

Russia's Digital Crackdown

Oleg Loginov on the Kremlin's push for full control over Russia's internet

By Oleg Loginov

04 мая 2026

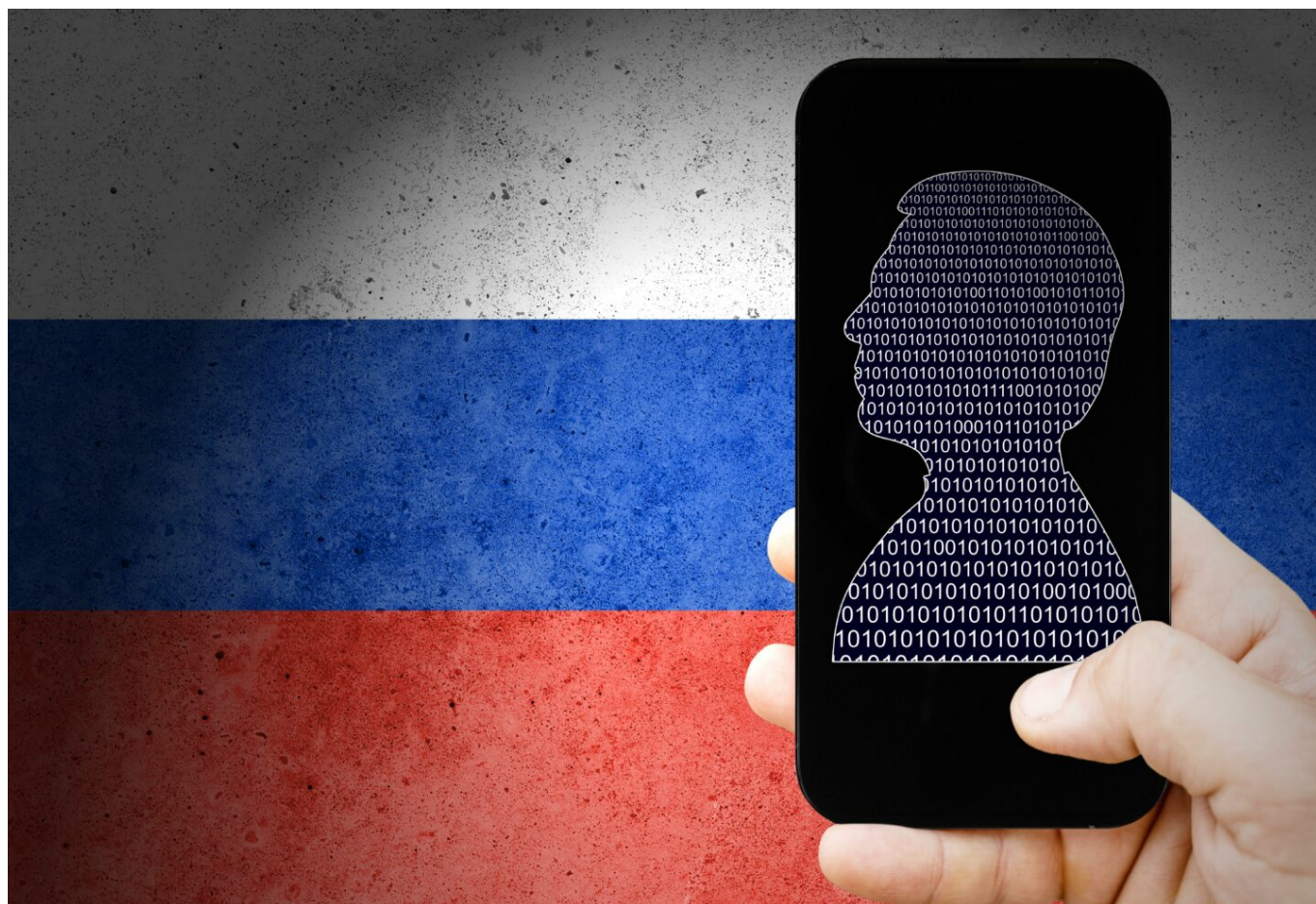


Фото: Scanpix

The blocking of Telegram, Russia's most popular messaging app; the forced rollout of Max, a state-backed alternative; a sweeping crackdown on VPNs involving the country's largest internet companies; and repeated, prolonged mobile internet shutdowns — including in Moscow — have hit Russian users almost simultaneously.

