e-ISSN **3041-2498**

Public Management and Policy

https://www.eu-scientists.com/index.php/pmap

Building a "Sovereign Internet": Russia's Digital Policies as a Tool of Censorship and Social Control

Sude Güvenç [1] *

[1] *Istanbul University (Turkey). Independent Researcher, Graduate of Department of Political Science and International Relations.*

*** *Corresponding Author,*** e-mail: guvenccsude@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3041-2498/2025.12.13

Received:
10 November 2025
Accepted:
14 December 2025
Published online:
21 December 2025

ABSTRACT

Russia has increasingly focused on developing comprehensive digital policies aimed at establishing "digital sovereignty" which seeks to reduce dependence on foreign technologies, internet infrastructure, and multinational platforms. These policies integrate internet governance, media regulation, cybersecurity, and content monitoring under the overarching concept of "information security". The state's digital strategy is historically rooted in Cold War-era concerns, including military-industrial competition, national identity preservation, and control over information flows. In recent years, Russia's digital policies have intensified in response to domestic economic stagnation, political crises, and social movements that challenge the legitimacy of the regime. This study employs a mixed-methods approach combining the analysis of legal documents, policy papers, official statements, international indices, and datasets on internet censorship, online prosecutions, and digital surveillance. It examines how Russia's digital sovereignty policies – including the Sovereign Internet Law, Yarovaya amendments, VPN restrictions, and mandatory data localization – impact freedom of speech, privacy, and access to information. The research demonstrates that while these measures are framed as necessary for national security, they enable broad censorship, state surveillance, and the suppression of civil liberties. Furthermore, Russia's model reflects a form of "digital authoritarianism" which relies on both legal frameworks and technical measures to control the internet, regulate content, and influence public opinion. The findings underscore that Russia's prioritization of regime stability over citizens' rights has significant implications for freedom of expression, human rights, and global internet governance, highlighting a growing tension between national security imperatives and digital freedoms.

KEYWORDS

digital non-alignment, censorship, Russia, digital sovereignty, information security, cybersecurity, content security, political stagnation, digital regulations.

e-ISSN **3041-2498**

Публічне управління і політика

https://www.eu-scientists.com/index.php/pmap

Побудова «суверенного інтернету»: цифрова політика Росії як інструмент цензури та суспільного контролю

Суде Гювенч [1]*

[1] *Стамбульський університет (Туреччина). Незалежна дослідниця, випускниця кафедри політичних наук та міжнародних відносин.*

*** *Автор-кореспондент,*** e-mail: guvenccsude@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3041-2498/2025.12.13

Отримана: 10.10.2025 р.
Прийнята: 14.12.2025 р.
Опублікована: 21.12.2025 р.

АНОТАЦІЯ

Росія дедалі більше зосереджується на розробці комплексних цифрових політик, спрямованих на встановлення «цифрового суверенітету», що передбачає зменшення залежності від іноземних технологій, інтернет-інфраструктури та міжнародних платформ. Ці політики інтегрують управління інтернетом, регулювання медіа, кібербезпеку та моніторинг контенту в межах загальної концепції «інформаційної безпеки». Цифрова стратегія держави має історичне коріння у періоді Холодної війни, включаючи військово-промислове суперництво, збереження національної ідентичності та контроль над інформаційними потоками. У останні роки цифрова політика Росії посилилася у відповідь на економічну стагнацію, політичні кризи та суспільні рухи, які ставлять під сумнів легітимність режиму. Дослідження використовує змішаний методологічний підхід, що поєднує аналіз правових документів, політичних програм, офіційних заяв, міжнародних індексів та наборів даних щодо цензури в інтернеті, онлайн-переслідувань та цифрового спостереження. Воно досліджує, як політика цифрового суверенітету Росії – включно з Законом про суверенний інтернет, поправками Ярової, обмеженнями VPN та обов'язковим зберіганням даних у країні – впливає на свободу слова, приватність та доступ до інформації. Дослідження показує, що хоча ці заходи подаються як необхідні для національної безпеки, вони фактично забезпечують масштабну цензуру, державне спостереження та обмеження громадянських свобод. Крім того, модель Росії відображає форму «цифрового авторитаризму», що покладається як на правові механізми, так і на технічні засоби для контролю інтернету, регулювання контенту та впливу на громадську думку. Результати підкреслюють, що пріоритетність стабільності режиму над правами громадян має значні наслідки для свободи слова, прав людини та глобального управління інтернетом, висвітлюючи зростаючу напругу між національною безпекою та цифровими свободами.

