Report
on Human Rights Implications of VPN Censorship in Russia

January 2025

Authors: VPN Guild, RKS Global
Address for inquiries: info@vpnguild.org

Executive Summary

This report examines the role of Virtual Private Networks (VPNs) in Russia as a tool for protecting human rights and ensuring digital privacy amidst increasing government censorship and surveillance. VPNs are essential for protecting digital rights, particularly in authoritarian regimes where online censorship is prevalent.

According to UN Special Rapporteur David Kaye, VPNs safeguard personal privacy by encrypting internet traffic, preventing unauthorized access by governments, ISPs, and cybercriminals. This aligns with Article 12 of the Universal Declaration of Human Rights, which protects against arbitrary interference in private life. VPNs also enable access to independent information, helping users bypass government-imposed restrictions on media, human rights organizations, and activists.

In Russia, VPNs serve as a crucial bridge between the tightly controlled domestic internet and external sources of information. They allow users to access independent media and dissident content that has been labeled as “foreign agent” or “extremist” by Russian authorities. The European Court of Human Rights has repeatedly ruled against Russian laws restricting VPN access, recognizing them as violations of free expression under the European Convention on Human Rights.

Key Findings:

VPNs enable secure access to independent media, human rights organizations, and online platforms restricted by the Russian government. Encryption safeguards users from surveillance, aligning with international human rights standards, including UN resolutions on digital privacy. The European Court of Human Rights (ECHR) has repeatedly ruled that Russia’s internet censorship laws violate fundamental rights.

In 2025, Russia expanded its Deep Packet Inspection (DPI) technology, known as TSPU, to block VPN services at a national scale. Authorities now block VPN protocols directly (OpenVPN, IKEv2, WireGuard), making traditional circumvention methods ineffective. The government allocated 60 billion rubles ($600 million USD) in its 2025-2027 budget to further enhance VPN-blocking technologies.

In March 2024, a law banned the dissemination of VPN-related information, making it illegal to educate users about bypassing censorship. In November 2024, a new order extended the ban to scientific research and statistical data on VPNs. Strict penalties have been introduced for non-compliance, forcing further self-censorship.

Corporations such as Apple are involved in censorship efforts by complying with Russian censorship legislation. Despite officially withdrawing from Russia, Apple continues to dominate the smartphone market (~30% share). In 2024, Apple removed over 100 VPN applications from the App Store following demands from Roskomnadzor. Unlike other censored countries, such as China and Iran, Russia's large iPhone user base amplifies Apple's influence, making its cooperation with Russian authorities particularly harmful to free speech. Human rights groups have called on Apple to stop complying with Russian censorship, but the company has not responded.

The increasing restrictions on VPN usage in Russia represent a severe violation of digital rights, including freedom of expression, access to information, and online privacy. The government's technical, legal, and corporate measures to suppress VPNs are part of a broader strategy to control digital communication. These restrictions are supported by compliance policies of tech corporations which provide neither transparency nor accountability.

In an era of growing digital authoritarianism, ensuring unrestricted access to VPNs remains a global priority for safeguarding internet freedom and human rights.

How VPN Technology Works

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over the internet, allowing users to protect their online privacy and bypass censorship or geographic restrictions. VPNs hide the user's real IP address and route internet traffic through a remote server, making it appear as if the user is accessing the internet from a different location.

When a user connects to a VPN, their internet traffic is encrypted, meaning their data is scrambled into unreadable code. This prevents third parties (such as ISPs, governments, or hackers) from seeing what the user is doing online.

The VPN server assigns the user a new IP address, masking their real location and making it difficult for websites or authorities to track them. Also VPNs help users circumvent censorship by routing their traffic through a server in another country where access to certain websites is unrestricted.

VPNs use various tunneling protocols to securely transmit data, such as OpenVPN, WireGuard IKEv2/IPSec L2TP/IPSec and a number of custom ones.

VPN as a Human Rights Tool in the Digital Age

As highlighted in the report (A/HRC/29/32) of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, the expansion of mass digital surveillance by both corporate and state actors, coupled with increasing online censorship in states characterized by digital authoritarianism, has significantly restricted access to independent information and personal digital privacy. According to assessments by Freedom House and Reporters Without Borders, one of the most effective means of circumventing these restrictions and safeguarding digital rights is the use of Virtual Private Network (VPN) technology.

VPN technology encrypts a user's internet traffic, rendering it unreadable to third parties, including internet service providers (ISPs), government agencies, and cybercriminals. The application of encryption prevents the large-scale collection of personal data, a practice that contravenes Article 12 of the Universal Declaration of Human Rights (UDHR), which guarantees protection against arbitrary interference in private life. UN resolutions on the right to privacy in the digital age underscore the necessity of safeguarding such technologies to ensure the protection of human rights online.