It increasingly feels as if Russia's internet is being rapidly transformed into «Cheburnet.» The term was originally a joke — coined when such a scenario seemed unthinkable. The authoritarian state's assault on digital rights has been underway for years. What is unexpected is this: these developments have triggered something resembling a public debate. The question is whether it can change the trajectory of this process — or at least slow it down.

«Core Restrictions»

On April 23, during a meeting with the government, Vladimir Putin [attempted](#) to explain what is happening to Russia's internet. He described the situation as «certain problems and disruptions.» The issue came up almost incidentally in discussions about Arctic connectivity.

Glancing at handwritten notes, the Russian president said the disruptions were caused by «operational work to prevent terrorist attacks,» which, as he put it, «we sometimes fail to stop.» By «sometimes,» he was most likely referring to regular Ukrainian drone strikes on Russian infrastructure, which the Investigative Committee of Russia classifies as acts of terrorism.

Putin's remarks point to a clear conclusion: these «problems and disruptions» are not going away, as priority will always be given to «ensuring people's safety.» At the same time, to limit inconvenience, security agencies are expected to show «ingenuity,» while the Digital Development Ministry must ensure that key services — government portals, payment systems, and medical appointment platforms — continue to operate even during what he called «core restrictions.»

In practical terms, this means refining the so-called «whitelist» — a limited set of websites and online services that remain accessible even during shutdowns. Sergey Anokhin, CEO of VimpelCom, one of Russia's largest mobile operators, first [proposed](#) the idea in autumn 2025, as outages became routine in some regions. The Digital Development Ministry later approved the idea, and all operators implemented it.

However, the system remains far from perfect. The issue is not so much expanding the «whitelist,» which currently includes [about 500 services](#), as improving its reliability. During a three-week shutdown in Moscow in March, even whitelisted services experienced [significant disruptions](#). Experts point to two [main reasons](#): overloaded traffic filtering equipment and the architecture of the services themselves. Many rely on external resources — such as mapping tools or analytics systems — that are not included in the whitelist. Both issues are technically solvable.

During his meeting with the government, Putin also instructed officials to inform the public about the shutdowns — but not in advance or during «operational work,» so that criminals cannot «adjust their criminal behavior,» but at least after the fact.

The following day, the FSB promptly fulfilled the president's request. The agency [reported](#) that it had prevented a terrorist attack against the leadership of Roskomnadzor a week earlier. Roskomnadzor is Russia's internet censorship regulator and formally reports to the Digital Development Ministry. According to the FSB, seven individuals described as «supporters of right-wing radical and neo-fascist ideology» had been planning «bombings and arson attacks on the vehicles of Roskomnadzor employees» to disrupt «measures to ensure the security of the information space, including the blocking of Telegram.» They allegedly received their instructions from Ukrainian intelligence services.

The human rights project First Department offered a [different account](#): the detainees were most likely linked to an anonymous movement known as «Scarlet Swan,» which [had called](#) for protests against internet restrictions in Russia. The group conducted a voice analysis of one of the detainees and found a «high degree of similarity» with the voice of Sofia Chepik, the administrator of a Telegram channel associated with the movement. [According to TV Rain](#), four members of the movement stopped communicating on the day of the arrests in Moscow, Ufa,

Novosibirsk, and Yaroslavl. One of them — a 20-year-old Muscovite — was killed during the arrest.

The FSB did not say whether mass internet shutdowns and the blocking of Telegram played any role in the operation. Judging by the available information, they did not. According to the FSB itself, the suspects were allegedly recruited via the very messaging app that had been blocked.

Who is driving the crackdown?

A [recent investigation](#) by The Bell suggests that the «problems and disruptions» in Russia's internet may have become more frequent following a change in oversight. Historically, telecommunications, the internet, and IT were overseen by the FSB's Information Security Center and its Scientific and Technical Service. However, about a year ago, Vladimir Putin transferred that responsibility to the FSB's Second Service — described as «the most hardline division of the agency, responsible for protecting the constitutional order from opposition and combating terrorism.» The immediate trigger for the decision was likely the Crocus City Hall attack in March 2024, when more than 150 people were killed and hundreds were injured in a mass shooting at a concert venue outside Moscow. Islamic State claimed responsibility. State media, citing case materials, [emphasized](#) that both the organizers and perpetrators had communicated via Telegram.

