The State of the Internet and Digital Rights in Russian Federation (2019–2025)

The report provides a comprehensive analysis of the transformation of the Russian internet space over the past six years. The document examines in detail how, under the guise of "protecting sovereignty" and "combating threats", Russia has systematically built one of the most complex and multi-layered state censorship systems in the world. From legislative initiatives such as the "sovereign internet law" to the creation of a sophisticated technical infrastructure for deep traffic filtering (TSPU) — the report consistently reveals the mechanisms that laid the groundwork for unprecedented control over the digital sphere.

The year 2025 became a turning point when the theoretical capabilities of the control system were applied in practice on an unprecedented scale. This report sheds detailed light on the key events of this year: the shift from blocking individual resources to mass mobile internet shutdowns in dozens of regions of the country, which turned from an emergency measure into a routine tool. Moreover, the document analyses a qualitatively new stage of censorship — the introduction of so-called "whitelists", which fundamentally change the very paradigm of access to information according to the principle "everything that is not permitted is prohibited".

What does this mean for the future of the internet in Russia? How do new technologies affect citizens' fundamental rights and freedom of speech? This report does not merely state facts but offers an in-depth dive into the details, analysing the technical, legal and social aspects of these changes. It provides the reader with a comprehensive picture of how the digital environment in Russia has evolved from relatively free to rigidly controlled, and what risks this poses to society.

Disclaimer: This document was partially generated using several large language models (LLM). The information presented in it is based on the analysis and generalization of data from the specified sources, however, the process of its structuring, generalization, and presentation was performed using artificial intelligence technologies. It is recommended to use this text as a starting point for further research and to verify critically important data from primary sources.

1. General Information

1.1. Geographical Location

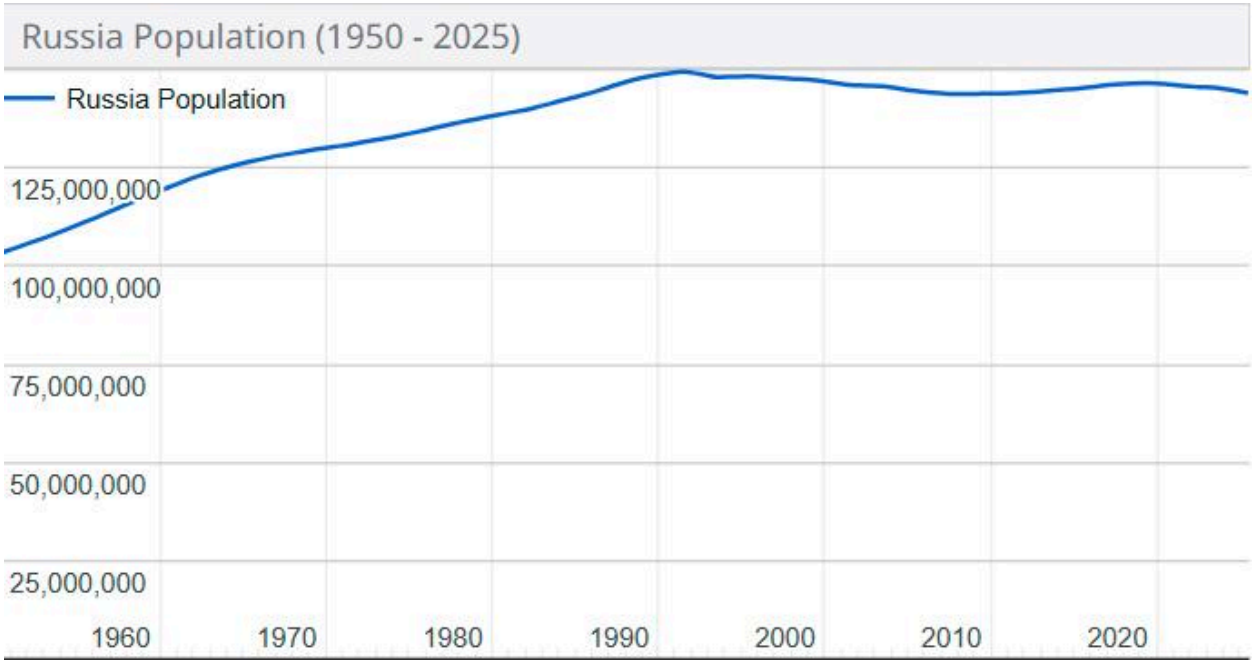
The Russian Federation is the largest country in the world by area, located in Eastern Europe and Northern Asia. The country is washed by the waters of the Pacific and Arctic Oceans, as well as by the Baltic, Black, Azov Seas of the Atlantic Ocean and the Caspian Sea. The Russian Federation has land borders with eighteen countries. The geographical location determines the diversity of climatic zones, rich natural resources and the country's significant geopolitical influence, which in turn affects the development of infrastructure, including the telecommunications network.

1.2. Population

The population of the Russian Federation is characterised by significant uneven distribution across the country's vast territory, with the greatest concentration of residents in the European part. The demographic situation in recent years remains difficult. There is a natural population decline, which is only partially offset by migration growth, and the latter also shows unstable dynamics. For example, according to 2023 data, the annual population growth was negative (-0.3%), and net migration in 2024 was estimated as a negative value amounting to -178,042 people.[1] The average life expectancy at birth in 2023 reached 73 years[1], which indicates a gradual improvement of this indicator, but it still lags behind the levels of many economically developed countries.

The dynamics of the population of the Russian Federation are presented in the table below. The data indicate an overall trend towards a decrease in population during the period under review.

Graph 1: Dynamics of the population of the Russian Federation (1950–2025)



Source: worldometers.info

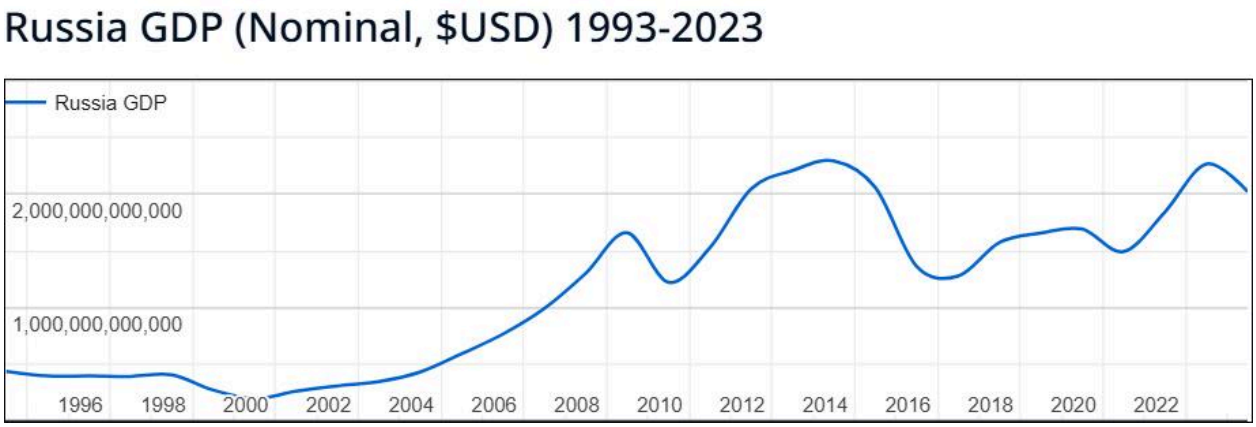
A decreasePhilippine population decline, especially if accompanied by negative net migration, as shown by the 2023–2024 data[1], may in the long term lead to a reduction in the domestic market and a shortage of labour. This, in turn, can slow down the development of labour-intensive sectors of the IT industry, despite state efforts on import substitution and support for the technological sector. The reduction in the total number of young specialists may exacerbate the already existing problem of shortage of qualified personnel in high-tech industries.

1.3. Gross Domestic Product

The economy of the Russian Federation is largely oriented towards the export of raw materials, primarily oil and gas. This structural feature makes the country's GDP dynamics sensitive to fluctuations in global energy prices, as well as to changes in the geopolitical situation, including international sanctions.[6] During the period under review, the Russian economy experienced both growth phases and periods of decline, reflecting both global economic cycles and specific challenges facing the country. According to the World Bank, Russia's GDP in 2023 amounted to

2021.42 billion US dollars.[7] In global GDP rankings, Russia occupies different positions depending on the calculation methodology (nominal GDP or GDP at purchasing power parity).[6]

Graph 2: Dynamics of nominal GDP of the Russian Federation (1993–2023)



Source: worldometers.info

Significant fluctuations in GDP in dollar terms with a more stable, though not always high, growth in ruble terms[9] indicate a high dependence of the external assessment of the state of the Russian economy on the national currency exchange rate. The ruble exchange rate, in turn, is strongly influenced by global energy prices and geopolitical factors, including sanction regimes.[6] Such volatility creates an atmosphere of uncertainty for foreign investors and companies operating in the Russian market, which is especially relevant for the technology sector, which often depends on the import of equipment, software and components.

World Bank GDP growth forecasts of 1.6% in 2025 and 1.1% in 2026[11] indicate an expected slowdown in economic development rates. This, combined with the bank's mentioned "limitations of production capacities, including labour resources"[11], may force the state to be more selective in financing large infrastructure projects. Such projects include those related to the provision of the so-called "sovereign internet".[13]

A potential reduction in available resources may slow down the implementation of these initiatives or require the reallocation of funds from other important sectors of the economy and social sphere.

1.4. Main Economic Characteristics

The Russian economy in the period from 2019 to 2025 was characterised by alternating periods of growth and recession, which was largely due to external shocks such as the COVID-19 pandemic

and the imposition of large-scale international sanctions. The key industries forming the country's GDP remain the extraction of minerals (primarily oil and gas), manufacturing, agriculture and the dynamically developing services sector, including information technology and telecommunications.[6] Despite certain successes in individual sectors, the economy continues to face a number of systemic structural problems. These include high dependence on the export of raw materials, insufficient diversification of the economic structure, technological lag in a number of industries, difficulties in attracting investment, corruption problems and unfavourable demographic trends.[6]

In 2023, according to preliminary estimates, GDP growth amounted to 3.6%, but the World Bank forecasts a slowdown of this indicator to 3.4% in 2024 and to 1.6% in 2025.[6] There is a trend towards a decrease in the share of foreign trade turnover in the GDP structure: by the end of 2023, the share of imports decreased to 19.1%, and the share of exports of goods and services reached a record low level of 23.3%.[6] This dynamic, partly due to sanction pressure and state policy of import substitution, may indicate the growing isolation of the Russian economy. Although such a situation can stimulate domestic production in some industries, including the IT sector, as noted in a number of reviews[6], in the long term it carries risks of reducing overall competitiveness due to limited access to advanced global technologies, global capital markets and international cooperation.

Despite the declared growth in certain high-tech sectors, such as information technology[6], fundamental structural problems of the economy, including raw-material dependence and institutional constraints[15], may restrain the sustainability of this growth and its real impact on the diversification of the national economy. Local successes in the IT sphere may not lead to a radical solution of systemic problems without deep structural reforms aimed at improving the investment climate, protecting property rights and developing competition.

1.5. General Political Situation

The Russian Federation, according to the Constitution, is a democratic federative rule-of-law state with a republican form of government.[17] The state system is characterised as a mixed (presidential-parliamentary) republic, but with a pronounced dominance of presidential power. The President of the Russian Federation is the head of state, determines the main directions of domestic and foreign policy and possesses broad powers.[17] Legislative power is exercised by the bicameral Federal Assembly, consisting of the State Duma (lower chamber) and the Council of Federation (upper chamber). Executive power belongs to the Government of the Russian Federation. Judicial power is represented by the system of courts, the highest of which are the Constitutional Court of the Russian Federation and the Supreme Court of the Russian Federation.[17]

The political system is characterised by the dominance of the "United Russia" party and a tendency towards centralisation of power.

The administrative-territorial division of the country includes various types of federal subjects: republics, krais, oblasts, cities of federal significance, an autonomous oblast and autonomous okrugs.[18] These subjects are united into eight federal districts, which are not constitutional units but serve to coordinate the activities of federal executive bodies on the ground.[19]

In the period from 2019 to 2025, a steady trend towards further centralisation of state power and strengthening of state control over various spheres of public life, including the economy, mass media and the information space as a whole, was observed in Russia's political life. International organisations and experts assess the political regime in Russia differently, with some characterising it as authoritarian.[17] This trend towards centralisation and strengthening of state control directly correlates with legislative initiatives in the sphere of internet regulation. The adoption of laws such as the "sovereign internet law"[13] and amendments to the Criminal Code introducing liability for the dissemination of "fakes"[20] is a reflection of the state's strategic desire to extend and strengthen its control over the digital sphere.

Formally, the Russian Federation is defined as a mixed presidential-parliamentary republic[17], but the actual dominance of the executive branch headed by the President and his Administration, as well as the significant influence of the pro-presidential party in parliament, may explain the relative ease and speed of adoption of legislative acts aimed at tightening regulation, including in the internet sphere. The weakening of the role of parliament as an independent and counterbalancing branch of power reduces barriers to initiatives coming from the executive branch or security structures, creating an environment in which legislation strengthening state control over the internet can be quickly adopted and implemented.

2. Internet

2.1. National Domain

The national top-level domain (ccTLD) for the Russian Federation is .RU. There is also the Cyrillic national domain .РФ. The .RU domain is intended for internet resources related to the Russian Federation, although there are no strict restrictions on the subject matter of hosted sites.[22] Registration of domain names in the .RU and .РФ zones is carried out through a network of accredited registrars.

The .RU domain was officially delegated to Russia on 7 April 1994. Management and coordination of the development of the national domains .RU and .РФ is carried out by the Coordination Center for the National Domain of the Internet (CC).[22] An important event in the history of national domain management was the entry of the Russian Federation, represented by the Federal Service for Supervision of Communications, Information Technology and Mass Communications (Roskomnadzor), into the founders of the CC on 3 June 2020.[23] This step is regarded as an element of the overall state policy aimed at strengthening control over critical information infrastructure and the "sovereignisation" of the Russian segment of the internet.