In the context of the Russian Federation, VPN technology facilitates access to independent information, media content, and digital services that have been subject to state-imposed restrictions. Following the full-scale invasion of Ukraine, numerous independent media outlets, human rights organizations, and civil society groups were designated as foreign agents, extremist organizations, or undesirable entities, effectively curtailing their ability to operate within the Russian information space. As a result, VPNs remain one of the few viable tools for Russian citizens to access independent journalism and human rights reporting.

Moreover, VPN technology plays a crucial role in upholding the right to "seek, receive, and impart information and ideas through any media and regardless of frontiers", as enshrined in Article 19 of the UDHR. In an increasingly fragmented digital environment, VPNs serve as a critical gateway bridging the controlled domestic internet within Russia — under strict oversight by Roskomnadzor — with independent media and online platforms operated by Russian journalists and activists in exile.

Beyond its role in ensuring access to information, VPN technology is vital for the security and anonymity of human rights defenders, journalists, and dissidents operating under repressive regimes. Secure digital communications are essential for the protection of journalistic sources, a principle firmly established in international human rights law and press freedom standards.

International soft law frameworks emphasize the importance of ensuring widespread access to VPN technology. The European Court of Human Rights (ECtHR) has ruled on several occasions that restrictions on internet access must meet strict necessity and proportionality criteria. In Engels v. Russia, the Court noted that prohibiting the use of technology to bypass censorship

cannot be justified solely on the basis that such tools might facilitate access to illegal content. The judgment reaffirmed that VPN technology serves numerous legitimate purposes, such as ensuring secure remote access and improving internet connectivity.

The ECtHR has consistently ruled against Russia's legal framework on internet restrictions, including in the cases of Kablis v. Russia, Engels v. Russia, Flavus and Others v. Russia, Kharitonov v. Russia, and Bulgakov v. Russia. These rulings highlight the legal ambiguity and overbroad nature of Russia's information control policies, which are found to be inconsistent with Article 10 of the European Convention on Human Rights (ECHR). The Court further observed in Engels v. Russia that "*Suppressing information about the technologies for accessing information online on the grounds they may incidentally facilitate access to extremist material is no different from seeking to restrict access to printers and photocopiers because they can be used for reproducing such material. The blocking of information about such technologies interferes with access to all content which might be accessed using those technologies.*"

In 2022, the United Nations Human Rights Committee expressed concern over reports of widespread internet restrictions, including the blocking of thousands of websites, digital platforms, and independent news outlets. The Committee urged the immediate repeal of laws that impose undue restrictions on freedom of expression and access to information.

Given the increasing scope of digital censorship and mass surveillance, VPN technology is no longer merely a tool of convenience but a fundamental instrument for preserving democratic values and freedoms in the digital age. Its role in ensuring privacy, security, and open access to information is essential to upholding the human rights commitments outlined in international treaties and human rights frameworks.

VPN Blocking via TSPU

In 2025, the Russian authorities significantly escalated technical measures aimed at blocking VPN services through the deployment of a Deep Packet Inspection (DPI) system known as TSPU (Technical Threat Countermeasures). This system enhances the state's ability to enforce large-scale censorship by identifying and filtering various types of internet traffic.

Key developments in the implementation of TSPU include:

- Centralized Management: The TSPU system, while installed across all internet service providers (ISPs), operates under centralized control by Roskomnadzor, enabling the rapid and coordinated implementation of censorship measures. The system can detect

and filter specific traffic types, including Server Name Indication (SNI) fields and QUIC traffic, thereby increasing the efficiency of VPN blocking.

- TLS-Level Blocking: A significant portion of VPN traffic is now blocked at the Transport Layer Security (TLS) level, making it considerably more challenging for users to bypass restrictions. This method disrupts encrypted connections, affecting the reliability of traditional VPN services.
- Automated Blocking Mechanisms: Internet service providers have adopted automated blocking systems, enabling them to detect and restrict access to new website mirrors within minutes. This automation renders conventional circumvention techniques ineffective and further limits users' ability to restore access to restricted content.
- Blocking of VPN Protocols: According to the public report by Roskomsvoboda, titled *"VPN in Russia: From Blocking Services to Blocking Protocols"*, Roskomnadzor has shifted from blocking VPN-related information to directly targeting VPN technology itself. Since 2023, Russian authorities have expanded their censorship efforts by blocking VPN applications and protocols on major ISP networks. In addition to blocking IP addresses and domains associated with VPN providers, Roskomnadzor has successfully restricted VPN protocols, including OpenVPN, IKEv2/IPSec, and WireGuard, thereby disrupting VPN functionality across all major internet providers in the country.

These measures represent a systematic escalation of state-led efforts to control digital access, further undermining freedom of expression, privacy, and the right to access information, in violation of international human rights standards.