The internet restrictions, which shocked many Russians and appear to have dented Vladimir Putin's [approval ratings](#), were [described](#) by Digital Development Minister Maksut Shadayev as a «difficult compromise.» Announcing measures to «reduce VPN use,» he repeated the phrase. He also indicated that the alternative could have been the introduction of administrative penalties for using circumvention tools — a step he said he «categorically dislikes.»

The substance of this «difficult compromise» is already becoming clear. Major Russian internet companies are required to [identify users](#) who are using VPNs and restrict their access to services. Those who refuse to comply risk being excluded from the «whitelist.» Many services already stop working when a VPN is enabled. Mobile operators have also been required to [disable Apple ID top-ups](#) via phone billing — one of the simplest ways for iPhone users to pay for app subscriptions, including VPN services. In addition, [paid tariffs](#) for international traffic have been announced. Since VPN traffic is routed through foreign servers, users will be charged 150 rubles per gigabyte beyond a monthly limit of 15 GB.

The introduction of [administrative penalties](#) for bypassing restrictions has not been ruled out, although it remains unclear how such measures would work in practice. At the same time, the use of VPNs is already being treated as an aggravating factor in other offenses, and the first such [cases](#) have already emerged.

Trying to Reach Putin

Attempts by the Digital Development Ministry to soften the most radical proposals from the security services can be viewed through the lens of a [widely discussed theory](#) about divisions within the government. According to this view, there are two competing approaches to controlling the internet: a «civilian» one and a «security-driven» one. The theory is reinforced by statements from some [officials](#), [regional governors](#), [members of the State Duma](#), and [Kremlin-aligned media executives](#), as well as by [reports](#) that the presidential administration's political bloc opposes further restrictions. For now, the security-driven approach appears to be prevailing, although the outcome of the standoff remains uncertain. Supporters of the «civilian» camp hope that if Putin can be convinced that full «Cheburnetization» would do more

harm than good, he may step in to rein in the security services.

The same logic is evident in public statements by representatives of Russian IT companies, whose operations are directly affected by mobile internet shutdowns and blocking measures.

A particularly notable example was a [post](#) by Natalya Kaspersky, head of InfoWatch. Addressing what she described as the «uninitiated,» she made a simple but important point: while VPNs can be used to bypass restrictions, that is not their primary function. Their main role is to provide secure communication channels for organizations. Blocking the services through which users access platforms like Telegram or YouTube inevitably affects critical infrastructure, already leading to disruptions in the banking sector: customers are experiencing problems with payments, transfers, and even cash withdrawals at ATMs.

There are no precise estimates yet of the damage caused by shutdowns and blocking measures, but rough calculations are striking. According to experts [cited](#) by Kommersant, the three-week shutdown in Moscow in March alone cost businesses 0.6–1 billion rubles per day. Over 19 days, total losses amounted to around 19 billion rubles.

Kaspersky and the heads of several Russian IT companies, members of the Association of Software Developers (ARPP), later laid out the risks of the restrictions in a [letter](#) to Prime Minister Mikhail Mishustin and Anton Vaino, head of the presidential administration. In addition to disruptions across a wide range of consumer and corporate services, the crackdown on VPNs is also hampering the development of Russian software. Developers rely on VPNs to access foreign repositories — online platforms hosting software code and libraries — many of which restrict access from Russia. For example, Microsoft-owned platforms GitHub and GitLab are [inaccessible](#) to users from Russia. The authors of the letter also noted that the «deterioration of the political climate» is causing frustration among IT professionals and prompting thoughts of emigration. At the same time, they wrote, «they do not feel tied to their country and can easily find work anywhere in the world.»

The evolution of internet restrictions in Russia

It is reasonable to assume that Vladimir Putin is not deeply involved in the technical details of internet restrictions, may not even know what VPN stands for, and has only a superficial understanding of the challenges facing IT companies. That is most likely the case. He may even have a distorted view of the success of the state-backed messaging app Max: its press service recently [claimed](#) 77 million daily users and 107 million registered accounts — [roughly the same](#) as Telegram had before it was blocked. The credibility of these figures is [open to question](#).

Even so, it is hard to believe that the president is entirely detached from what is happening and has delegated all decisions to the security services. If only because the current campaign is not an impulse, but the logical continuation of a process that began long before the change in oversight of the Russian internet.