КЛЮЧОВІ СЛОВА

цифрове неприєднання, цензура, Росія, цифровий суверенітет, інформаційна безпека, кібербезпека, безпека контенту, політична стагнація, цифрові регуляції.

1. Introduction

New channels and communication methods have significantly improved global networks of information. Non-state actors have gained greater international legal standing thanks to global digitization. The so-called Big Tech corporations are becoming an equal part of both domestic and international government affairs and should no longer be ignored as a national security concern. Security services are interested in the data they collect and the modern technology they utilize. However, their capacity to spread diverse information messages, whether directly or indirectly, to a vast audience is increasingly emerging as a significant political element [4].

By prioritizing regime security over all other considerations and equating "sovereignty" with it, the Kremlin restricts the country's technological advancement, thereby undermining its technological sovereignty [7]. The early stages of Russian Internet policymaking were characterized by laws that bore a resemblance to the state bureaucratic control procedures of the Soviet Union, at the expense of both the industry's uncontrolled expansion and the benefits of executive policymaking. The Internet in Russia is subject to legislation concerning media regulation and business regulation, as it is in Western industrialized countries. As in many other countries, the private sector in Russia creates, owns, and maintains the physical infrastructure of the internet. Businesses that provide services such as blogging platforms, social networking sites (SNSs), Internet service providers (ISPs), and internet firms more effectively hold private regulation over online conduct [12]. There may be legal conflicts resulting from this private rule-making. Information and communications technology (ICT) corporations could be subject to restrictions, influence, and even coercion from governments in the absence of established laws and regulations. Beginning in the early 1990s, the Russian government expressed concern regarding two other aspects of Internet use: national identity (i.e., safeguarding any communication medium from unnecessary foreign influence) and security of new technology, which was rooted in the rivalry between the military and industrial complex during the Cold War [1]. Russia is facing a crisis of legitimacy under Vladimir Putin due to economic stagnation and a lack of political change. The high oil prices in the early 2000s boosted the economy and elevated Putin's popularity. However, real incomes have been decreasing for eight years, and economic growth remains stagnant. The regime is now seeking more control over the internet to prevent the spread of information that could challenge its power. Internet regulations are focused on "content security" and politically provocative content [7].

Three methods are identified by Ognyanova as the means by which the Russian government controls the media: state control over mainstream (particularly broadcast) media, censorship and the chilling effects it causes, and the selective application of unrelated laws (such as building codes, tax laws, criminal laws, and intellectual property laws) to impose pressure on media organizations and on individual journalists, bloggers, and activists. According to Ognyanova, this represents a continuation of the strategies employed by the Russian and Soviet governments in the past to maintain control over traditional print and broadcast media [17]. The legal issues gave rise to a complex collection of regulations in the 1990s that only partially addressed the Internet, which was still a relatively new phenomenon at the time [1].

The information revolution, fueled by the significant increase in domestic internet access, was gradually viewed by Vladimir Putin as one of the most pervasive aspects of U.S. expansionism in the post-Soviet sphere in the 2000s, as Russia struggled to regain its full sovereignty and the "permeability" of its neighboring countries. "Russian authorities' approach to the internet rests on two pillars: control and increasing isolation from the World Wide Web", said Hugh Williamson, Europe and Central Asia Human Rights Watch director. "The government has built up an entire arsenal of tools to reign over information, internet users, and communications networks". This was especially true in Russia. However, for a long time, authorities have only moderately followed RuNet's development, supporting its economic benefits while allowing certain online places for opposition activities. Russia is moving to establish an online "kill switch" that will enable it to cut the RuNet off from the international network "in case of crisis". However, other than making oblique references to the internet being cut off from the outside world, Russia has not specified what such a crisis might involve.

