2,500 rubles deters no one — bloggers continue to post advertising on banned social networks." In October, the first fine for advertising on Instagram was reported: an unnamed "third party" complained about a blogger for content posted before the law came into force.

In 2026, this logic extended to major platforms that hold no extremist or undesirable designation but are simply under a blocking order. Telegram and YouTube became subjects of separate scrutiny. Russia's Federal Antimonopoly Service clarified that advertising on Telegram and YouTube is assessed by analyzing the content of the ad, the contract date, the publication date, and the date restrictions on the platform were introduced; the agency then announced a transitional period through the end

of 2026, during which penalties for advertising on these two platforms would not be enforced.

The advertising infrastructure is becoming ever more tightly bound to registries, platform status designations, and regulatory decisions — turning marketing business processes into yet another mechanism of pressure on independent media, bloggers, and circumvention services.

13. Toward Runet Isolation: Reducing Dependence on Global Infrastructure and Technology

In 2025, censors practice not total isolation of Runet but selective availability: throttling in some cases, functional degradation in others, and access permitted only via whitelist exceptions during shutdowns.

Selective availability has become the stable operating mode of Runet: censorship agencies disrupted services to the point of making them inconvenient to use. In the early stages of messaging app blocks, for instance, apps could still function without a VPN, but messages and media files were delivered with delays, VoIP calls failed to connect, or call quality dropped sharply.

That said, complete isolation remains difficult even as censors' toolset expands. Russia still depends on global content delivery networks (CDNs), cloud infrastructure, and cross-border connectivity, meaning that any pressure on infrastructure intermediaries rapidly produces collateral damage across a vast range of unrelated resources.

During regional mobile internet shutdowns, for example, partial connectivity was maintained through whitelists — but even in that mode, reliability was unpredictable: lists expanded and changed, and resources nominally designated as permitted did not always work.

14. Conclusions and Forecasts

All of the observations documented above aim to record the stages of digital censorship development in Russia in 2025. A retrospective review of censorship practices in Russia may be useful to researchers, journalists, digital activists, developers of anti-censorship tools, and ordinary internet users in Russia who wish to anticipate the likely course of events and prepare accordingly.

A year on from the publication of the first 2024 review, the internet situation in Russia has become even less predictable than before. Taking everything described above into account, experts consider the following developments likely:

1. The technological war that Roskomnadzor is waging against the free internet in Russia depends on how the military conflict between Russia and Ukraine unfolds.

   The economic dimension matters here: how Russia's budget will be allocated and reallocated under conditions of deficit, how much money will be directed toward censorship, and how efficiently those funds will be spent.

   Also significant is whether communications infrastructure — data centers, internet exchange points, relay stations, and so on — becomes a target of military strikes, what damage such strikes might cause, and how quickly recovery could occur.

2. The physical infrastructure of the Russian internet will in all likelihood continue to degrade. This is partly a function of underinvestment and insufficient domestic production capacity, and partly a consequence of sanctions and the prohibitive cost of parallel imports. Imports from China will likely not cover all needs.

   As a result, the situation around slowdowns and the degradation of global services will become even more opaque. It is increasingly unclear whether disruptions stem from ordinary equipment wear or from deliberate action by Roskomnadzor.
3. Infrastructure degradation means that new loads placed on it — through blocking, throttling, and connectivity disruption — may produce unpredictable effects. In March 2026, for instance, when a new major wave of Telegram blocking began, TSPU equipment at several nodes entered bypass mode, temporarily making blocked resources — including YouTube and WhatsApp —

accessible again. Such incidents may recur and become more frequent.

4. As the budget and infrastructure situation grows more complex, the state will seek to shift part of its censorship obligations onto businesses. In April 2026, Russian IT companies were already compelled to comply with a requirement to implement VPN surveillance on users' devices.

5. Internet shutdowns across various regions will continue — an extension of the degradation of connectivity that Russia began implementing in full in 2025.

6. Censors will continue their hunt for VPNs, targeting first the largest and most popular services. The goal is to inflict maximum damage and disconnect as many users as possible at once. Blocking of VPN servers, statistical blocking methods, and removal of apps from stores — primarily the App Store — will continue. The user experience will deteriorate further.

7. Since every VPN service will sooner or later come under attack and lose functionality for a period, a common user practice is emerging: running several VPNs and other anti-censorship tools simultaneously to maintain uninterrupted access to the open internet.

   Experts nonetheless stress that it is critically important to research any VPN before installing it, and to treat free solutions with particular caution. For guidance on reliable options, users can consult: vpnlove.org, vpnguild.org, vpnpay.io, and vpn-ru.net, as well as the recommendations at privacyguides.org and the Electronic Frontier Foundation's guide.

8. The risk of tightening legislation around the advertising and distribution of anti-censorship tools — and the potential introduction of penalties for using them — remains very much high.

9. Following the logic of import substitution and state control over services in Runet, realization of the "state VPN" idea likely be seen — a product that will receive regulatory preferences and be positioned as a legal alternative to other services, much as was seen with the MAX messenger.

This overview was compiled on the basis of open-source information, media reports, original research by the RKS Global team, and input gathered from digital rights experts. It incorporates data from VPN protocol blocking tests conducted by the DPIDetector project, made possible by volunteer node operators.

The report would not have been possible without drawing on the work of colleagues from the Roskomsvoboda, Tech Talk, Na Svyazi, OONI, VPN Guild, and Amnezia VPN teams. We extend our deep gratitude for their work and their efforts.