The entry of Roskomnadzor, the main state body responsible for the regulation and blocking of internet resources[24], into the founders of the Coordination Center for the National Domain[23] is a significant factor indicating the strengthening of state influence on the management of the country's key internet infrastructure. This may potentially lead to a tightening of domain name registration policy and the use of the domain system as one of the tools for censorship or rapid blocking of resources deemed undesirable. Strengthening state control over the national domain, combined with the provisions of Federal Law No. 90-FZ ("on the sovereign internet"), which provides for the creation of a national domain name system[13], forms the technical and administrative basis for the potential isolation of the Russian internet segment or selective disconnection from the global DNS system in the event of certain "threats".

2.2. Number of Users

As of the beginning of 2025, according to Datareportal, the Russian Federation had 133 million internet users, corresponding to an internet penetration level of 92.2% of the total population.[4] Somewhat different data are provided by Mediascope: in October 2024, the monthly internet audience in Russia amounted to 103 million people, or 85% of the population aged 12 and older.[26] Data from the Federal Reserve Bank of St. Louis (FRED) indicate 92.2 internet users per 100 population in 2023.[28]

Sources of data on the number of internet users and the level of its penetration include: Datareportal[2], Mediascope[26] and FRED (St. Louis Fed).[28]

Dynamics of the number of internet users and the level of internet penetration in Russia by year:

Year	Number of Internet Users (millions)	Internet Penetration Rate (%)	Source(s)
2019	118.0 (January 2020)	81.0 (January 2020) / 82.6 (year)	[2] (Datareportal)[28] (FRED)
2020	118.0	81.0 / 85.0 (year)	[2] (Datareportal)[28] (FRED)
2021	124.0	85.0 / 88.2 (year)	[2] (Datareportal)[28] (FRED)
2022	129.8	89.0 / 90.4 (year)	[2] (Datareportal)[28] (FRED)
2023	127.6	88.2 / 92.2 (year)	[2] (Datareportal)[28] (FRED)
2024 (beginning)	130.4	90.4	[3] (Datareportal)
2025 (beginning)	133.0	92.2	[4] (Datareportal)

Note: Data from different sources may differ slightly due to differences in counting methodologies and research periods.

A high level of internet penetration exceeding 90% according to the latest available data[4] means that the internet is the main source of information and a key communication platform for the overwhelming majority of the Russian population. This factor makes control over the internet space critically important for state bodies seeking to influence public opinion and information flows, especially in conditions of limited access to independent traditional media.

Some discrepancy in the absolute number of users from various research agencies (e.g. Mediascope[26] and Datareportal[3]) may be related to differences in counting methodologies, such as the age groups taken into account, frequency of internet use or the definition of an "active" user. Nevertheless, the overall trend towards almost complete coverage of the population by internet services is obvious. A slight decrease in the absolute number of users noted by Datareportal in certain periods (for example, by 711 thousand people between January 2024 and January 2025[4]), with an overall increase in the relative level of penetration, is probably related to demographic factors such as the overall population decline or methodological adjustments in studies, rather than a real reduction in internet use. It is important to note that the share of the population not using the

internet remains small (7.8% at the beginning of 2025[4]), which confirms the total coverage of the country with internet access.

2.2.1. Fixed Internet

The fixed broadband internet access (BBA) market in the Russian Federation is characterised by a high level of competition in large cities and regional centres. However, in small settlements and remote areas of the country, the level of BBA penetration and the choice of available providers may be significantly lower. State programmes such as the project to eliminate digital inequality (EDI) are aimed at increasing the accessibility of modern communication services, including BBA, for residents of small and remote settlements. The main technologies used to provide fixed BBA services are various versions of FTTx (fibre to the building/apartment), providing high data transfer speeds.

According to the analytical company TMT Consulting, in the second quarter of 2024 the number of BBA subscribers in the B2C segment in Russia reached 36.5 million, showing a growth of 0.4% compared to the same period of the previous year.[29] The dynamics of the number of fixed BBA users for earlier years in the provided materials are not detailed enough to build a complete table from 2019.

The largest operators in the Russian fixed BBA market, which, according to TMT Consulting for the second quarter of 2023, accounted for about 71% of the subscriber base[30], are:

- **Rostelecom**: It is the market leader. In the first quarter of 2023, the company's subscriber base grew by 0.6%.[30] Website: https://rt.ru/
- **MTS**: One of the leading players, demonstrating subscriber base growth due to network expansion in the regions and the offer of convergent services. In the second quarter of 2024, subscriber base growth amounted to 0.9%.[29] Website: https://mts.ru/
- **ER-Telecom** (operates under the brands Dom.ru, previously also Akado): After the consolidation of assets, including the Moscow operator Akado in 2023, the company strengthened its position, increasing its market share by subscribers to 12% in the first quarter of 2023.[30] Websites: https://dom.ru/, https://www.akado.ru/
- **VimpelCom** (Beeline brand): It is among the largest BBA operators. Website: https://beeline.ru/
- **TTK (TransTeleCom)**: Ranks fifth in the market, with a share of about 2% in subscribers and revenue.[30] Website: https://ttk.ru/

Consolidation processes in the BBA market, such as the acquisition of Akado by ER-Telecom holding[30], lead to the strengthening of the positions of the largest players. On the one hand, this can contribute to improving the quality of services provided and accelerating network modernisation due to greater investment opportunities of consolidated companies. On the other hand, the reduction in the number of independent operators may lead to a weakening of competition and, as a consequence, a potential increase in tariffs for end users in the long term, especially in those market segments where the choice of providers is limited.

Despite the high overall level of internet penetration in the country, the growth rates of the fixed BBA subscriber base are slowing down (for example, growth of 0.4% in the second quarter of 2024[29]). This may indicate a gradual saturation of the market in large cities, where the penetration level is already high (for example, in Moscow — 87.5%[30]). Further growth of the BBA market will largely depend on the success of connecting subscribers in remote and hard-to-reach territories, where the economic feasibility of building infrastructure for operators is lower. This, in turn, may require more active state participation, including subsidy programmes and support for operators working in such regions.

2.2.2. Mobile Internet

Mobile internet plays a key role in providing network access for a significant part of the population of the Russian Federation. Its importance is especially great in regions with insufficient fixed BBA network coverage, as well as for users who need internet access outside the home or office. The mobile communications and mobile internet market in Russia is characterised by a high degree of competition between the operators of the so-called “big four”. Operators continue to develop 4G/LTE standard networks, providing increasingly wider coverage and increased data transfer speeds. The introduction of 5G technology is at an early stage and faces a number of difficulties, including limited access to the necessary equipment due to sanctions and issues of frequency resource allocation.

As of the beginning of 2025, Russia had 216 million active mobile connections, equivalent to 150% of the total population. However, it should be borne in mind that not all of these connections provide internet access (some may be used only for voice communication and SMS) and one user can have several active SIM cards.[4] The number of mobile connections decreased by 3.3 million (-1.5%) in the period from the beginning of 2024 to the beginning of 2025.[4] A similar trend was observed a year earlier: at the beginning of 2024, 219.8 million mobile connections were recorded (152.5% of the population), which is 4.6 million (-2.0%) less than at the beginning of 2023.[3]

The largest mobile communications and mobile internet operators in Russia are:

- **MTS**: As of the end of 2023, the company served 81.8 million mobile subscribers[31], and according to data for the third quarter of 2024 — 81.9 million.[32] Website: https://mts.ru/
- **MegaFon**: The number of mobile subscribers at the end of 2023 was 67.7 million[31], and in the second quarter of 2024 — 77.26 million.[32] Website: https://megafon.ru/
- **VimpelCom** (Beeline brand): At the end of 2023, the operator had 44.1 million mobile subscribers[31], the same figure is given for the third quarter of 2023.[32] Website: https://beeline.ru/
- **Tele2** (part of the Rostelecom group): Rostelecom in total (including Tele2) served 48.1 million mobile subscribers at the end of 2023.[31] Separately for Tele2, data for the third quarter of 2024 — 48.0 million subscribers.[32] Website: https://tele2.ru/

A significant excess of the number of mobile connections over the total population (more than 150%[3]) indicates the widespread practice of using several SIM cards by one subscriber (for example, for different tariffs, for work and personal needs) or the active use of SIM cards in various M2M (machine-to-machine) and IoT (Internet of Things) devices. The observed decrease in the total number of mobile connections in 2024–2025[3] may be related to market saturation, optimisation of user expenses (refusal of excess SIM cards) or the influence of general economic and demographic factors.

The dependence of the development of new-generation 5G networks on the availability of foreign telecommunications equipment and allocated frequencies, especially in the context of international sanctions and the state policy of import substitution, may lead to a slowdown in the pace of implementation of this technology in Russia compared to other countries. This, in turn, can limit the development of new digital services and applications requiring ultra-high data transfer speeds and minimal delays (for example, in the fields of industrial internet of things, unmanned transport, advanced virtual and augmented reality technologies). Such a lag can potentially increase Russia's "digital divide" with technologically more advanced states and affect the competitiveness of the Russian digital economy in the long term.

2.3. Internet Access Speed and Quality of Services Provided

Internet access speed in Russia shows steady growth both in mobile and fixed segments, but the country still lags behind the leaders of global rankings. According to Ookla Speedtest Global Index for April 2025, the median download speed in mobile networks in Russia was 50.50 Mbit/s, corresponding to 90th place in the world. In the fixed BBA segment, the median download speed

reached 158.89 Mbit/s.[33] Datareportal data, also based on Ookla measurements, at the beginning of 2025 showed a median mobile speed of 26.21 Mbit/s (growth of 9.3% over the year) and a median fixed speed of 89.39 Mbit/s.[4] A year earlier, at the beginning of 2024, these indicators were 23.97 Mbit/s for mobile and 84.74 Mbit/s for fixed internet, respectively.[3] Earlier data from Roskachestvo (beginning of 2022) indicated an average mobile speed of 17.84 Mbit/s and an average fixed speed of 61.65 Mbit/s.[34]

Regional differences in access speeds are also significant. According to the operator Dom.ru for March 2024, the leaders in average BBA speed among Russian cities were Krasnodar (240.5 Mbit/s), Rostov-on-Don (179 Mbit/s) and Saint Petersburg (177.8 Mbit/s), while Moscow ranked fifth with a result of 168.5 Mbit/s.[35]

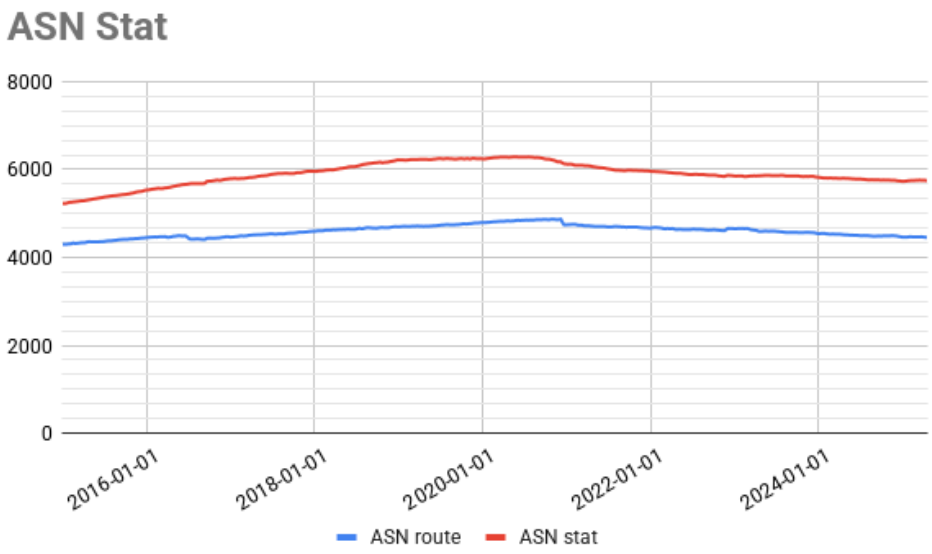
The observed steady growth of median access speeds[3] indicates continued investment by communication operators in the modernisation and development of network infrastructure. Nevertheless, Russia's lag behind the countries leading in global internet speed rankings[33] indicates significant potential for further improvement. This may be related to the scale of the country's territory, the need to update outdated network sections or economic restrictions affecting the pace of investment.

The significant difference in internet access speeds between large agglomerations[35] and the country's overall average indicators[4] emphasises the persisting problem of "digital inequality" within Russia. Such inequality can limit citizens' equal access to modern information, online education, digital-format public services and the opportunities provided by the digital economy. This, in turn, can exacerbate existing regional disparities in socio-economic development and limit the realisation of digital rights for part of the population.

2.4. Development of Providers and Autonomous Systems

Autonomous systems (AS) are key components of the global internet infrastructure, representing a set of IP networks and routers managed by one or more operators and having a single routing policy. The number of registered and actively routed AS in a country is an important indicator of the development and complexity of its internet ecosystem. According to RIPE NCC (Regional Internet Registry for Europe, the Middle East and part of Central Asia) as of April 2017, 1404 local internet registrars (LIR) were registered in Russia and 5822 autonomous system numbers (ASN) were allocated. Of these, 4509 AS actively announced 26320 IP prefixes.[37]

Graph 3: Dynamics of Autonomous Systems in the Russian Federation (2015–2025)



Traditionally, the growth in the number of autonomous systems indicates the development of competition in the internet provider market and an increase in the decentralisation of internet infrastructure. However, in the context of Russian legislation, in particular Federal Law "on the sovereign internet"[13], which provides for the creation of a register of traffic exchange points and the possibility of centralised routing management, the quantitative growth of AS does not necessarily guarantee an increase in network resilience to arbitrary blockings or a greater degree of freedom. On the contrary, there is a possibility that these autonomous systems can be more effectively subordinated to the requirements of the national regulator.

The graph demonstrates two clearly defined phases in the dynamics of the number of autonomous systems in Russia. From 2015 to the beginning of 2021, there was a steady positive trend indicating extensive growth in the number of internet infrastructure entities. However, starting from 2021, this trend is replaced by stagnation with a subsequent slight decrease in both the total number of registered AS and the number of active AS. As of April 2025, 5720 autonomous systems are recorded in the Russian Federation, of which 4434 announce routes in the global network.

With a population of about 146 million people, the density ratio of active autonomous systems for Russia is **30.4 AS per 1 million inhabitants**.

For contextualisation of the obtained data, a comparative analysis with the indicators of Eastern European countries was carried out. It was found that the Russian Federation significantly lags behind a number of states in this parameter.