This study has two major hypotheses:

1. Although the Russian government's efforts to maintain national security and digital sovereignty have been successful in reducing the impact of claimed outside threats, it has restricted the liberties of its residents.

2. Due to these measures, there is now more censorship, monitoring, and control over digital communications, which restricts information access, invades privacy, and hinders free speech.

To address these hypotheses, I will attempt to answer my research question: How do Russia's digital policies, aimed at ensuring digital sovereignty, impact the freedom of speech and other civil liberties of its citizens?

2. Problem Statement

Despite rapid internet expansion and digitalization, Russia's government increasingly prioritizes national security and digital sovereignty over citizens' freedoms. A series of laws and regulations, including the Sovereign Internet Law, VPN restrictions, and mandatory data localization, have enabled extensive state surveillance, censorship, and control of online content. While intended to protect national interests, these measures limit freedom of speech, privacy, and access to information. The problem addressed in this study is the tension between Russia's pursuit of digital sovereignty and the protection of civil liberties, and how the state's digital policies affect the rights of internet users in practice.

3. Methods and Materials

The paper employs a mixed-methods approach to examine the overall impact of Russian digital policy, which aims to ensure digital sovereignty, on freedom of speech and other civil liberties. This study will examine selected legal documents, government reports, and policy papers, as well as outputs from international human rights organizations, to reveal the official position of Russia and its real objectives in terms of digital policies, aiming to understand their stated effects. The analysis will be based on data from international indices and reports on restrictions on internet freedom and human rights in Russia. Other sources include research from organizations such as Freedom House, Amnesty International and the United Nations Human Rights Council. I will extract and analyze this data to provide a quantitative framework for the study. Qualitative data will be gathered from policy documents and official statements, while quantitative data will include metrics on internet usage, censorship incidents, and cases of state prosecution for online activities.

4. Results and Discussion

The first official internet limitations were put in place in 2002–2003 with the intention of combating "extremism" [16]. The Roskominform Statute, the Law on Databases, the Law on Communications, the Law on Information, and the Law on Information Exchange comprise the majority of these earlier statutes. The new communication law, which governs ownership relationships, radio frequency band distribution, and communications industry licensing, was signed into law by Russian President Vladimir Putin in July 2003. As a result, bureaucratic processes became more transparent. The law has not banned IP telephony; other operators are still free to establish their own long-distance networks, even though it confirms Rostelecom's monopoly on long-distance voice connections, which is to be reconsidered in 2005.

This legislation showed the Russian government's growing interest in "informatization" policymaking, allowing it to move beyond simple regulation. Specifically, Roskominform was legally defined as a hybrid executive–legislative body that could implement broad policies and was sufficiently close to the president's office to have access to resources and cabinet power brokers. This legislation shows that the government was making progress toward creating Internet policy mechanisms, though slowly and maybe in the wrong direction. The Federal Security Service (FSB) was given the authority "to monitor all private communications" of citizens, including electronic communications, when Russia passed the "Law on Operational Investigations" in 1995.

Additionally, the first "System for Operative Investigative Activities" (SORM) infrastructure was established and later expanded (SORM-2) to enable Internet traffic monitoring. In the era of IT, SORM has frequently mentioned as the worst kind of interference from the government [1]. This legislation empowers the government to ban certain materials, collect user data, and hold content intermediaries accountable.

The Russian government uses the SORM program to monitor citizens' phone and internet conversations [2]. Internet service providers were required by the Federal Security Service (FSB) to install equipment, allowing the agency to access their clients' emails and Internet activity. In 2012, social networking sites were also subject to SORM, which concerned Russian authorities due to their involvement in many "color revolutions" and the 2011 Arab Spring. Levenchuk stated, "Introducing SORM is equivalent to having to surrender copies of the keys to your flat or car or garage to the nearest police station so that the police can visit your home or break into your car or garage whenever they like, supposedly to catch potential criminals" [1].