One of the most effective solutions for maintaining VPN functionality in Russia has been the AmneziaWG protocol, developed by the Amnezia team. This protocol is a modern adaptation of the WireGuard VPN protocol, designed to evade detection by Technical Threat Countermeasure (TSPU) systems while maintaining the simplified architecture and high performance of the original WireGuard.

Another notable protocol is VLESS, which has demonstrated consistent functionality even under the constraints of the "Sovereign Runet" system, including in testing conducted in the North Caucasus region. Under Russia's current blacklist-based regulatory framework, it is significantly more challenging to block services using such obfuscation protocols. These protocols disguise VPN traffic as regular internet activity, operate without traditional connection establishment procedures (handshakeless technology), and employ advanced evasion techniques to bypass TSPUdetection mechanisms.

At the same time, the Russian government has substantially increased funding for its efforts to counter VPN services. For the first time, the 2025–2027 state budget includes an allocation for "network sovereignty," with 60 billion rubles (approximately 600 million USD) designated for Roskomnadzor's anti-VPN initiatives. These funds will be directed toward:

- Modernizing Technical Threat Countermeasures (TSPU) across all telecom operator networks.
- Expanding internet traffic filtering capabilities to disrupt VPN operations.
- Implementing automated systems to block and “slow down” restricted resources.

According to official documentation, these measures aim to enhance the efficiency of VPN-blocking mechanisms to 96%, marking a significant escalation in state-led digital repression efforts. These developments raise serious concerns regarding the right to privacy, access to information, and freedom of expression, as enshrined in international human rights standards.

Ban on Information about VPNs

On March 1, 2024, a new law came into force in Russia, prohibiting the dissemination of information on methods to bypass internet restrictions, including the use of Virtual Private Networks (VPNs). This legislative measure represents a significant escalation in state-imposed restrictions on digital rights and access to information.

On November 20, 2024, an official order was published on the government’s legal acts portal, coming into effect on November 30, 2024. This order expanded the criteria for classifying information as prohibited. Under the new provisions, Roskomnadzor extended restrictions to include the dissemination of scientific, technical, and statistical information on VPN technologies, further reinforcing censorship mechanisms. The only exception is for VPN-related information intended for secure remote access in professional and governmental settings.

These legislative restrictions have fostered a climate of fear and self-censorship, particularly among citizens, journalists, bloggers, and independent media organizations.

Key Provisions of the Law:

- Prohibition on VPN-related information: It is now illegal to share or popularize VPN technologies as a means to circumvent censorship. This includes scientific, technical, and statistical research on VPN services.
- Penalties for non-compliance: Companies and individuals face significant fines for failing to remove prohibited information on VPN services.
- Blocking of online resources: Websites that distribute VPN-related content are subject to immediate blocking by state authorities.

These measures constitute a direct violation of international human rights obligations, particularly regarding freedom of expression, access to information, and digital privacy.

Apple's Censorship and Removal of VPN Services

Despite international sanctions and the company's official withdrawal from the Russian market, Apple Inc. remains a leading smartphone provider in the Russian Federation, accounting for approximately 33% of all smartphone sales in the country.

Throughout 2024, Apple engaged in the systematic removal of VPN applications from its App Store in Russia, significantly restricting users' ability to bypass state-imposed censorship. According to data from the GreatFire project, between June and September 2024, Apple removed approximately 60 VPN services, bringing the total number of deletions to over 100.

One of the most striking cases involved Amnezia VPN, whose developers received a midnight notification from Applestating that their application had been flagged by Roskomnadzor for removal. Within three hours, the application was no longer available on the Russian App Store. In October and November 2024, Apple also removed applications of independent media outlets, including Radio Liberty's regional publications "Sibir.Realii" and "Sever.Realii". Other independent media organizations, such as BBC, Meduza, and Dozhd, face similar risks of removal.

In response, human rights organizations, media representatives, and individuals affected by VPN censorship submitted an open letter to Apple CEO Tim Cook, outlining the reputational risks and human rights implications of the company's collaboration with Russian censors. To date, this letter remains unanswered.

While Apple maintains that its global policies are applied uniformly across all regions and that it complies with the local laws of the countries where it operates, the company's actions in Russia raise serious concerns regarding corporate complicity in human rights violations. Unlike countries such as China, Iran, and Myanmar, where state-imposed digital restrictions are widely recognized, Russia's substantial iPhone user base — accounting for approximately 30% of mobile devices — magnifies the societal impact of such corporate decisions.

Notably, the number of Apple smartphones in use in Russia continues to grow, despite the company's official exit from the market and a decline in iPhone retail sales within the country. This paradox underscores the significant role Apple plays in the Russian digital ecosystem and highlights the far-reaching consequences of corporate collaboration with authoritarian regimes in restricting access to independent information, freedom of expression, and digital rights.