Ukraine shows the highest level of decentralisation of internet infrastructure in the region: the density ratio of active AS reaches **76.7 per 1 million people**. **Poland** also demonstrates a high indicator — **63.1 AS per 1 million people**. Such a significant excess of Russian values indicates a higher degree of competition between internet service providers and a greater variety of independent network operators in these countries.

The indicators of **the Republic of Belarus** are comparable to Russian ones and amount to **30.2 AS per 1 million inhabitants**, which indicates a similar market structure. At the same time, **Kazakhstan** demonstrates a lower level of penetration of independent networks with a ratio of **12.6 AS per 1 million people**.

If current data showed stagnation or a decrease in the number of actively routed AS in recent years, this could serve as an indicator of consolidation processes in the internet provider market or the departure from the market of smaller players. Such processes may be caused by the tightening of regulatory requirements, for example, significant costs for the implementation and maintenance of SORM systems (System of Operational-Investigative Measures) as well as deep packet inspection (DPI) equipment in accordance with the requirements of the "Yarovaya law" and the "sovereign internet law".[25] Such financial and administrative barriers can lead to a decrease in competition and strengthening of the positions of large, often state-affiliated providers, which in turn can affect the choice and quality of services for end users.

Table 2: Top 10 largest Autonomous Systems of the Russian Federation

#	Number of AS	Name	Web Site	Foreign neighbour count	Local neighbour count	Total neighbour count	Foreign neighbours share
1	20764	CJSC RASCOM ISP	https://rascom.ru/en/	4902	1077	5979	81%
2	20485	TRANSTELECOM	https://www.ttk.ru	3771	2136	5907	63%
3	3216	Beeline, VimpelCom, Sovintel, Golden Telecom, Sovam	https://beeline.ru	1786	1730	3516	50%
4	57304	RETNRU-AS	https://www.retn.ru	2706	450	3156	85%
5	31133	PJSC MegaFon	https://www.megafo	1245	1854	3099	40%

			n.ru				
6	12389	Rostelecom	https://www.company.rt.ru/en/	454	2312	2766	16%
7	48858	Milecom-as	https://www.milecom.ru	2006	200	2206	90%
8	8359	Mobile TeleSystems PJSC	https://ir.mts.ru/	846	958	1804	46%
9	43727	KVANT-TELECOM CJSC	https://www.kvant-telecom.ru	884	572	1456	60%
10	9049	Dom ru, Дом.ru	https://ertelecom.ru	80	1010	1090	7%

Analysis of the top 10 largest autonomous systems of the Russian Federation confirms and complements the conclusion about the high concentration of the internet access market. The data in the table make it possible to identify the structure of the Russian segment of the Internet and determine the roles of key players.

Main conclusions on the market structure:

High degree of concentration. Russia's internet backbone is controlled by a limited number of large telecommunications companies. These include the operators of the "big three" (MTS, MegaFon, Beeline), the state operator Rostelecom, as well as large providers such as TransTeleCom (TTK) and ER-Telecom (Dom.ru). This fact explains the stagnation in the growth of the total number of autonomous systems: it is extremely difficult for new players to compete with infrastructure giants that have thousands of peering connections.

Functional specialisation of operators. The table clearly divides operators into several categories according to their role in the network infrastructure:

- International transit operators: Companies RETN (85% foreign connections), Milecom (90%) and RASCOM (81%) act as the main gateways connecting Runet to the global network. Their business model is focused on providing international traffic transit, which is confirmed by the dominant share of foreign peers.
- National operators focusing on the domestic market: Rostelecom (only 16% foreign connections) and Dom.ru (7%) are classic examples of "last mile" giants. They have the widest coverage within the country (especially Rostelecom with its 2312 local connections — an absolutely dominant indicator), but for access to the global network they mainly use the services of transit operators.

- Universal operators: The largest mobile operators (MTS, MegaFon, Beeline) maintain a balanced network policy. They have an extensive network of peering connections both within Russia for traffic exchange between their subscribers and abroad to optimise routes and reduce costs for purchasing transit.

Special role of Rostelecom. Rostelecom's absolute leadership in the number of local connections (2312) emphasises its status as an infrastructure monopolist and system-forming operator. A significant part of domestic Russian traffic in one way or another passes through its networks.

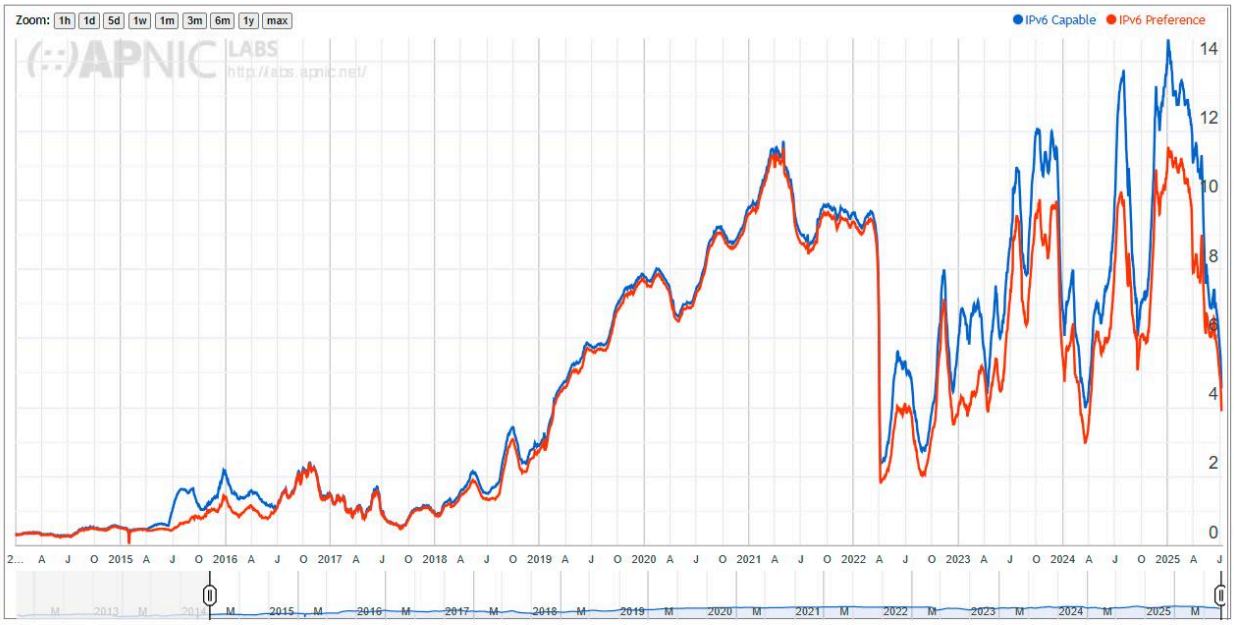
Taken together, the presented data paint a picture of a mature, concentrated market with several dominant players and a clear division of functions between international transit operators and domestic access providers.

2.5. IPv6 Penetration

The transition to the new version of the internet protocol IPv6 is a global necessity due to the exhaustion of IPv4 address space and the growing number of devices connected to the network (including the Internet of Things, IoT). The dynamics of IPv6 implementation in Russia is an important aspect of the development of the national internet infrastructure.

Data on IPv6 penetration in Russia vary significantly depending on the source and measurement methodology. According to Google, as of 9 June 2025, 44.65% of Google users from Russia used IPv6 to access the company's services.[39] Similar figures (44.62% of Google's global traffic via IPv6) were provided by VASExperts citing APNIC Labs as of 18 November 2024, but without specifying the Russian indicator from APNIC in that source.[40] Meanwhile, earlier data from APNIC Labs presented by RIPE Labs in 2020 showed a significantly lower level of IPv6 penetration in Russia: 7.2% according to Akamai measurements, 7.01% according to APNIC itself, 9.43% according to Facebook and 3.85% according to Google.[41] Also, according to APNIC in 2020, the IPv6 usage ratio (V6 Use ratio) for Russia was 7.78%.[42]

Graph 4: Dynamics of IPv6 penetration in the Russian Federation (2015–2025)



Source: stats.labs.apnic.net

Discussions in technical communities[44] suggest that the introduction of IPv6 may have been delayed by some operators due to the need to ensure compatibility of the new protocol with DPI systems used for state censorship and traffic filtering. After updating these systems, IPv6 deployment could accelerate. If this hypothesis is correct, then the growth in IPv6 use paradoxically may be associated with the strengthening of technical capabilities for controlling internet traffic in the country.

If a significant increase in IPv6 penetration to the level of 40–60% is confirmed, this will indicate that Russian communication operators and the state are aware of the need to transition to the new protocol to ensure the long-term development of Runet and support the growing number of connected devices. This also means that technical and possibly regulatory barriers to IPv6 implementation, including its integration with control systems, have been largely overcome.

Accelerated implementation of IPv6, if it is really taking place and supported by the state (for example, through regulatory requirements for operators), can also be used to strengthen measures for the "sovereignisation" of the internet. The presence of a developed IPv6 infrastructure managed by national operators and fully compatible with DPI systems facilitates control over traffic

and the implementation of filtering and blocking policies in the new protocol environment, which corresponds to the overall state strategy to strengthen control over the information space.

2.6. Connectivity Index

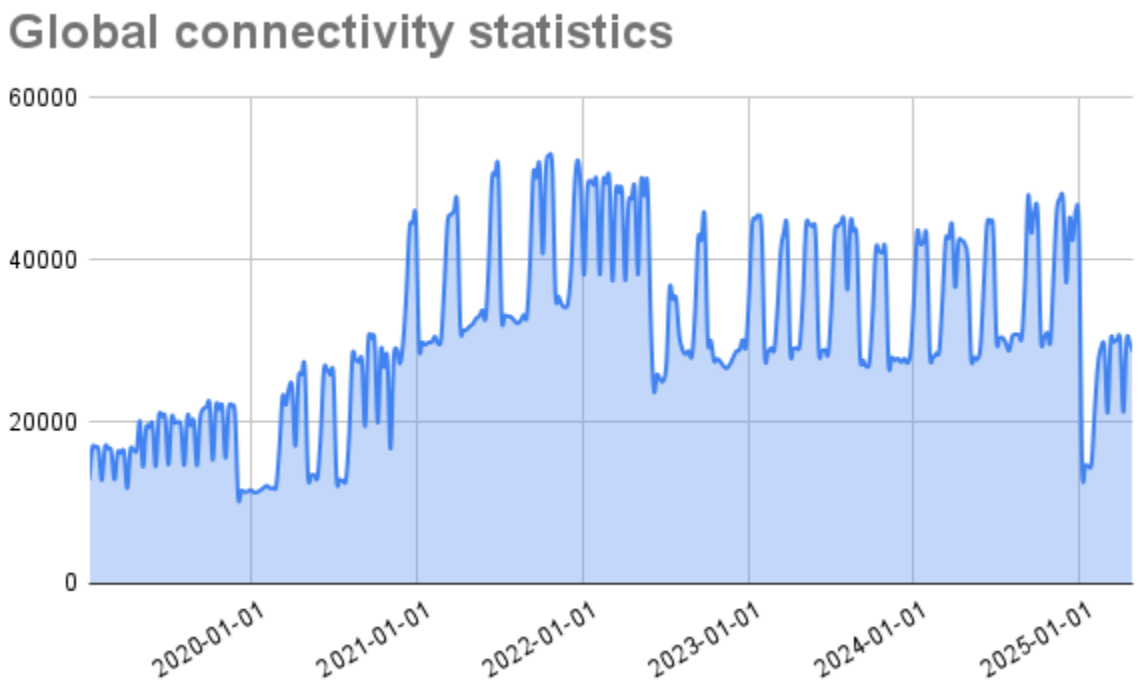
To assess the level of integration of the internet segment, two key indicators are used, based on the analysis of pairwise connections (peerings) between Autonomous Systems (ASN).

Global Connectivity Index: This index represents the total number of unique connections between each Russian ASN and each external (foreign) ASN. Essentially, it measures how widely and diversely the Russian internet segment is connected to the rest of the world. The higher this indicator, the more “windows” the country has to the global network.

Local Connectivity Index: This index is calculated as the total number of unique connections between different Russian ASNs. It reflects the intensity and complexity of the domestic internet market, in particular the activity at traffic exchange points (IXP). A high indicator indicates a developed internal ecosystem that allows efficient traffic exchange within the country, minimising delays and dependence on external channels for local data.

Analysis of the ratio of these two indices allows us to understand the strategic orientation of the national network: whether it is predominantly self-sufficient or deeply integrated into the global infrastructure.

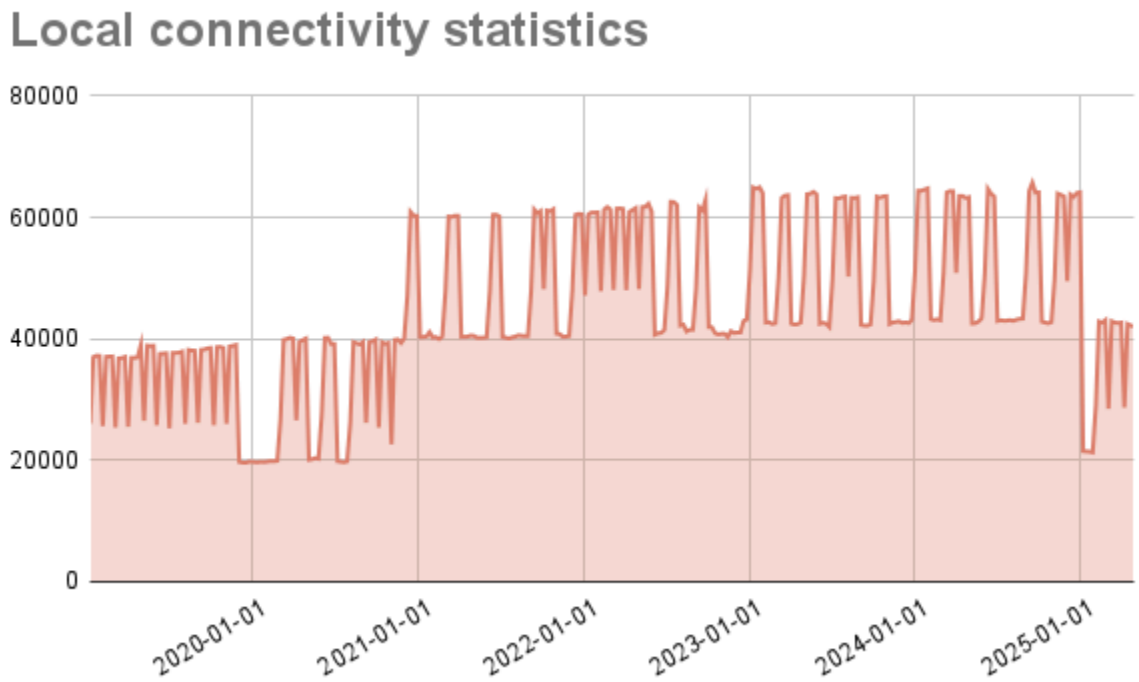
Graph 5: Dynamics of global connectivity of Autonomous Systems of the Russian Federation (2019–2025)



The graph illustrates the number of unique connections between Russian and foreign autonomous systems. From 2020 to the beginning of 2022, there was intensive growth in the indicator, which reached peak values of over 50,000 connections, indicating active integration of Runet into the global network. However, in the first half of 2022, a sharp structural shift occurred: the global connectivity index instantly decreased and stabilised at a new, lower level in the range of 30,000–40,000 connections, while demonstrating increased volatility.