The government's ISP licensing process was supervised by FSB, which also forced those providers that disobeyed to go offline. Under its versions SORM-2 and SORM-3, SORM, which the Soviet KGB first created for phone call surveillance, has evolved to monitor internet communications, including emails and web browsing. By 2015, all telecommunications were covered by SORM-3. ISPs and telecom providers in Russia are required by law to install SORM equipment, which grants the FSB access to all online data without the knowledge or consent of the companies. By delivering two copies of the same data to the government and the intended recipient, SORM doubles the data flow. More state agencies, including as Roskomnadzor, the Federal Drug Control Service, the Prosecutor General's Office, and Rospotrebnadzor, have been granted access to SORM since Putin's 2012 reelection to the presidency, under the reasons of public safety, counterterrorism, or anti-extremism. Barber-Slavia in Volgograd, for instance, had its capital assets blocked, and its services cut when the ISP threatened to sue the FSB for illegally obtaining its customers' passwords without a warrant. The FSB justified its aggressive action by pointing to "licensing errors" [1].

Russia regularly presented resolutions to the UN General Assembly on the development of information and telecommunications for international security. In 1999, it recommended guidelines for international information security. In 2000, President Putin signed the "Information Security Doctrine of the Russian Federation" in response to media coverage of the Kursk submarine disaster. This Security Council-developed theory recognized the dangers that information flows posed to national security while ostensibly endorsing freedom of expression and the media. By the early 2010s, Russia has established a distinctive and experimental method of information manipulation, especially following the 2011–2012 White Ribbon Protest Movement and Vladimir Putin's reelection to the presidency. Russia's model uses a combination of less overt, more legally feasible, and often non-technical means to control online content, shape narratives, and influence public opinion, in contrast to China's "Great Firewall" which primarily relies on systemic technical censorship [10].

Allegations of manipulation of elections favoring Putin's party, United Russia, occurred shortly after the December 2011 parliamentary elections, causing great unrest among the Russian population. Tens of thousands protested at Moscow's Bolotnaya Square on December 10, 2011. Within two weeks, the number had grown to 100,000, making these the largest antigovernment protests since the fall of the Soviet Union. Social media sites like Twitter, LiveJournal, Facebook, and VKontakte played a crucial role in organizing these demonstrations, raising funds, and exposing electoral fraud. Videos created by users showing electoral infractions, such as ballot stuffing and carousel voting, were extensively circulated on the internet. Journalist Konstantin von Eggert from Russia observed that online politics were now strongly influencing offline politics for the first time. Vladimir Putin has tightened control over the internet since December 2011 by enacting several laws rapidly. These laws, which were frequently drafted incoherently, were intended to limit internet freedom and have been linked to building Russia's version of China's "Great Firewall". The Moscow Times brought attention to the government's practice of enacting internet restriction laws quickly and without seeking approval from the IT industry or web community.

Less than six months after the protests of late 2011 and early 2012, Federal Law No. 89417-6, also known as the "Blacklist Bill", was signed into law on July 28, 2012. It was formally titled "On the Protection of Children from Information Harmful to Their Health and Development" but it is more popularly known as the "Blacklist Bill" [6]. The register initially included narcotics and child pornography, but expanded to include rioting, extremist content, and public demonstrations in 2014. Since 2015, all internet service providers have been required to ensure the protection of Russian individuals' personal data on Russian servers. Yarovaya's Law, named after its co-author and United Russia party member in the State Duma, Irina Yarovaya, came into force in 2016. Since then, telecommunications firms have been mandated to retain metadata for three years within Russian territory, in addition to the content of text messages, phone conversations, photos, and videos for six

months [7]. The primary targets of authorized monitoring, persecution, and censorship have been civil society organizations and independent media outlets. In July 2017, the Russian government began censoring access to content via virtual private networks, or VPNs. A broad power to prohibit social media sites and other online information sources whose activities are considered "undesirable" or "extremist" is also granted to the Russian authorities under the law. In January 2018, regulations were implemented that made it impossible for users of social media and messaging apps to stay anonymous. Due to the resistance of private companies, these have been challenging to implement so far [14].