Key Aspects of Apple's Compliance with VPN Censorship in Russia

- Removal of VPN Applications: As of November 2024, more than 102 applications have been removed from the Russian App Store, including widely used and effective VPN services such as Amnezia VPN, Red Shield VPN, ExpressVPN, NordVPN, ProtonVPN, and others.
- Restricted Access to Information: In addition to removing VPN applications, Apple's actions have contributed to limited accessibility of VPN-related information, making it increasingly difficult for users to obtain details about circumvention tools through search engines and app stores.
- Collaboration with Authorities: Apple has demonstrated swift compliance with Roskomnadzor's takedown requests, reportedly removing flagged applications within four hours of receiving official orders from the Russian authorities.

These measures raise serious concerns regarding corporate complicity in digital repression, reinforcing state-imposed censorship and undermining fundamental rights to privacy, freedom of expression, and access to information.

Conclusion

The VPN situation in Russia in 2025 presents serious human rights concerns, as the technical, legislative, and corporate measures implemented to restrict VPN usage constitute significant violations of fundamental rights, including freedom of expression, access to information, and privacy. Authorities are now considering the introduction of fines and legal penalties for individuals using prohibited VPN applications, further exacerbating digital repression.

In light of these developments, we call upon the UN Special Rapporteur on the situation of human rights in the Russian Federation, Ms. Mariana Katzarova, to:

- Conduct a comprehensive investigation into the described human rights violations.
- Include an assessment of the critical threat to VPN access in the Special Rapporteur's general report to the Human Rights Committee and the UN General Assembly.
- Engage in dialogue with Russian authorities to urge compliance with international human rights obligations related to digital rights and online freedoms.
- Consider the application of international human rights mechanisms to counter digital repression and censorship in Russia.
- Initiate joint efforts with thematic UN Special Rapporteurs to examine the role of technology corporations in violating the right to privacy and freedom of expression, as well as their compliance with censorship policies in Russia.

- Call on technology companies to uphold transparency, accountability, and human rights principles in their operations and to revise local compliance policies in countries with high levels of digital authoritarianism.

Ensuring the protection of digital rights in Russia requires coordinated international action. Only through joint efforts by the global human rights community, international organizations, and civil society can the fundamental freedoms of Russian citizens in the digital sphere be safeguarded.

VPN Guild

Empowering Secure and Open Internet Access

https://vpnguild.org

Contact us: info@vpnguild.org

VPN Guild is a newly established association dedicated to advocating for secure, private, and unrestricted internet access worldwide. Formed in response to increasing internet censorship, we unite VPN application developers committed to digital freedom.

We believe that VPNs are essential tools that help individuals bypass censorship, protect their privacy, and exercise their rights to freedom of expression and access to information. The removal of VPN apps not only infringes on these rights but also hampers the work of journalists, activists, and civil society organizations.

Our Mission

- **Protect Digital Rights**: Advocate for users' rights to freely and securely access information online.
- **Promote Transparency and Accountability**: Encourage technology companies to adopt policies that respect user privacy and freedom.
- **Strengthen Collaboration**: Unite stakeholders across various sectors to amplify efforts against internet censorship.

Key Initiatives

Advocacy and Coalition Building

We are forming alliances with international human rights organizations and expert networks. By bringing together VPN developers, human rights activists and cybersecurity experts, we aim to create a unified front to challenge internet censorship and promote digital rights.

Engagement with Technology Companies

A primary focus is addressing the role of major tech companies in enabling censorship. We are advocating for policy changes at gatekeeper companies like Apple and Google, urging them to resist unlawful government demands that infringe on human rights. Our efforts include research, open letters, and establishing ongoing dialogue to promote transparency and accountability.

Legal Action

Recognizing the power of legal avenues, we are exploring litigation options to challenge unlawful censorship practices. We aim to hold both governments and corporations accountable for violations of digital rights.

Capacity building

At VPN Guild, we believe in the power of collaboration and shared knowledge. By joining the association, members gain access to a network of professionals and organizations dedicated to internet freedom.

Get Involved

We invite VPN developers, cybersecurity professionals, human rights advocates, and all stakeholders committed to a free and open internet to join us. By becoming a member or partner of VPN Guild, you will be part of a crucial movement to defend internet freedom at a time when it is under significant threat. Your involvement will contribute to:

- **Protecting Fundamental Rights**: Support efforts to uphold the rights to freedom of expression and access to information.
- **Shaping Policy and Industry Standards**: Influence how technology companies operate and ensure they prioritize user rights.
- **Collaborating for Greater Impact**: Work alongside a network of experts and organizations to share experiences, foster partnerships and amplify our collective voice.