This drop directly reflects the reduction in the number of international partners and routes, probably due to geopolitical events and the departure from the Russian market of a number of foreign operators. Based on the current average level of 30,000 global connections and the presence of 4434 active AS in the country, it can be concluded that each active autonomous system in Russia has on average about 6.8 connections with foreign networks. This quantitatively confirms the reduction in the diversity of external communication channels.

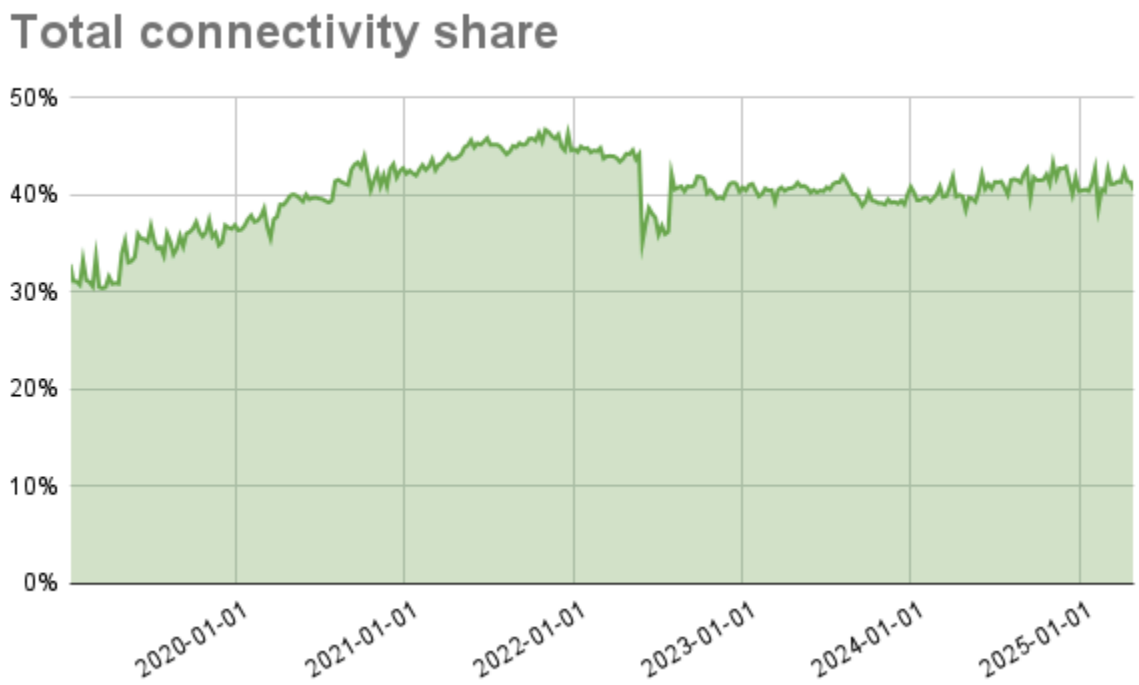
Graph 6: Dynamics of local connectivity of Autonomous Systems of the Russian Federation (2019–2025)



The local connectivity index, reflecting the number of unique peerings within Russia, demonstrates a different trajectory. At the beginning of 2021, the indicator jumped from ~40,000 to more than 60,000 connections, indicating a qualitative development of the internal internet infrastructure, in particular traffic exchange points (IXP). The key point is that, unlike the global index, the high level of local connectivity has been maintained throughout the entire period of 2022–2024.

This dynamic indicates a purposeful strengthening of the internal network ecosystem and the development of its self-sufficiency. In the context of the reduction of external connections, Russian operators began to interact more actively with each other to optimise traffic routing within the country. With the current indicator of ~60,000 local connections, each active AS has on average 13.5 internal connections. This indicator, more than twice the average number of external connections, confirms the orientation towards internal connectivity.

Graph 7: Dynamics of the ratio of global and local connectivity of Autonomous Systems of the Russian Federation (2019–2025)



This graph most clearly demonstrates the strategic turn in the architecture of Runet. It shows the share of global connections in the total pool of connections. Until the beginning of 2022, this share was growing, reaching a peak of almost 48%, which reflected the course towards ever greater global integration. The sharp drop in the indicator in 2022 to a new stable level in the region of 40% is a direct consequence of the above-mentioned opposite trends: reduction of external peerings while maintaining and developing internal ones.

Thus, the analysis of the ratio of indices records a fundamental shift from a model of growing openness to a model oriented towards increasing internal stability and autonomy. A structural rebalancing of the Russian internet segment has occurred, as a result of which the relative dependence on external channels has decreased in favour of strengthening internal infrastructure connections.

3. Internet Legislation

3.1. Principles of Internet Governance

Internet governance in the Russian Federation is a complex, multi-level system that includes state bodies, industry organisations (such as the Coordination Center for the National Domain) and representatives of the business community. However, the determining role in shaping the rules and practices of Runet functioning is played by the state, whose policy in recent years has been consistently aimed at strengthening control and regulation of the digital space. The principles of internet governance in Russia have undergone significant evolution: from a period of relatively free development in the 1990s and early 2000s to a model where the emphasis has shifted to ensuring "digital sovereignty", information security (in its state interpretation) and expansion of control over content and infrastructure.

The Russian Internet Governance Forum (RIGF), annually organised by the Coordination Center for the National Domain of the Internet, is positioned as a platform for dialogue and consensus building between state bodies, the professional telecommunications community, business and civil society on issues of further internet development.[45] Nevertheless, real decisions determining the vector of regulation development are made predominantly at the state level.

The desire for "consensus search" declared at such platforms[45] often contradicts the practice of adopting legislative decisions, where the position of state bodies aimed at strengthening control dominates. This creates a certain gap between public discussion and real policy in the field of internet regulation, which is confirmed by the adoption of a number of high-profile laws despite criticism from part of the expert community and human rights organisations.

3.1.1. Regulation

Regulation of the internet in the Russian Federation is carried out through an extensive system of federal laws, by-laws (government decrees, orders of specialised ministries and departments) and direct activities of authorised state bodies. The key directions of state regulation of the internet sphere are:

- **Control over network infrastructure:** This is most clearly manifested in the provisions of Federal Law No. 90-FZ ("on the sovereign internet"), which is aimed at ensuring the integrity, stability and security of the functioning of the Russian segment of the network, but also

creates technical and legal prerequisites for its possible isolation and centralised traffic management.[13]

- **Content filtering and blocking:** There is a ramified system of grounds and procedures for restricting access to information recognised as prohibited. This includes maintaining the Unified Register of Prohibited Sites by Roskomnadzor.
- **Control over information dissemination:** Laws have been introduced establishing liability for the dissemination of "fake" information (in particular, about the activities of the Armed Forces of the Russian Federation), information expressing "clear disrespect" to the authorities, as well as for calls for extremism and mass riots.
- **Requirements for localisation of personal data:** Operators collecting personal data of Russian citizens are required to ensure their storage and processing on the territory of Russia.
- **Regulation of the activities of IT companies and social networks:** Requirements have been introduced for foreign IT giants to open representative offices, moderate content, and remove prohibited information.

Overall, the regulation of the internet sphere in Russia is characterised by a trend towards consistent tightening, expansion of powers of state bodies and an increase in the number of obligations imposed on communication operators, owners of internet resources and users themselves.[25] Regulation is becoming increasingly comprehensive and all-penetrating, affecting both the infrastructure level[13] and content[25] and behavioural aspects. This creates a complex and often opaque system of obligations and prohibitions for all participants in the internet space, which increases risks for doing business and limits users' rights.

3.1.2. Regulatory Authorities and Responsible Persons

The following state authorities play a key role in the regulation and control of the internet space in Russia:

- **Federal Service for Supervision of Communications, Information Technology and Mass Communications (Roskomnadzor)**: It is the main regulatory and supervisory body. Its competence includes blocking sites, maintaining various registers (including the register of prohibited information, the register of information dissemination organisers, the register of news aggregators), monitoring compliance with legislation on personal data, control and supervision in the field of mass media and communications. Roskomnadzor is subordinate to the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation.[24]

- **Ministry of Digital Development, Communications and Mass Communications of the Russian Federation (MinTsifry Russia)**: Responsible for the formation and implementation of state policy and legal regulation in the field of information technology, communications and mass communications.
- **Federal Security Service of the Russian Federation (FSB of Russia)**: Exercises control over compliance by communication operators with the requirements for the installation and functioning of the System of Technical Means for Ensuring the Functions of Operational-Investigative Measures (SORM). Participates in resolving issues of information security and countering cyber threats.
- **Prosecutor General's Office of the Russian Federation**: Has the authority to send requests to Roskomnadzor for extrajudicial blocking of internet resources containing calls for mass riots, extremist activities, participation in unauthorised public events, as well as disseminating deliberately false socially significant information ("fakes") and information expressing clear disrespect for state authorities.
- **Ministry of Internal Affairs of the Russian Federation (MVD Russia), Investigative Committee of the Russian Federation (SK Russia)**: Deal with the investigation of crimes committed using information and telecommunication technologies, as well as criminal cases initiated for illegal dissemination of information on the internet (for example, under articles on extremism, slander, dissemination of "fakes").

Leadership of Roskomnadzor (as of February 2025)[24]:

- **Head**: Lipov Andrey Yuryevich (appointed 29 March 2020).
  - Official biography: https://rkn.gov.ru/about/management/person/news77.htm (the link may change; the current one should be searched on the official website rkn.gov.ru in the section "About Roskomnadzor" → "Leadership").
- **Deputy Heads**[47]:
  - Logunov Vladimir Viktorovich
    - Official biography: (available on the official website of Roskomnadzor)
  - Subbotin Vadim Alekseevich
    - Official biography: (available on the official website of Roskomnadzor)
  - Terlyakov Oleg Aleksandrovich
    - Official biography: (available on the official website of Roskomnadzor)
  - Vagner Milosh Eduardovich
    - Official biography: (available on the official website of Roskomnadzor)

The concentration of the main regulatory and law-enforcement functions in the hands of Roskomnadzor[24], acting under the general leadership of MinTsifry and in close cooperation with security structures (FSB, Prosecutor General's Office), creates a powerful centralised mechanism of state control over the internet. Such a structure of powers simplifies for the state the implementation of its policy in the digital sphere, but can lead to a decrease in the transparency of decisions taken and limit the possibilities for their independent contestation.

3.2. Monopolisation of the Market

Formally, Russian legislation, including the Federal Law "On Protection of Competition", is aimed at preventing monopolisation of markets, including the market for communications services and internet access. There are no special laws directly encouraging monopolisation in this sphere. Nevertheless, a number of legislative initiatives and the established law-enforcement practice may indirectly contribute to strengthening the market positions of a limited number of large players, many of which are state-owned companies or companies with state participation. For example, high financial and technical requirements for communication operators related to the need to store user data ("Yarovaya law") or install equipment for the implementation of the "sovereign internet law" (technical means of countering threats — TSPU) may be more burdensome for small and medium-sized providers, potentially leading to their departure from the market or absorption by larger companies.[25]

In the Russian market of fixed broadband access and mobile communications, several large operators actually dominate: Rostelecom, MTS, MegaFon, VimpelCom (Beeline) and ER-Telecom (Dom.ru).[29] Rostelecom, being a company with a significant share of state participation, plays a special role in the implementation of state infrastructure projects (for example, the programme for eliminating digital inequality, creation and development of telecommunications infrastructure for the needs of state bodies). This company is often regarded as the key executor of state policy in the field of "sovereignisation" of Runet.

Although formally the legislation does not encourage monopolisation, economic and regulatory barriers, such as the high cost of fulfilling the requirements of the "Yarovaya law" and the "sovereign Runet law"[25], create conditions in which only large players with significant financial and administrative resources can effectively compete and develop. This leads to the actual oligopolisation of the market and strengthening of the role of companies with state participation. Strengthening the positions of large operators controlled or loyal to the state, in turn, facilitates the implementation of state policy on control over internet traffic and infrastructure. It is easier for state bodies to interact (and, if necessary, exert pressure) with a limited number of large companies than

with numerous small independent providers. This simplifies the introduction of centralised traffic management systems (for example, TSPU) and ensuring universal compliance with the requirements for blocking and providing access to data for law enforcement agencies. Thus, the observed oligopolisation of the market may be not only a consequence of economic processes, but also a factor contributing to the achievement of the state's political goals in the digital sphere.

3.3. Internet Shutdowns on Government Orders

Federal Law No. 90-FZ of 1 May 2019, widely known as the "sovereign internet law"[13], laid the legal and technical foundation for centralised management of the Russian segment of the Internet. The law declares the goals of ensuring the integrity, stability and security of Runet functioning, including in the event of external threats. However, its provisions also create the possibility of isolating the Russian segment from the global network or disconnecting internet access in certain areas of the country. The concept of "threats" in the law is interpreted quite broadly, which leaves room for various interpretations.