Roskomnadzor, a government regulatory organization similar to the U.S. Federal Communications Commission, is required by law to create a blacklist. In the Russian Federation, the Federal Service for Supervision of Communications, Information Technology, and Mass Media, commonly referred to as Roskomnadzor, is a component of the Ministry of Communications and Mass Media that regulates all media, including the internet. A court order is not necessary for Roskomnadzor to block certain types of content, such as calls for unapproved public actions (such as protests), so-called extremist content, materials that violate copyright, information about juvenile victims of crime, child abuse imagery, drug propaganda, and suicide information. In contrast, independent agencies like the UK's Ofcom and the U.S. Federal Communications Commission have no power of prior restraint and only have the authority to assess fines [13]. The websites may be blocked if the offensive content was taken removed within 72 hours.

The legislation also gives Roskomnadzor the authority to ban websites that encourage "mass riots" or "participation in unsanctioned events" as well as to filter specific URLs, domain names, and IP addresses. The Blacklist Bill's passage sparked debate over government overreach and the potential for disproportionate censorship due to the bill's unclear language and oversight deficiencies. Many Russian websites went down in protest on July 10, 2012, while the measure passed the State Duma swiftly. There have been numerous applications of the Blacklist Bill. More than 180 websites were blocked in the first two weeks following the bill's passage; just four months later, in February 2013, the total number of websites prohibited by the Blacklist Bill had risen to 4,000. Six websites were blocked in March 2014, including those of dissident Alexei Navalny, people planning protests against the Russian occupation of Crimea, and pages belonging to Ukrainian rights organizations on Russia's biggest social media platform.

According to research by the independent watchdog organization Freedom House, between January 2012 and February 2013, there was a roughly 60% rise in the number of websites prohibited for hosting content that the Ministry of Justice considered "extremist". More power was granted to Roskomnadzor on February 1, 2014. The "Lugovoi Law" so named for the State Duma member who proposed it and was also charged with killing a Kremlin opponent in 2006, provided the communications regulator the authority to prohibit websites that it considered extreme or a threat to public order without a court's approval.

Following the parliamentary elections in December 2011, the Russian authorities started to attack prominent independent news websites. In an attempt to stop unauthorized protests, the Prosecutor General sent a list to internet service providers (ISPs) on March 13, 2014, instructing them to cease hosting content from opposition leaders and organizations, such as the critical daily Grani. Two antiterrorism laws substantially reduced internet freedom in April 2014. The first law allowed authorities to store communication data with uncertain standards. The second law restricted anonymous online money transfers, impacting WebMoney and PayPal. The "Bloggers Law" of May 2014 required bloggers with over 3,000 daily views to register with the government and abide by fact-checking rules. The "Law against Retweets" of June 2014 imposed up to five years in prison for spreading extremist content, formalizing the government's anti-propaganda policy.

On July 4, 2014, a significant data retention rule was implemented, requiring internet giants such as Google, Twitter, and Facebook to store Russian user data on local servers for a minimum of six months. If not complied with by September 2016, the account would be blocked. This regulation aimed to keep Russian data within national borders and was driven by the desire for digital sovereignty, as well as concerns about foreign spying. Similar to the NSA's PRISM program, the Russian government can monitor internet traffic in great detail thanks to the SORM surveillance program, which raises serious privacy issues [6].

The regulator may issue warnings to an outlet's editorial board regarding "abuse of freedom of mass media" under Article 4 of the law "On Mass Media". This category includes offenses like using abusive language, delivering information about illegal drugs, encouraging extremism or terrorism, and using cruelty or propaganda [17]. Once more, censorship resulting from the particular meaning of these

terms goes much beyond what would be implied by a literal interpretation of the law. The media have been warned, for instance, not to publish articles about calls for government reform and increased local governance, or about international news stories concerning the right to free speech, such as the January 2015 attack on the Charlie Hebdo offices in Paris [5]. The Russian broadcast media and political elite collaborate to portray online material as "unreliable, biased, and dangerous" and the internet as a dangerous place [11; 17].