The starting point can be traced to the [adoption](#) of the so-called Yarovaya law package in 2016. At the time, telecom operators and internet companies were required to store user data, hand it over to security services, and assist in decrypting traffic. As today, these restrictions — including the effective removal of citizens' right to privacy of correspondence — were justified by the need to combat terrorism. In 2019, the «sovereign internet» [law](#) was adopted (its development was [overseen by Andrey Lipov](#), now head of Roskomnadzor). The law laid the foundation for the National Domain Name System, a Russian network of DNS servers. Formally, it was designed to ensure that the Russian segment of the internet could continue functioning even if disconnected from the global network. In practice, however, this infrastructure is now

used for blocking. The law also required providers to install so-called TSPU (technical means of countering threats) — equipment that allows Roskomnadzor to reroute, slow down, and block internet traffic centrally.

In the early stages, the authorities' censorship ambitions repeatedly ran up against technical constraints. The Yarovaya package was not implemented immediately, as the country [lacked](#) the necessary equipment to store user data. [Similar problems](#) arose with the «sovereign internet» law. The most high-profile failure was the attempt to block Telegram in 2018–2020, when the app's founder, Pavel Durov, [openly mocked](#) Roskomnadzor. These setbacks contributed to a perception that the restrictions were not serious, with regulators appearing ineffective.

Over time, however, those capabilities steadily expanded. Demand for surveillance and blocking tools helped drive the growth of a major industry. IX Holding, its flagship company and a major tech group with close ties to the FSB, [has become](#) one of Russia's largest IT companies in terms of revenue. The group's turnover rose from 91 billion rubles in 2022 to 260 billion rubles in 2024. It has consolidated key manufacturers of traffic-filtering equipment, produces base stations for telecom operators, and is involved in efforts to build a Russian alternative to Starlink.

As a result, following the start of the full-scale war in Ukraine, when most major Western services were blocked in Russia, Roskomnadzor no longer looked ineffective.

«Digital Resistance»

Viewed in retrospect, further tightening of control over Russia's internet — including continued pressure on VPNs — appears the most likely path.

The same conclusion can be drawn from the government's published plans. By 2030, the Digital Development Ministry [aims to increase](#) the capacity of the TSPU system by 2.5 times, to 954 Tbps. For comparison, average traffic across Russian networks in 2024 was only about 30 Tbps per day. Such a massive capacity buffer is clearly intended to support efforts to counter circumvention tools, as processing traffic masked by VPN services requires significantly greater computational resources.

Notably, the principle of «sovereignty» is now extending to the regulation of artificial intelligence. A recently introduced bill [requires](#) developers to train models exclusively on Russian data and infrastructure. Businesses [warn](#) that this will drive up costs and reduce efficiency, but the state is clearly prioritizing control over efficiency. Sber, which is positioning itself as a leader in AI in Russia, operates along the same lines: its models are [described](#) as «fully Russian, down to the nuts and bolts.»

At the same time, the process may accelerate, slow down, or periodically stall — including due to technical constraints. Businesses, already accustomed to operating under restrictions, would prefer a more gradual and predictable process. That, in essence, is what the current public debate is about.

The ARPP does not propose abandoning further restrictions on VPNs altogether, but rather creating a dedicated body to develop a more balanced policy on VPN blocking. Such a body could draw on international experience. For example, China began restricting VPN services more than a decade ago. Initially, the measures [harmed](#) local businesses, but over time, the authorities developed a system more workable for companies: firms can access the global internet only with special authorization. Roskomnadzor has, in effect, [already responded](#) to the ARPP's proposal: the use of corporate VPNs will not be restricted. The current focus is on limiting [private use](#)

of such services.

However, VPN services that remain committed to the Russian market and continue to invest in new ways to bypass restrictions are [still operating](#). The good news for users is that full isolation of the Russian internet is unlikely. The audience for Russia's internet is large enough to make continued investment worthwhile for VPN providers. At the same time, stable and fast connections [are not guaranteed](#). To ensure reliable access to blocked resources, users will likely need to subscribe to multiple services.

Life in a state of «digital resistance,» as Pavel Durov has put it, is inherently uncomfortable. That persistent friction will gradually push users toward Russian alternatives to blocked services. A [planned ban on advertising](#) in Telegram and YouTube — postponed until the end of 2026 — will reinforce that shift, forcing Russian bloggers and brands to move more actively to platforms such as Max and VK Video, a state-controlled YouTube alternative.

For emergencies, the authorities already have a well-tested shutdown mechanism, under which only a pre-approved «whitelist» of services remains accessible. The technology is likely to continue evolving. For example, Russian specialists [are reportedly](#) refining these systems in Iran, helping local authorities build out their internet censorship infrastructure.