The law provides for the creation of the Centre for Monitoring and Management of Public Communication Networks (CMU SSOP), which is under the jurisdiction of Roskomnadzor. Communication operators are required to install technical means of countering threats (TSPU) on their networks, which allow Roskomnadzor to filter traffic and, if necessary, restrict access to information or even disconnect network segments. Decisions on the introduction of "centralised management" of the network are made by Roskomnadzor on the basis of rules approved by the Government of the Russian Federation and in coordination with the FSB and the Federal Guard Service (FSO). The reasons for such actions may include external cyberattacks, internal threats (for example, mass riots that can be qualified as a security threat), as well as conducting exercises to ensure the resilience of Runet. The Freedom House report for 2022 mentions that the Russian government conducted tests to disconnect Runet from the global internet.[25]

The "sovereign internet law"[13], under the pretext of protecting national internet infrastructure from external threats, actually creates a legal mechanism for carrying out internal shutdowns or large-scale traffic filtering for political reasons. This poses a serious threat to freedom of information, freedom of expression and other digital rights of citizens. The broad interpretation of the concept of "threat" allows these mechanisms to be used in various situations, including periods of political instability or to suppress protest activity.

The requirement for mandatory installation of TSPU on the networks of all communication operators[25] and the creation of a centralised management system through CMU SSOP actually

transfer to the state, represented by Roskomnadzor, direct control over data flows within the country. This not only reduces the autonomy of communication operators, but also creates an infrastructure for potentially total surveillance and censorship, the capabilities of which go far beyond simply disconnecting network access. Such a system allows granular control over the entire internet space, including blocking specific resources, protocols, slowing down traffic to "undesirable" sites and analysing the content of transmitted information.

In 2025, the practice of internet shutdowns on government orders moved from a theoretical possibility to mass application, affecting dozens of regions. Starting from May 2025, during the "Victory" parades, mobile internet was preventively disconnected in more than 30 cities of Russia under the pretext of protection against drone attacks. These shutdowns became the first case of coordinated shutdown on such a scale, demonstrating the readiness of the authorities to use the created infrastructure of centralised network management (TSPU) to restrict access to communications over vast territories.

The situation escalated dramatically in the summer of 2025 after the Ukrainian forces conducted Operation "Web", during which mobile internet was used to guide drones to strategic aviation airfields deep inside Russia. In response, the Russian authorities began to apply the practice of regular and prolonged mobile internet shutdowns as a countermeasure. According to independent observers, in June and July 2025 the number of local shutdowns numbered in the hundreds and affected more than half of the country's regions, including those thousands of kilometres from the combat zone.

Thus, "protection from external threats", originally declared as the goal of the "sovereign internet law", in practice turned into a legal basis for mass and prolonged mobile internet shutdowns for the civilian population. These shutdowns, sometimes lasting for several days, have become a new reality for millions of Russians, significantly limiting their basic rights to access information, communication and use of digital services.

3.4. Legislation on "Words on the Internet"

Russian legislation contains a number of norms establishing liability of citizens and organisations for statements and dissemination of information on the internet. The most resonant norm of recent years has become Article 207.3 of the Criminal Code of the Russian Federation "Public dissemination of knowingly false information about the use of the Armed Forces of the Russian Federation, the performance by state bodies of the Russian Federation of their powers". This article was introduced into the Criminal Code on 4 March 2022.[20]

This norm provides for criminal liability for the public dissemination, under the guise of reliable reports, of information which, in the opinion of law enforcement agencies and the court, is knowingly false and concerns the use of the Armed Forces of the Russian Federation or the performance by state bodies of the Russian Federation of their powers, including outside the territory of Russia.[21] The definition of "knowingly false" information in practice is often based on its non-compliance with the official position of state bodies, in particular the Ministry of Defence of the Russian Federation. Any criticism of the official version of events, presentation of alternative data or independent assessments can be interpreted as dissemination of "fakes". The law provides for severe penalties, including large monetary fines and imprisonment for up to 15 years (in the event of grave consequences).[25] After the introduction of this article, numerous criminal and administrative prosecutions of citizens, journalists and public activists for their publications and comments on the internet began, primarily concerning the conflict in Ukraine.[25]

In addition to Article 207.3 of the Criminal Code, there are other legislative acts regulating statements on the internet:

- Laws on liability for the dissemination of information expressing "clear disrespect" to society, the state, official state symbols, the Constitution of the Russian Federation or bodies exercising state power (the so-called "law on disrespect for authorities").
- Laws on liability for public calls for extremist or terrorist activities, as well as for justifying terrorism. The concepts of "extremism" and "justifying terrorism" can be interpreted quite broadly by law enforcement agencies.
- Laws on liability for slander.
- Legislation on the prohibition of rehabilitation of Nazism.

The introduction of Article 207.3 of the Criminal Code ("on fakes about the army")[20] and its active enforcement[25] became a direct response of the state to the need to establish strict control over the information field in the context of an armed conflict. The broad and vague wording of this article, as well as the severe sanctions provided for by it, are aimed at suppressing any information and opinions that contradict the official state version of events. This indicates a purposeful policy to establish a state monopoly on information about key events of important socio-political significance.

The "fakes law" and the practice of its application create a powerful "chilling effect" on freedom of speech on the internet. Citizens, journalists and the media, fearing prosecution, increasingly resort to self-censorship.[25] This leads to a significant narrowing of the space for open public discussion, independent journalism and criticism of the authorities' actions, which negatively affects the state

of civil society and the implementation of the constitutional right to freedom of speech and information. The uncertainty of the concept of "knowingly false information" and its dependence on the official interpretation of events increase the risks for anyone who publishes information different from that disseminated by state sources.

3.5. Legislation on Internet Blocking

In the Russian Federation, a ramified system of legislation has been formed and is constantly developing, allowing state bodies to block internet resources on a wide range of grounds. Blockings can be carried out both on the basis of a court decision and extrajudicially at the request of authorised state bodies, such as Roskomnadzor or the Prosecutor General's Office. The number of blocked internet resources is steadily growing, which indicates the active use of this tool of state control.

3.5.1. Legislation

Yes, in Russia there is extensive legislation regulating the procedure and grounds for blocking internet resources. The key regulatory legal acts in this sphere are:

- **Federal Law of 27.07.2006 No. 149-FZ "On Information, Information Technologies and Information Protection":** This law is fundamental and contains general provisions on the procedure for restricting access to information whose dissemination in the Russian Federation is prohibited. It defines the categories of prohibited information and the procedures for its blocking.
- **"Lugovoy Law" (amendments to Federal Law No. 149-FZ):** Grants the Prosecutor General's Office of the Russian Federation and its deputies the right to demand from Roskomnadzor immediate extrajudicial blocking of sites containing calls for mass riots, extremist activities, participation in unauthorised public events, as well as disseminating deliberately false socially significant information under the guise of reliable reports ("fakes") and information expressing clear disrespect for state authorities.
- **Legislation on the protection of children from information harmful to their health and development (Federal Law No. 436-FZ):** Establishes grounds for blocking resources containing child pornography, information on methods of committing suicide, information on methods of manufacture and use of narcotic substances, etc.
- **Legislation on copyright and related rights ("anti-piracy legislation"):** Provides for the possibility of blocking resources illegally distributing objects of copyright by court decision.

- **Legislation on countering extremist activity and terrorism:** Serves as a basis for blocking materials and resources recognised as extremist or terrorist.
- **Federal Law No. 90-FZ ("on the sovereign internet"):** Although not a direct law on blocking, it creates the technical infrastructure (in particular, TSPU) that is used to implement blockings initiated on the basis of other laws.[25]

3.5.2. Blocking Procedures

Blocking procedures for internet resources in Russia can be divided into two main types: judicial and extrajudicial.

- **Judicial procedure:** Restriction of access to information or an internet resource is carried out on the basis of a court decision that has entered into legal force. A lawsuit for recognition of information as prohibited for dissemination and for blocking a resource can be filed by an authorised state body (for example, the prosecutor's office, Roskomnadzor for certain categories of cases) or a copyright holder (in case of copyright infringement).
- **Extrajudicial procedure:** Provides for blocking resources by decision of authorised state bodies without prior judicial proceedings. This mechanism is most often used:
    - **By the Prosecutor General's Office of the Russian Federation and its deputies:** On the basis of the "Lugovoy law" for blocking sites with calls for mass riots, extremism, participation in unauthorised actions, dissemination of "fakes" about socially significant events or activities of state bodies, as well as information containing disrespect for authorities.
    - **By Roskomnadzor:** On appeals from other federal executive bodies (for example, the Federal Tax Service – in relation to sites with illegal gambling; the Federal Service for Alcohol Market Regulation – in relation to sites illegally trading alcohol; the Ministry of Internal Affairs – on issues of child pornography, dissemination of drugs, information on methods of committing suicide).
    - **By Roskomnadzor independently:** In relation to resources containing child pornography, information on methods of manufacture and use of narcotic drugs, psychotropic substances and their precursors, information on methods of committing suicide, as well as calls for committing suicide.

After a decision is made (judicial or extrajudicial), information about the resource (domain name, URL of the page, network address) is entered into the Unified Automated Information System "Unified Register of Domain Names, Page Pointers of Sites on the Internet and Network Addresses

Allowing to Identify Sites on the Internet Containing Information the Dissemination of Which in the Russian Federation is Prohibited" (EAIS "Unified Register"). Communication operators operating on the territory of Russia are obliged within the period established by law (usually 24 hours) to restrict access to resources entered into this register. Blocking can be carried out by various technical methods, including blocking by IP address, by URL, by domain name, as well as using technical means of countering threats (TSPU), which allow deep packet inspection (DPI) and more targeted traffic filtering.

The Freedom House report notes that blocking procedures carried out by Roskomnadzor often remain opaque, and access restrictions can be carried out in violation of procedural norms, including blocking sites without prior notification of their owners.[25]

3.5.3. Registries of Blocked Internet Resources

Yes, in the Russian Federation there is an official centralised register of internet resources containing information the dissemination of which is prohibited. This register is known as the Unified Automated Information System **"Unified Register of Domain Names, Page Pointers of Sites on the Internet and Network Addresses Allowing to Identify Sites on the Internet Containing Information the Dissemination of Which in the Russian Federation is Prohibited"** (abbreviated EAIS "Unified Register" or simply "Register of Prohibited Sites"). The maintenance of this register is entrusted to Roskomnadzor.[49]

Public access to the full database of this register is **limited**. Ordinary users cannot view the entire list of blocked resources. However, Roskomnadzor provides a public service on its official website (eais.rkn.gov.ru), which allows checking whether a specific URL address, domain name or IP address is in the register.[49] Communication operators licensed to provide communication services on the territory of the Russian Federation receive regular downloads from the register from Roskomnadzor to implement technical measures to restrict access to prohibited resources.

In addition to the official register, there are unofficial projects and initiatives that try to aggregate data on blockings and provide them in a more open form. One of the most well-known such projects is the register maintained by the public organisation "Roskomsvoboda".[50] These unofficial registers often collect information from various sources, including data available to communication operators, user messages, own technical measurements and analysis of public court and state body decisions.

There are both official and unofficial resources providing information on blocked sites in Russia:

1. **Official service for checking the presence of a resource in the Unified Register of Roskomnadzor:**
   - **Link:** http://eais.rkn.gov.ru/ [49]
   - **Description:** This service, provided by Roskomnadzor, allows any user to check whether a specific domain, URL of a page or IP address is entered into the Unified Register of Prohibited Sites. The service does not provide the full list of blocked resources, but only responds to a specific request about the status of the specified resource. Through the official website of Roskomnadzor (rkn.gov.ru), it is also possible to send a message about the presence of illegal information on the Internet.[52]
2. **Register of blocked sites of the "Roskomsvoboda" project:**
   - **Link:** https://reestr.rublacklist.net/ [50]
   - **Description:** This is a public project that since 2012 has been collecting and systematising information on blocking internet resources in Russia. "Roskomsvoboda" aggregates data from various sources, including official downloads (when they were available), data from communication operators, user messages and own technical research. The resource provides statistics on blockings, the possibility of searching its database, as well as an API for automated retrieval of information. It seeks to ensure greater transparency in the issue of internet censorship in the country.

In addition to these two main resources, there are other projects and tools that can track blockings, for example, Censor Tracker (extension from "Roskomsvoboda") [50], as well as international projects such as OONI (Open Observatory of Network Interference), which collect data on network anomalies indicating censorship.

3.5.4. Development of Blockings

Open Observatory of Network Interference (OONI) is an international project that collects and analyses data on internet censorship around the world, using specialised OONI Probe software for this purpose. OONI reports and data provide valuable information on the scale and methods of blockings in various countries, including the Russian Federation.

Analysis of OONI data, especially for the period after February 2022, shows a significant strengthening of internet censorship in Russia:

- **Almost complete blocking of independent media:** Practically all foreign (for example, BBC, Deutsche Welle) and independent Russian news websites (such as "Meduza", "Novaya Gazeta", The New Times) are blocked.[53]

- **Growth in the number of blocked domains:** According to OONI, if in 2023 139 news domains were confirmed blocked in Russia, then by September 2024 this number increased to at least 279 domains. This indicates ongoing and expanding suppression of independent sources of information.[53]
- **Technical methods of blockings:**
  - **TLS interference:** Most news site blockings in Russia, according to OONI, are implemented through interference in the process of establishing a TLS connection (TLS interference). This includes TLS session timeout or injection of an RST packet (connection reset) after sending a ClientHello message during the TLS handshake. Such methods indicate the use of deep packet inspection (DPI) systems that analyse the Server Name Indication (SNI) field in ClientHello to make a blocking decision.[53]
  - **DNS blockings:** Blockings at the DNS level are also applied, when a false or null response is returned when requesting the IP address of a blocked domain. These blockings are apparently implemented by providers in a decentralised manner and could have existed even before the mass introduction of TSPU.[53]
- **Centralised management of blockings:** Despite the fact that technical means of countering threats (TSPU) equipped with DPI are installed by each communication operator on its network (decentralised deployment), the decisions on blockings and lists of blocked resources themselves are probably managed centrally by Roskomnadzor. This is indicated by the simultaneity of blocking the same resources on the networks of different providers, as well as the correlation of blockings with the dates of entering resources into the Roskomnadzor register.[53]
- **"Censorship war" with the EU:** In response to the blocking of Russian state media (such as Sputnik and RT) in European Union countries, Russian authorities took retaliatory measures, blocking access to a number of European news publications on the territory of the Russian Federation. OONI recorded such blockings since August 2024.[53]
- **Opacity of blockings:** OONI notes that the implementation of internet censorship is becoming less transparent. If earlier users often saw a stub page informing about blocking, now blockings can be disguised as technical failures.[54]

Conclusion on the development of blockings: Data from OONI and other observers[25] confirm that Russia is systematically and constantly expanding the use of internet blockings, especially in relation to news resources, independent media and content that the authorities consider undesirable or "fake". Technical methods of blockings are becoming more sophisticated, with active use of DPI systems managed centrally. This practice seriously limits citizens' right to access information and freedom of expression. The evolution of legislation and blocking practice in Russia

demonstrates a clear transition from targeted restrictions (for example, on narrow categories of prohibited information, such as child pornography or drug propaganda) to large-scale political and news censorship, which has especially intensified after February 2022.