According to Ognyanova (2015), the mayor of Moscow stated that the internet is filled with propaganda about drugs, violence, human trafficking, and child prostitution [17]. The mayor further claimed that unconcealed terrorists are gradually settling the Internet, turning it into a real underground military infrastructure rather than just their own mailbox. The plan appears to be working. As evidenced by the report "Benchmarking Public Dissent: Russia's Appetite for Internet Control" 49% of Russians overall think that content on the internet should be censored, 42% think that foreign governments are using the internet against Russia and its interests, and 24% think that the internet threatens political stability [15]. The kind of propaganda mentioned above enables the Kremlin to portray its limitations on the free exchange of information as a response to the people's desires.

A study on how Russian ICT companies protect the digital rights of their clients was carried out in 2013 by the now-defunct Centre for the Study of Media and Society at the New Economic School in Moscow. The conclusion that was reached was that the companies attempted to avoid discussing human rights; they prefer the term "user rights" and typically comply with government requests due to the fear of facing severe sanctions. That was with the threat of prosecution or retaliation from powerful actors, such as oligarchs or FSB agents, which made the company extremely cautious in its content moderation [19]. Since it failed to comply with data localization regulations and reportedly mishandled user data, LinkedIn became the first foreign social media company to be banned in Russia. The court decided to restrict access to LinkedIn, and Apple and Google were forced to take the LinkedIn app down from their Russian app stores by Roskomnadzor. The actions of American corporations such as Google, Facebook, and Twitter will test their dedication to user privacy and freedom of expression, as Roskomnadzor intends to implement data localization laws more strictly [13].

Increasingly, Russian authorities are using old laws to pursue online speech, frequently linking criticism of the government with "extremism" especially when it comes to contentious issues like the Russian Orthodox Church and military operations in Syria. The number of social media users found guilty of acts of extremism increased from 30 in 2010 to 216 in 2015, according to the SOVA Center. Fifty-five percent of convictions for extremism between 2014 and 2016 involved online criticisms, imposing penalties ranging from fines to jail time. In September 2015, 54 individuals were imprisoned for making extremist statements; by February 2017, that number had increased to 94. A blogger from the Siberian city of Tomsk was given a five-year prison sentence for "extremism" in December 2015 by a court making negative comments about people who arrived in Russia from eastern Ukraine, posted videos on social media and YouTube criticizing Russia's military intervention in Ukraine, and claimed local officials were corrupt.

After publishing a blog post opposing Russia's military involvement in Syria, another blogger from Tyumen, Siberia, was sentenced to two and a half years in prison for the extremist crime of "public justification of terrorism" one year later, in December 2016. The second blogger was found guilty of a crime and imprisoned only for voicing his opinions, but the first blogger's sentence was wildly disproportionate. Authorities have violently suppressed dissent in the three years after Russia occupied Crimea, using the pretext of "combating extremism". Opponents of the occupation, especially Crimean Tatars, have been subjected to intimidation, harassment, and false accusations of criminal activity. Activists, their attorneys, and other people who peacefully oppose Russia's policies have been targeted in this assault. All independent media outlets in Crimea have also been closed by Russian authorities. The anti-LGBT "propaganda" law of 2013, which forbade the publication of material about "nontraditional sexual relations" has been aggressively implemented by Russian authorities. In December 2022, the law prohibiting LGBT+ "propaganda" went into effect, and in 2023, the authorities began releasing administrative regulations for displaying and promoting "nontraditional sexual relations" in films and television shows. In 2023, 33 protocols were issued against Russian online movie and television broadcasters, including Megafon TV, Start, More.tv, Ivi, Beeline TV, TV-3 Russia, and TNT Music.

The freedom of expression of independent nongovernmental organizations has been increasingly limited in Russia. Groups that accept foreign funds are considered evil and discredited under the 2012

"foreign agents" law. The prosecutor's office is also authorized to prohibit foreign or international organizations that are deemed to pose a threat to Russia's security, defense, or constitutional order, pursuant to the 2015 "undesirables" law. Additionally, this rule effectively isolates Russian groups from their foreign allies and collaborators by requiring them to sever any links with the prohibited organizations [9].