The opacity of blocking procedures[25] and limited public access to the full official register of blocked sites[49] create an atmosphere of legal uncertainty. This makes it difficult for resource owners and users to understand the exact reasons for blocking and the possibility of its effective contestation, which increases the risks of arbitrariness on the part of regulatory bodies and limits the right to access information and fair trial. The use of modern blocking technologies, such as DPI for SNI analysis and interference in TLS connections[53], indicates the state's significant technological potential in the field of internet control. This makes traditional methods of bypassing blockings less effective and requires users to search for more complex and technologically advanced solutions to maintain access to information.

A logical development and tightening of the blocking policy was the introduction in Russia since August–September 2025 of the mechanism of so-called "whitelists". This technology is applied during mass mobile internet shutdowns and represents a fundamental shift in the approach to censorship: instead of blocking individual "prohibited" resources (blacklist), access to the network is completely cut off, except for a limited list of pre-approved sites and services. Thus, the principle "everything that is not permitted is prohibited" is implemented.

The first experiments on the application of "whitelists" were recorded in September 2025 in a number of regions, including Dagestan, Tatarstan, Rostov and Volgograd oblasts. According to explanations from MinTsifry, the list of permitted resources included "the most in-demand and socially significant" Russian services: the "Gosuslugi" portal, sites of state bodies, social networks "VKontakte" and "Odnoklassniki", Yandex services, marketplaces Ozon and Wildberries, as well as personal accounts of communication operators. At the same time, the list is dynamic and can be updated weekly based on analysis of resource popularity.

The introduction of "whitelists" is the most radical step to date in restricting access to information and building an isolated digital ecosystem. This mechanism, currently operating only in mobile networks, allows the authorities at any moment to cut off users from the global internet, leaving them only access to state-approved services. This is not only a qualitatively new technological level of censorship, but also a serious blow to citizens' digital rights, creating conditions for complete control over the information field during shutdowns.

4. Human Rights Violations on the Internet

Numerous reports from both Russian and international human rights organisations, including Freedom House[25], Human Rights Watch[48], and "Roskomsvoboda"[25], as well as independent mass media, indicate systematic and large-scale violations of human rights in the Russian segment of the internet. These violations cover a wide range of rights, including freedom of expression, the right to access information, the right to privacy and the right to a fair trial.

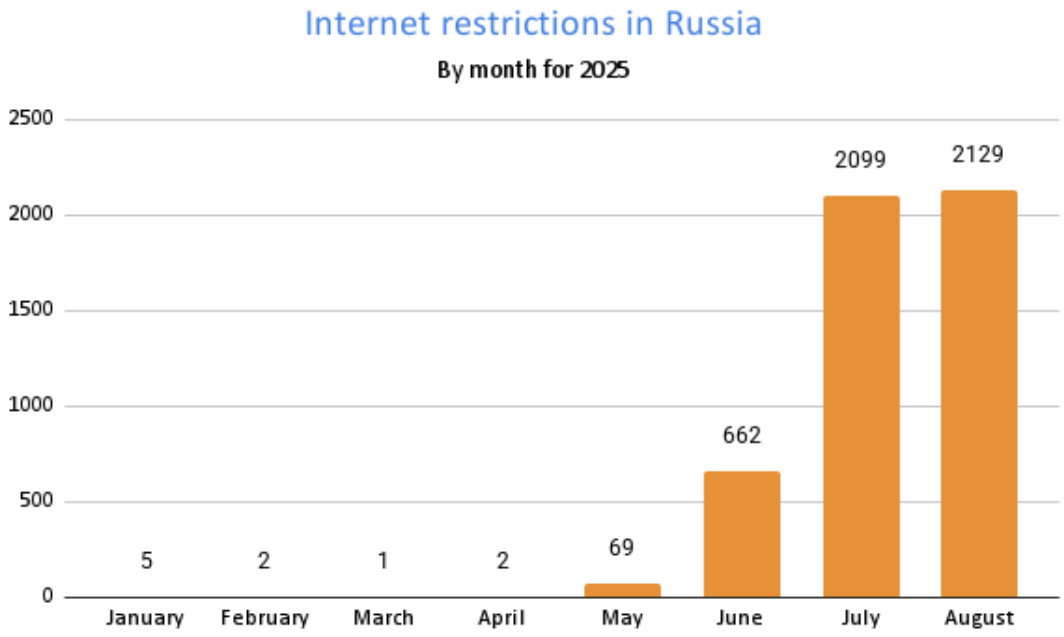
The situation has particularly worsened after February 2022, which is reflected in the sharp drop in Russia's positions in international internet freedom rankings.[25] Key manifestations of digital rights violations include: arbitrary and mass blockings of internet resources, including independent media and social networks; criminal and administrative prosecution of citizens for their statements on the internet, especially under new articles on "fakes" and "discreditation of the army"; increased pressure on independent media projects and non-governmental organisations working in the digital sphere; expansion of state surveillance practices and requirements for storing user data, which undermines the right to privacy.

4.1. Internet Shutdowns on Government Orders

The "sovereign internet law" created the technical and legal basis, which in 2025 was used for mass restriction of access to communications. If previously internet shutdowns by Russian authorities were recorded mainly outside the Russian Federation, in particular on the territory of Ukraine, then starting from May 2025 this practice began to be actively and massively applied inside Russia itself.

The situation changed dramatically in the summer of 2025, when after a series of drone attacks on military facilities deep inside the country, the authorities began to apply total mobile internet shutdowns as a countermeasure. This practice quickly turned from isolated cases into a mass phenomenon affecting dozens of regions. Monitoring and counting of mobile internet shutdown cases is carried out, in particular, by the "NaSvyazi" project, recording the geography and duration of shutdowns.

Graph 8: Dynamics of reports on internet shutdowns in regions of the Russian Federation for 2025



Thus, by the end of 2025, there was a qualitative shift in the policy of control over the internet. If previously the main emphasis was on filtering and blocking content, now mass shutdowns have been added to this as one of the key elements of control over the information space in Russia.

4.2. Criminalisation of Statements on the Internet

In the Russian Federation, there is a steady trend towards criminalisation of statements on the internet, especially those concerning socio-political topics, activities of state bodies and the Armed Forces. This leads to numerous cases of both criminal (imprisonment, suspended sentences) and administrative (fines, arrests) prosecution of citizens for their publications, comments, likes or reposts on social networks and other internet platforms.

The most resonant tool of such prosecution in recent years has become Article 207.3 of the Criminal Code of the Russian Federation ("on fakes about the army"), introduced in March 2022.[20] This article is actively applied to suppress information about the conflict in Ukraine that differs from the official position of the Russian authorities.

Examples of the most mentioned cases of prosecution:

- **Case of Maria Ponomarenko:** Journalist from Barnaul Maria Ponomarenko was sentenced in April 2023 to six years in a general regime colony under the article on "military fakes" (paragraph "d" part 2 of Article 207.3 of the Criminal Code of the Russian Federation) for a post in a Telegram channel about an airstrike on a drama theatre in Mariupol.[56] Later, already in the colony, another criminal case was initiated against her for an alleged attack on FSIN employees, for which her term was added.[56] Ponomarenko's case received wide public resonance, reports were made about serious problems with her psychological state in custody.
- **Case of Ilya Yashin:** Opposition politician Ilya Yashin was sentenced in December 2022 by the Meshchansky Court of Moscow to 8 years and 6 months in a general regime colony for disseminating "fakes" about the army motivated by political hatred (paragraph "d" part 2 of Article 207.3 of the Criminal Code of the Russian Federation).[58] The reason for criminal prosecution was his live broadcast on a YouTube channel dated 7 April 2022, in which he talked about events in the Ukrainian city of Bucha, including referring to international sources and media reports. The prosecution claimed that Yashin "affirmatively reported under the guise of reliable information" that Russian military killed residents of Bucha. Yashin did not admit guilt, insisting that he presented various points of view and fulfilled his civic duty by critically evaluating information.[58]

In addition to these high-profile cases, there are many other cases of bringing to responsibility under Article 207.3 of the Criminal Code, as well as under other articles, such as "discreditation of the use of the Armed Forces of the Russian Federation" (Article 280.3 of the Criminal Code and Article 20.3.3 of the Administrative Offences Code), articles on extremism, justifying terrorism, disrespect for authorities and slander. The Freedom House report for 2022 indicates that after the adoption of the law on "fakes", Russians began to be fined and prosecuted more often for publications and comments on social networks, and on 8 July 2022 the first criminal sentence was passed under the new article.[25] In at least 53 countries of the world (including Russia, according to the context of the report), users faced legal consequences for self-expression on the internet, up to long prison terms.[25]

Such law-enforcement practice creates an atmosphere of fear and contributes to self-censorship among internet users fearing prosecution for expressing their opinion, even if it is based on open sources or is an evaluative judgment.

4.3. Persecution of Media and NGOs

Mass media and non-governmental organisations (NGOs) in Russia, especially those that take an independent position or criticise the actions of the authorities, are subjected to significant pressure, including for their activities and publications on the internet. This pressure manifests in various forms:

- **Blockings of internet resources:** After 24 February 2022, Russian authorities have practically completely blocked access to foreign (for example, BBC, Deutsche Welle) and independent Russian media and social networks.[25]
- **Legislation on "foreign agents" and "undesirable organisations":** Legislation on "foreign agents" is widely applied, which imposes burdensome requirements for reporting, labelling materials and audit on media and NGOs, as well as individuals receiving foreign funding (even indirect) and engaged in "political activity" (interpreted very broadly). Many independent media and NGOs have been included in the registers of "foreign agents", which significantly complicates their work, leads to loss of advertisers, audience trust and creates risks of persecution. Activities of organisations recognised as "undesirable" on the territory of the Russian Federation are completely prohibited, and cooperation with them entails criminal liability. The law on "foreign agents" has been significantly expanded.[25]
- **Fines and administrative pressure:** Media and NGOs, as well as their heads and employees, are regularly subjected to large fines for non-compliance with legislation requirements (for example, for the absence of "foreign agent" labelling, for refusal to delete "prohibited content" at the request of Roskomnadzor). Roskomnadzor has repeatedly fined online platforms for refusal to delete content and localise user data.[25]
- **Criminal prosecution of journalists and NGO employees:** Journalists and NGO employees may be subjected to criminal prosecution under various articles, including "fakes about the army", "discreditation of the army", "extremism", "slander".
- **Forced cessation of activities or relocation:** Due to imposed fines, access blockings to sites, as well as persecutions of individual journalists, some media were forced to cease their activities in Russia or transfer their editorial offices abroad in order not to expose their employees to even greater danger.[25]
- **Recognition of Meta as an extremist organisation:** The decision of a Russian court to recognise Meta (owning Facebook and Instagram) as an extremist organisation and ban its activities in the Russian Federation created additional risks for users of these platforms and for businesses using them for promotion.[25]

The Human Rights Watch report for 2020 analysed the totality of laws adopted since 2017 (including the "Yarovaya package"), which provided Russian authorities with broad opportunities for control over internet infrastructure and digital activity, which directly affects the activities of media and NGOs.[48] The US State Department report on human rights practices in Russia for 2022 also highlights problems related to arbitrary or unlawful interference with privacy, which is relevant for the activities of online media and NGOs.[60]

These measures lead to a significant reduction in the space for independent journalism and civil society activities in Russia, restriction of citizens' access to alternative sources of information and strengthening of state propaganda.

5. Civil Society in the Field of Internet Governance

Civil society in the Russian Federation dealing with issues of internet governance and protection of digital rights operates in difficult conditions. On the one hand, there is a number of organisations and activists who seek to defend the principles of freedom of information, privacy and openness of the network. On the other hand, their activities face increasing pressure from the state, legislative restrictions and narrowing of the space for public discussion and influence on decision-making.

Despite this, civil society organisations continue to play an important role in monitoring violations of digital rights, providing legal assistance to victims, educating users on cybersecurity and bypassing blockings, as well as attempting to participate in the discussion of legislative initiatives concerning the internet. They also contribute to raising public awareness of internet censorship issues and the need to protect digital freedoms.

5.1. Organisations

Several organisations operate in Russia that actively deal with protecting citizens' rights on the internet, monitoring legislation and law-enforcement practice, as well as educational activities. Among them, the following can be highlighted:

- **"Roskomsvoboda":**
  - **Description:** "Roskomsvoboda" is one of the leading Russian public organisations specialising in the protection of digital rights and promotion of ideas of freedom of information, privacy and anonymity on the internet. The organisation was created in 2012 in response to the introduction of the Unified Register of Prohibited Sites. "Roskomsvoboda" monitors blockings of internet resources (project

reestr.rublacklist.net), analyses legislative initiatives in the field of internet regulation, provides legal assistance to citizens and organisations whose digital rights have been violated, conducts public campaigns and educational events.[50] The technical team of "Roskomsvoboda" also develops tools for bypassing censorship and improving digital security, such as the Censor Tracker extension and the VPNlove.me marketplace for VPN services.[50]

- **Internet resource:** https://roskomsvoboda.org/ [61]

- **International human rights group "Agora":**
  - **Description:** "Agora" is an association of lawyers and advocates providing legal assistance in cases related to human rights violations in Russia, including cases of freedom of speech, freedom of assembly and persecution of activists, journalists and bloggers for their statements on the internet. "Agora" was founded in 2005 and handled many high-profile cases, defending citizens from illegal actions of state officials.[62] Although the main focus of "Agora" is broader than just digital rights, a significant part of their work is related to protecting rights in the online space. In 2014, the organisation was awarded the international Rafto human rights prize. Subsequently, Russian authorities recognised the "Agora" Association as a "foreign agent", and in 2016 it was liquidated by court decision. The international human rights group "Agora" continued its activities, but in June 2023 the Prosecutor General's Office of the Russian Federation recognised its activities as "undesirable" on the territory of Russia.[62]
  - **Internet resource:** agora.legal (main site of the international group), openinform.ru (mentioned as a site in Wikipedia for the previously existing organisation).[62]
- **Society for Internet Protection (OZI):**
  - **Description:** a Russian public organisation founded in 2016, which deals with research on freedom and connectivity of the internet in Russia. The organisation monitors and analyses legislative initiatives aimed at regulating the network, tracks cases of blockings and shutdowns, as well as conducts projects to measure the level of internet penetration and connectivity of regions. OZI regularly publishes reports, studies and comments on key issues of Runet development, advocating for the preservation of its openness and accessibility.
  - **Internet resource:** https://ozi-ru.net/

In addition to these organisations, there are other groups, lawyers and activists who contribute to the protection of digital rights in Russia, but their activities are often less formalised or covered in the provided materials.

5.2. VPN and Means of Bypassing Blockings

The use of VPN (Virtual Private Network) and other means of bypassing blockings has become widespread in Russia, especially against the background of tightening internet censorship and blocking popular foreign social networks, news resources and other websites. VPN services allow users to access blocked content, as well as increase their level of anonymity and privacy on the network.

Russian authorities are taking active steps to restrict access to VPN services themselves and the protocols they use, as well as to information on ways to bypass blockings. This creates a kind of "arms race" between regulators seeking to fully control the information space and users seeking ways to preserve access to the global network.

5.2.1. Status of VPN Services

Formally, the use of VPN services by citizens for personal purposes in Russia is **not prohibited**.[64] However, since 2017, legislation has been in force (amendments to Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection"), which obliges owners of VPN services and anonymisers to connect to the Federal State Information System (FGIS) containing a register of blocked sites, and to filter the traffic of their users, not allowing them to prohibited resources.[65] VPN services that refuse to comply with these requirements may be blocked by Roskomnadzor.

From 1 March 2024, a Roskomnadzor order came into force, which introduces criteria for blocking sites containing information on ways to bypass blockings established in Russia. This includes a ban on popularising VPN services that do not comply with Russian legislation (i.e. do not filter traffic).[66] From 30 November 2024, restrictions should also extend to scientific, scientific-technical and statistical information on ways to bypass blockings.[66]

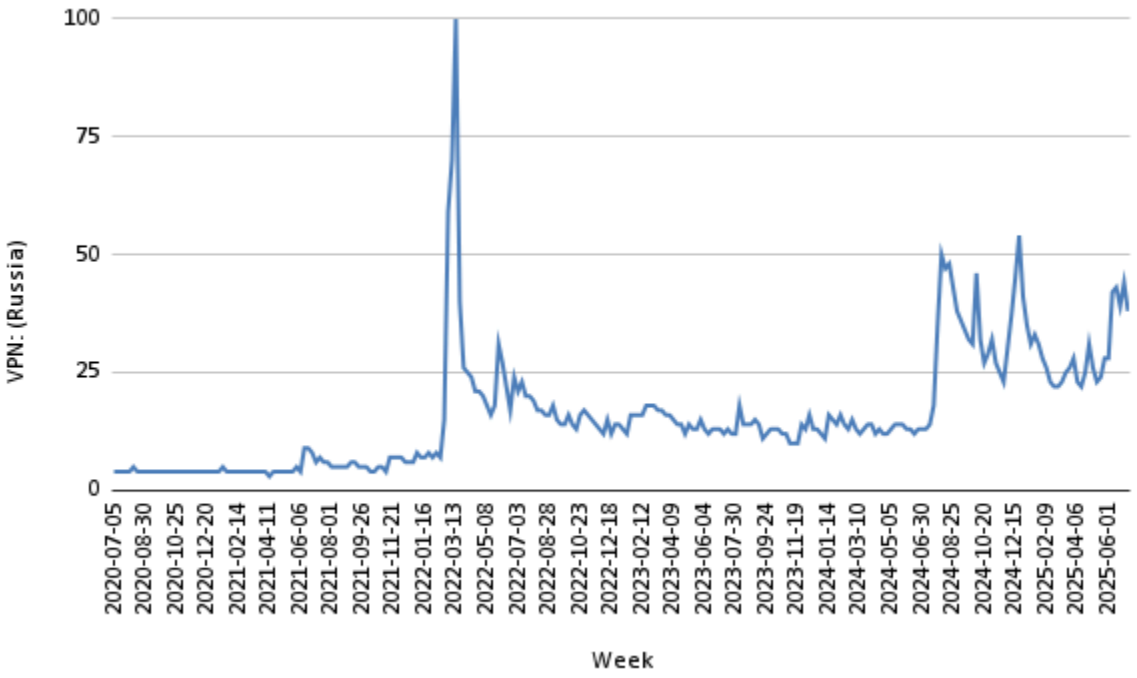
The main laws regulating this sphere:

- **Federal Law of 27.07.2006 No. 149-FZ "On Information, Information Technologies and Information Protection"** (as amended by Federal Law of 29.07.2017 No. 276-FZ, which introduced provisions on VPN and anonymisers).[65]
- **Roskomnadzor orders** establishing the procedure for blocking VPN services and information about them.

5.2.2. Number of VPN Users

It is difficult to collect exact data on the number of VPN users in Russia by year, as many studies rely on surveys or indirect estimates. Nevertheless, the available data indicate a significant growth in the popularity of VPN services, especially after February 2022.

Graph 9: Dynamics of search queries about VPN in the Russian Federation (2020–2025)



Source: trends.google.com

Analysis of the dynamics of search queries on the topic “VPN” in Russia demonstrates a cardinal change in the role of this technology for users and directly correlates with the stages of strengthening state internet censorship.

The graph is clearly divided into three periods. Before the beginning of 2022, interest in VPN was at a stably low, background level, which speaks of its use mainly by a technically savvy, niche audience. From March 2022, the situation radically changes: VPN transforms into a mass tool necessary for access to basic information resources. This is confirmed by both peak values and the establishment of a new, significantly higher base level of interest in the technology throughout the subsequent time period.

Peaks of search activity are a direct indicator of the population's reaction to the regulator's actions (Roskomnadzor) and serve as an accurate marker of the introduction of new restrictions.

Absolute peak (March 2022): The maximum value (100) was reached in the period from the end of February to mid-March 2022. This explosive growth in interest is unambiguously associated with the beginning of full-scale hostilities in Ukraine and the subsequent unprecedented in scale blockings. In this short period, almost all foreign (Facebook, Instagram, Twitter) and many independent news publications were blocked in Russia. This peak represents a one-time, "shock" reaction of millions of users who for the first time faced the impossibility of accessing familiar platforms.

A series of peaks (from August 2024): The second wave of high activity, which began in August 2024, is associated with the application of a new tactic of restriction — the so-called "slowdown" of traffic to the YouTube video hosting. Unlike full blocking, throttling makes the use of the service practically impossible due to constant buffering of videos and low loading speed. In this situation, VPN becomes for users a key tool not so much for bypassing blocking as for restoring basic operability and acceptable access speed to critically important video content.

The wave-like nature of demand in this period is explained by the fact that users are looking not just for any VPN, but for one that effectively copes with bypassing throttling. This indicates a new, more complex stage of confrontation, when the regulator tries to restrict access to individual services without blocking them completely, and users are forced to constantly search for and test new technological solutions to maintain access quality to the Internet.

According to Forbes for December 2023, the main age of VPN users is 35–44 years (63% of those using VPN in this group). At the same time, the share of users aged 25–34 increased by 10 p.p. compared to 2022.[69] Among young people aged 18–24, more than half use VPN — 62% of respondents (Levada Center data for March 2023).[68]

Blockings of VPN services and protocols:

Roskomnadzor actively blocks VPN services that do not cooperate with the authorities and allow bypassing blockings. Blockings are carried out both by entering IP addresses and domains of VPN services themselves into the register of prohibited sites, and by blocking VPN protocols using TSPU (DPI).

Chronology of protocol blockings[66]:

- **September 2021:** Beginning of blocking VPN services (VyprVPN, Opera VPN).
- **2022:** Attempts to block services through API hosts, IP addresses; reports of blocking IPsec and IKEv2 in some regions.
- **Beginning of 2023:** Blockings of OpenVPN and IKEv2 protocols.
- **May, August, September 2023:** Waves of partial and temporary blockings of OpenVPN, IKEv2, IPSec, WireGuard. By the end of September, WireGuard stopped working for about 20% of users.
- **2024:**
  - From 1 August 2024 — blocking WireGuard in many regions.
  - From 15 October 2024 — blocking Shadowsocks on mobile internet.
  - OpenVPN is more actively blocked.
  - Reports of blocking Outline (VPN client).
  - Blockings often are not mass and not long-term, protocols can become available and unavailable again.[66]
- **Removal from app stores:** In July 2024, Apple at the request of Roskomnadzor began removing VPN applications from the Russian AppStore.[66]

Methods of blocking include: entering VPN sites into the register, blocking server IP addresses, blocking protocols using TSPU (DPI), removing applications from stores, ban on popularisation of VPN.[66]

5.2.3. Cases of Persecution for Using VPN

In the provided materials, there is no information on cases of criminal or administrative prosecution of ordinary users solely for the fact of using VPN services for personal purposes. The current legislation does not provide for direct liability for citizens for using VPN to access blocked resources.

However, several aspects should be taken into account:

1. **Liability for dissemination of information:** If a user using VPN gains access to prohibited information and then disseminates it (for example, makes a repost), he may be held liable for the dissemination of this information itself (for example, under articles on “fakes”, extremism, etc.), regardless of whether VPN was used to access the original source.

2. **Liability for owners of VPN services:** Legislation provides for liability for owners of VPN services and anonymisers for refusal to cooperate with the authorities (non-connection to FGIS, non-filtering of traffic).
3. **Deanonymisation:** Using VPN does not guarantee complete anonymity, and in case of committing illegal actions using VPN, law enforcement agencies may attempt to establish the user's identity.

Information on the persecution of **organisations providing VPN services** in the provided materials is reduced to their blockings by Roskomnadzor and requirements for connection to FGIS. There are no direct data on criminal cases against owners of VPN services specifically for providing VPN services (and not for related offences) in these materials.

5.2.4. Monitoring of Blockings

Several organisations and projects are engaged in monitoring blockings of internet resources in Russia:

1. **"Roskomsvoboda":**
   - Maintains a publicly available register of blocked sites (reestr.rublacklist.net).[50]
   - Publishes news and analytics on the topic of blockings and internet censorship.
   - Develops tools for monitoring and bypassing blockings (for example, Censor Tracker).[50]
   - **Digest of messages (based on the provided materials):**
     - **December 2022:** "Roskomsvoboda" reported blocking 14.8 thousand sites per week (5–11 December), which was significantly higher than the average indicator (4.9 thousand sites per week in 2022). It was noted that such mass blockings had not been observed since 2018 and 2021. The majority of blockings (60%) were carried out by court decisions, 14% — by decisions of an unnamed department (presumably the Prosecutor General's Office).[51]
     - **General activities:** "Roskomsvoboda" since its foundation in 2012 tracks legislative activities and law enforcement in the field of internet regulation, covers high-profile cases of blockings, tightening of laws and persecution of citizens.[61]
2. **OONI (Open Observatory of Network Interference):**
   - An international project collecting data on internet censorship around the world using OONI Probe tests.[54]
   - Publishes reports and data on blockings in Russia.
   - **Digest of messages (based on the provided materials):**

- **Report "Censorship Chronicles: The systematic suppression of the independent media in Russia" (published in 2024, covers the period from September 2023 to September 2024):** Confirmed blocking of at least 279 news domains (growth from 139 in the previous 2023 study). Most blockings are implemented through TLS interference (using DPI/TSPU), DNS blockings are also applied. Blockings are probably managed centrally by Roskomnadzor. Noted "censorship war" with the EU.[53]
- **General data (February 2025):** OONI collected more than two billion network measurements in more than 200 countries. OONI Explorer is one of the largest open databases on internet censorship. In its latest messages, OONI indicated the blocking of Discord in Russia.[54]

3. **Other projects:** There may be other local or international initiatives tracking the availability of internet resources in Russia, but they were not detailed in the provided materials.

Monitoring of blockings shows that internet censorship in Russia is a dynamic and constantly evolving process. The authorities not only expand the list of grounds for blockings and the number of blocked resources, but also improve technical methods of their implementation, seeking to make bypassing restrictions more difficult for users.

6. Conclusion

Analysis of the state of digital rights and the internet in the Russian Federation for the period from 2019 to 2025 reveals a complex and contradictory picture. On the one hand, Russia demonstrates a high level of internet penetration, development of digital services and the presence of modern telecommunications infrastructure in large cities. On the other hand, this period is characterised by consistent and significant strengthening of state control over the internet space, which leads to substantial restrictions on citizens' digital rights and freedoms.

Compliance with human rights in the field of access to information:

The right to access information in Russia is subjected to serious restrictions. This manifests through:

1. **Large-scale blockings of internet resources:** Almost complete blocking of foreign (for example, BBC, Deutsche Welle) and independent Russian media and social networks.[25]

2. **Legislation on "fakes" and "discreditation":** The introduced norms, especially Article 207.3 of the Criminal Code, have created a legal basis for prosecuting information about socio-political events that does not correspond to the official state position.[25]
3. **Pressure on media and NGOs:** Independent media and NGOs face unprecedented pressure, including blockings, assignment of "foreign agent" and "undesirable organisation" statuses, fines and persecution of employees. This leads to a reduction in the number of independent sources of information.[25]
4. **Control over infrastructure:** The "sovereign internet law" has created prerequisites for centralised management of Runet, including the possibility of its isolation.
5. **Restriction of the use of means of bypassing blockings:** The state is making efforts to block VPN services and information on ways to bypass censorship, seeking to limit citizens' access to blocked resources.

Taken together, these factors indicate the systemic nature of violations of the right to free access to information. State policy is aimed at forming a controlled information space where the official point of view dominates.

Forecast of event development:

- **Neutral scenario (stagnation with elements of further tightening):**
  - Preservation of the current level of state control over the internet with periodic "tightening of the screws" in response to internal or external political events.
  - Continuation of blockings of "undesirable" resources and VPN services, but without total disconnection from the global network.
  - Further development of national digital infrastructure (NSUD, TSPU) to increase the efficiency of traffic filtering and control.
  - Continuation of law-enforcement practice under articles on "fakes" and "discreditation", but without a sharp increase in the scale of repressions if there are no significant destabilising factors.
  - Gradual "squeezing out" of foreign digital platforms and services from the Russian market and their replacement with national analogues under tighter state control.
  - Preservation of a high level of self-censorship among users and media.
- **Positive scenario (weakening of regulation, liberalisation):**
  - This scenario seems unlikely in the current political and geopolitical conditions.
  - Theoretically, it could include:
    - Softening or cancellation of the most repressive laws (on "fakes", on "disrespect for authorities", on "foreign agents" in their current form).