The 2017 Russian law 276-FZ restricted VPNs and anonymizers to prevent access to blocked sites and banned search engines from linking to banned content. Millions of IP addresses were blocked in Roskomnadzor's attempt to stop Telegram in 2018, which refused to hand over the keys to its encryption; as a result, huge disruptions in service were experienced, leading to a massive spike in VPN usage, with some providers reporting a 1,000% increase in sales. Roskomnadzor blocked 50 VPNs and fined Google 500,000 rubles for non-compliance. The State Duma imposed fines of up to 700,000 rubles in June 2018 for breaking the prohibition on VPNs and anonymizers. Roskomnadzor threatened to stop nine out of ten VPN providers in June 2019 for failing to connect to its list of prohibited websites; Avast SecureLine withdrew from the Russian market while Kaspersky Secure Connection complied. Yet, many VPNs remain available in Russia [9].

Recent research conducted on November 2022 by the University of Michigan's Censored Planet project and Arizona State University detected 6,000 Roskomnadzor-produced TSPU devices on Russian networks. In contrast to China's Great Firewall, the researchers state that the TSPU is "a model of decentralized deployment, centralized control" because Roskomnadzor may utilize these devices to block websites across various networks unilaterally.

The RuNet Law, passed in 2019, authorizes Roskomnadzor to implement special-purpose DPIs to combat "threats" to the "stability, security, and integrity" of Russia's Internet. Importantly, this legislation establishes a legal foundation for mandating that ISPs incorporate government-supplied devices into their networks. About a year later, Russian users began to discover domains being blocked that were not included in the blocking register, which contradicted our previous knowledge of how censorship was performed [22]. This kind of event was seen in the Twitter throttling incident of 2021, the first known centrally controlled attempt that used throttling instead of outright blocking to put pressure on social media websites. The decentralized control mechanism has been transformed from an ISP-controlled censorship mode to a more centralized one by the Russian government [23].

The Sovereign Internet Law, passed in 2019, requires Russia's ISPs to install Deep Packet Inspection (DPI) systems, also known as "black boxes" to monitor, filter, throttle, and block content. This has considerably enhanced Roskomnadzor's ability to automatically block websites and restrict internet access while minimizing disruptions to RuNet. Before the Duma elections in September 2021, Roskomnadzor actively targeted opposition websites and blocked means for circumventing these prohibitions, including Alexei Navalny-related and mirror sites. Furthermore, in September 2021, Roskomnadzor disabled six VPN providers, and in December 2021, it utilized DPI to restrict the Tor network, which has the second-largest user base in Russia. To gain more control over the internet, the government plans to establish its own Domain Name System (DNS) under Roskomnadzor. These protocols are being adopted by major DNS providers, such as Yandex, Cloudflare, and Google, which makes censorship more difficult. In retaliation, the Russian government has introduced a bill that would prohibit websites from using protocols that mask web page names and require them to be taken down within a business day.

A regulation mandating international tech platforms with more than 500,000 daily users to establish representative offices in Russia was implemented by Russia in the summer of 2021. Additionally, they must register with Roskomnadzor, include feedback forms for Russian users, and filter any content that contravenes Russian laws. Penalties such as limited money transfers, slower traffic, or complete blocking may result from noncompliance. Thirteen foreign companies – Google, Meta, Apple, Twitter, TikTok, and Telegram – had to comply by January 1, 2022. Some companies have already registered with Roskomnadzor, including Apple and Twitter. Foreign corporations have come under criticism, but there has also been a noticeable movement in favor of local tech titans having more power. The main domestic social media network in Russia, VKontakte (VK), also known as "Russia's Facebook" was acquired in December 2021 by businesses linked to Yuri Kovalchuk, a close ally of Vladimir Putin, and the state-run gas giant Gazprom.