        - Reduction of the practice of extrajudicial blockings, increasing the transparency of procedures for restricting access to information.
        - Cessation of prosecution for peaceful statements on the internet.
        - Reduction of pressure on independent media and NGOs.
        - Refusal of plans to isolate Runet and more open interaction with the global internet community.
    - For the implementation of such a scenario, deep political changes in the country are necessary.
- **Negative scenario (strengthening of censorship, "digital iron curtain"):**
    - Further tightening of legislation, expansion of grounds for blockings and criminal prosecution for online activity.
    - Strengthening of technical measures to block VPN and other means of anonymisation, up to attempts to block by protocols at the national level.
    - More active use of artificial intelligence technologies for monitoring and identifying "undesirable" content and users.
    - Gradual or abrupt (in case of a crisis situation) restriction of access to global internet services and platforms, up to complete isolation of the Russian internet segment ("Chinese option" with a national firewall).
    - Gradual or abrupt restriction of access to global internet services and platforms.
    - This scenario can be implemented in case of escalation of internal political tension, intensification of external pressure or adoption of a strategic decision on building a completely autarkic digital ecosystem.

Taking into account current trends, the most likely seems to be the development of events according to a scenario close to neutral, with a constant risk of shifting towards a negative scenario when external or internal conditions change. The state of digital rights in Russia will remain a subject of serious concern both for the country's citizens and for the international community.

Sources

1. Russian Federation | Data, date of last access: June 13, 2025, https://data.worldbank.org/country/russian-federation
2. Digital in The Russian Federation — DataReportal – Global Digital ..., date of last access: June 13, 2025, https://datareportal.com/digital-in-the-russian-federation
3. Digital 2024: The Russian Federation - DataReportal, date of last access: June 13, 2025, https://datareportal.com/reports/digital-2024-russian-federation
4. Digital 2025: The Russian Federation — DataReportal – Global ..., date of last access: June 13, 2025, https://datareportal.com/reports/digital-2025-russian-federation
5. Population size, date of last access: June 13, 2025, https://rosstat.gov.ru/bgd/regl/b11_13/IssWWW.exe/Stg/d1/04-02.htm
6. GDP of Russia - TAdviser, date of last access: June 13, 2025, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%92%D0%92%D0%9F_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
7. Russia GDP - Trading Economics, date of last access: June 13, 2025, https://tradingeconomics.com/russia/gdp
8. Economy of Russia - Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
9. Gross domestic product of Russia — Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%92%D0%B0%D0%BB%D0%BE%D0%B2%D0%BE%D0%B9_%D0%B2%D0%BD%D1%83%D1%82%D1%80%D0%B5%D0%BD%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
10. Archive of currency exchange rates of the Central Bank of the Russian Federation, view currency exchange rates ... - Myfin.by, date of last access: June 13, 2025, https://myfin.by/currency/cb-rf-archive
11. World Bank confirms forecast for Russia's GDP growth at 1.6% in 2025, 1.1% in 2026, date of last access: June 13, 2025, https://interfax.com/newsroom/top-stories/109215/
12. Archive of dollar exchange rates of the Central Bank of the Russian Federation, view the dollar exchange rate of the Central Bank of Russia on the selected date - Myfin.by, date of last access: June 13, 2025, https://myfin.by/currency/cb-rf-archive/usd

13. FORMATION OF THE INSTITUTE OF “SOVEREIGN INTERNET” IN THE RUSSIAN FEDERATION Text of scientific article in the speciality “Political Sciences” - CyberLeninka, date of last access: June 13, 2025, https://cyberleninka.ru/article/n/formirovanie-instituta-suverennogo-interneta-v-rossiyskoy-federatsii
14. Law on “sovereign internet - Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%BE_%C2%AB%D1%81%D1%83%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%BE%D0%BC_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%C2%BB
15. CURRENT PROBLEMS OF THE RUSSIAN ECONOMY - Modern Europe, date of last access: June 13, 2025, http://www.sov-europe.ru/images/pdf/2015/3/Kudrov_3-2015.pdf
16. Structural problems of economic growth of the Russian Federation Text of scientific article in the speciality “Economics and Business - CyberLeninka, date of last access: June 13, 2025, https://cyberleninka.ru/article/n/strukturnye-problemy-ekonomicheskogo-rosta-rossiyskoy-federatsii
17. State system of Russia — Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%B9_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
18. Administrative-territorial division of Russia - IS MUNI, date of last access: June 13, 2025, https://is.muni.cz/el/phil/jaro2017/RJ_67/administrativnoe_delenie_RF.pdf
19. Territorial division of Russia - Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D1%80%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
20. 207.3: “Fakes” about the army - Tilda, date of last access: June 13, 2025, http://longreads.mr7.tilda.ws/statia_2073
21. What can no longer be written about the Armed Forces of the Russian Federation and the work of state bodies abroad?, date of last access: June 13, 2025, https://mmdc.ru/blog/2022/03/04/chto-teper-nelzya-pisat-o-vooruzhennyh-silah-rf/
22. .ru — Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/.ru
23. About the Coordination Center for domains .RU/.РФ, date of last access: June 13, 2025, https://cctld.ru/about/
24. Roskomnadzor - Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D0%BA%D0%BE%D0%BC%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80

25. Freedom on the Net 2022: Russia ranked 65 out of 70 in ..., date of last access: June 13, 2025, https://roskomsvoboda.org/post/freedom-on-the-net-2022/
26. Make it in 6 days: overview of internet audience, date of last access: June 13, 2025, https://mediascope.net/upload/iblock/9da/f39jd547adzptf0mu2j1tlmw44pjgt5d/Mediascope_%D0%9D%D0%A0%D0%A4_6%20%D1%81%D1%83%D1%82%D0%BE%D0%BA.pdf
27. Mediascope: monthly internet audience in the Russian Federation is ..., date of last access: June 13, 2025, https://habr.com/ru/news/858782/
28. Internet users for the Russian Federation (ITNETUSERP2RUS) | FRED | St. Louis Fed, date of last access: June 13, 2025, https://fred.stlouisfed.org/series/ITNETUSERP2RUS
29. The volume of the Russian BBA market in the b2c segment reached 42.2 billion rubles in the 2nd quarter of 2024 | Kabelshchik, date of last access: June 13, 2025, https://www.cableman.ru/content/obem-rossiiskogo-rynka-shpd-v-b2c-segmente-dostig-422-mlrd-rublei-v-2-kvartale-2024-goda
30. Internet access (Russian market) - TAdviser, date of last access: June 13, 2025, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%28%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8%29
31. The Russian telecom market is growing thanks to non-telecommunications services. Overview: Telecom 2024 - CNews, date of last access: June 13, 2025, https://www.cnews.ru/reviews/telekom_2024/articles/rossijskij_telekom-rynok_rastet
32. Communications in Russia — Wikipedia, date of last access: June 13, 2025, https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D1%8F%D0%B7%D1%8C_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
33. Speedtest Global Index – Internet Speed around the world ..., date of last access: June 13, 2025, https://www.speedtest.net/global-index
34. Internet in Russia: what does statistics say? | Experts explain from Roskachestvo, date of last access: June 13, 2025, https://rskrf.ru/tips/eksperty-obyasnyayut/internet-stats/
35. Russia promised 100-fold increase in internet speed - CNews, date of last access: June 13, 2025, https://www.cnews.ru/news/top/2024-03-06_rossii_predrekli_100-kratnyj
36. Ookla updated the ranking by speed of mobile and broadband internet, date of last access: June 13, 2025, https://timeweb.com/ru/community/articles/ookla-obnovili-reyting-po-skorosti-mobilnogo-i-shirokopolosnogo-interneta
37. Focus on Russia - RIPE NCC Statistics and Data, date of last access: June 13, 2025, https://labs.ripe.net/author/fergalc/focus-on-russia-ripe-ncc-statistics-and-data/

38. date of last access: January 1, 1970, https://stat.ripe.net/country/RU#tabId=routing
39. IPv6 Adoption - Google, date of last access: June 13, 2025, https://www.google.com/intl/en/ipv6/
40. Why IPv6 is faster and how to implement it. X-COM case study - VAS Experts, last accessed: June 13, 2025, https://vasexperts.ru/blog/ipv4-i-ipv6/pochemu-ipv6-bystree-i-kak-ego-vnedrit-kejs-x-com/
41. IPv6 Adoption Statistics: a Comparison of Different Metrics - RIPE Labs, last accessed: June 13, 2025, https://labs.ripe.net/author/wilhelm/ipv6-adoption-statistics-a-comparison-of-different-metrics/
42. IPv6 Users by Country - APNIC Labs, last accessed: June 13, 2025, https://labs.apnic.net/dists/v6dcc.html
43. IPv6 Capability Metrics - APNIC Labs Measurements, last accessed: June 13, 2025, https://stats.labs.apnic.net/ipv6/RU
44. Russia surpasses the USA in IPv6 adoption (60% vs. 48%) - Reddit, last accessed: June 13, 2025, https://www.reddit.com/r/ipv6/comments/1ggash9/russia_surpasses_the_usa_in_ipv6_adoption_60_vs_48/
45. Internet Governance - Coordination Center for TLD RU/РФ, last accessed: June 13, 2025, https://cctld.ru/help/wiki/upravlenie-internetom/
46. Lipov, Andrey Yuryevich - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/Липов,_Андрей_Юрьевич
47. Structure - Roskomnadzor, last accessed: June 13, 2025, https://rkn.gov.ru/about/structure/
48. Russia: Growing Internet Isolation, Control, and Censorship | Human Rights Watch, last accessed: June 13, 2025, https://www.hrw.org/ru/news/2020/06/18/russia-growing-internet-isolation-control-censorship
49. Unified Register of Prohibited Websites — Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/Единый_реестр_запрещённых_сайтов
50. Roskomsvoboda - Wikipedia, last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/Роскомсвобода
51. “Roskomsvoboda”: Nearly 15,000 resources added to the blocked sites registry in one week — Meduza, last accessed: June 13, 2025, https://meduza.io/news/2022/12/12/roskomsvoboda-v-reestr-zablokirovannyh-saytov-za-nedelyu-vnesli-pochti-15-tysyach-resursov
52. Roskomnadzor | Federal Service for Supervision of Communications, Information Technology and Mass Media, 2025 | VKontakte, last accessed: June 13, 2025, https://vk.com/rkn

53. Censorship Chronicles: The systematic suppression of independent media in Russia, last accessed: June 13, 2025, https://ooni.org/post/2024-russia-report/
54. OONI | Open Observatory of Network Interference | Censorship | Internet | Websites | Apps - Digital Rights Community, last accessed: June 13, 2025, https://www.digitalrights.community/blog/community-series-ooni
55. Freedom of speech in Russia. Joint report for the 4th cycle of the UN Universal Periodic Review | OVD-Info, last accessed: June 13, 2025, https://reports.ovd.info/svoboda-slova-v-rossii
56. Journalist Maria Ponomarenko sentenced to 1 year and 10 months in prison, last accessed: June 13, 2025, https://www.svoboda.org/a/zhurnalistku-mariyu-ponomarenko-osudili-na-god-i-10-mesyatsev-kolonii/33361563.html
57. Journalist Ponomarenko from Barnaul had her sentence extended for assaulting an FSIN officer - Interfax, last accessed: June 13, 2025, https://www.interfax.ru/russia/1016904
58. Ilya Yashin sentenced to 8.5 years in prison in “military fakes” case, last accessed: June 13, 2025, https://www.bbc.com/russian/news-63864402
59. Court finds Yashin guilty in “fakes about the army” case | Forbes.ru, last accessed: June 13, 2025, https://www.forbes.ru/society/482143-sud-priznal-asina-vinovnym-po-delu-o-fejkah-pro-armiu
60. 2022 Country Reports on Human Rights Practices: Russia - U.S. State Department, last accessed: June 13, 2025, https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/russia/
61. Roskomsvoboda, last accessed: June 13, 2025, https://roskomsvoboda.org/about/
62. Agora (organization) - Wikipedia (EN), last accessed: June 13, 2025, https://en.wikipedia.org/wiki/Agora_(organization)
63. Agora (organization) - Wikipedia (RU), last accessed: June 13, 2025, https://ru.wikipedia.org/wiki/Агора_(организация)
64. Ban on the use and advertising of VPN: myth or reality? - FirstVDS, last accessed: June 13, 2025, https://firstvds.ru/blog/zapret-na-ispolzovanie-i-reklamu-vpn-mif-ili-realnost
65. VPN ban in Russia: laws and their practical application | AdminVPS Blog, last accessed: June 13, 2025, https://adminvps.ru/blog/vpn-v-rossii-zaprety-i-ih-prakticheskoe-primenenie/
66. Timeline of VPN blocking in Russia 2019–2024. Where we are heading - Habr, last accessed: June 13, 2025, https://habr.com/ru/companies/amnezia/articles/861198/
67. Companies using VPN are advised to abandon foreign encryption protocols - Interfax, last accessed: June 13, 2025, https://www.interfax.ru/russia/1020310
68. After YouTube throttling, the number of VPN users in Russia reached 36%, last accessed: June 13, 2025,

https://www.agents.media/posle-zamedleniya-youtube-chislo-polzovatelej-vpn-v-rossii-dostiglo-36/
69. Number of VPN users in Russia grew by almost 40% in 2023, last accessed: June 13, 2025, https://www.forbes.ru/tekhnologii/501873-kolicestvo-pol-zovatelej-vpn-v-rossii-vyroslo-pocti-na-40-v-2023-godu
70. POPULATION SIZE, last accessed: June 13, 2025, https://rosstat.gov.ru/bgd/regl/b05_13/IssWWW.exe/Stg/04-02.htm
71. World Development Indicators | DataBank, last accessed: June 13, 2025, https://databank.worldbank.org/data/reports.aspx?source=2&country=RUS
72. Political system of Russia: structure, government bodies - Russian Society “Znanie”, last accessed: June 13, 2025, https://znanierussia.ru/articles/Государственный_строй_России
73. Government of Russia official website, last accessed: June 13, 2025, http://government.ru/