Vladimir Kiriyenko, the son of President Putin's first deputy chief of staff, was named VK's new CEO almost immediately following the agreement. The acquisition sets a precedent for the state transitioning from a "control through ownership" approach – that is, pushing oligarchs close to the

Kremlin to acquire control of the digital industry – to direct control over Russian IT companies. As of April 1, 2021, all cellphones sold in Russia must include Russian applications from a government-approved list, such as social media, search, email, payment, and maps. Similarly, desktops and laptops must include the Yandex browser, MyOffice suite, and Kaspersky antivirus. This measure favors Russian enterprises, such as Yandex, VK, and Kaspersky, by guaranteeing that Russian users primarily use services that the government can monitor. The approach aims to disadvantage large companies, such as Google and Facebook, by directing users to state-controlled Russian networks [7].

Following the invasion of Ukraine, Russian authorities increased their efforts to ban access to websites and social media platforms that may include material critical of the authorities or the invasion, as well as international news sites, civil society websites, and Ukrainian news sites. Roskomsvoboda stated in 2022 that 247,000 webpages had been blocked, including 9,000 blocked under military censorship since the start of the full-scale assault. A February 2023 report, produced by the Open Observatory of Network Interference and Roskomsvoboda, discovered that Russian government agencies blocked 494 internet domains in 2022. Between the beginning of the invasion and April 2022, the Russian government blocked social media services, including Facebook and Messenger, Twitter, and Instagram.

In the first wave of blocking, authorities blocked media sites such as the Russia-based student magazine DOXA, the BBC, Voice of America, Deutsche Welle, Bellingcat, Paper, Meduza, Mediazona, Interlocutor, RFE/RL, Echo of the Caucasus, Republic, Taiga.Info, 7x7 Horizontal Russia, and the Village, among others. Authorities also blocked civil society websites, including Amnesty International's Russian-language website, For Human Rights, the election observation organization Voice, and Human Rights Watch [8]. Individuals and journalists who targeted the Russian military were convicted to prison and punished under 2022 adjustments to the Criminal Code and Administrative Code, which prohibit "discrediting" or "knowingly spreading false information about" the military [21].

At least 140 people were condemned to prison for anti-war speeches, rallies, or other activities, up from 22 in 2022. Vladimir Kara-Murza, an opposition and human rights activist, was sentenced to 25 years in prison in April on false accusations of state treason, spread of "fake information" concerning the armed forces, and membership in a "undesirable organization". A court-maintained Vladimir Rumyantsev's three-year sentence for "disseminating knowingly false information about the Russian armed forces" on April 13. Vladimir Rumyantsev used a home radio studio to rebroadcast war-related information from forbidden media sites. Oleg Orlov, a well-known human rights activist, was put on trial for posting an article opposing Russia's invasion of Ukraine [3]. Ilya Yashin, a politician, was sentenced to eight and a half years in prison in December 2022 after releasing a YouTube video detailing crimes committed by the Russian forces in Bucha, a city in Ukraine's Kyiv Oblast. Authorities can impose significant penalties on internet providers and social media businesses that repeatedly violate the "sovereign internet" law by failing to install and operate state-controlled software. In April 2022, a Moscow court fined the Wikimedia Foundation 3 million rubles for failing to remove six Wikipedia pages about the Russian army's operations during the invasion of Ukraine at the request of Roskomnadzor.

In January 2023, a Moscow court fined Twitch 4 million rubles for failing to remove information about Russia's full-scale invasion of Ukraine [8]. Roskomsvoboda, an internet freedom NGO, reported that over 10,000 websites were blocked for supposedly undermining Russia's military forces. Under the "right to be forgotten" law, individuals in the country can request that search engine providers restrict results that contain personal information. Freedom House's 2021 Freedom on the Net report states that the regulation mandates search engines to remove links to websites containing personal information if they are no longer relevant. The statute did not limit the "right to be forgotten" if the sought material was in the public interest or involved public figures, limiting free expression. Social media users were increasingly being prosecuted for the political, religious, or other ideological content of their posts, shares, and "likes" particularly when it came to content about Ukraine. If found guilty, these users may face fines or lengthy prison terms.

5. Conclusions

To conclude, the Russian government has been adopting a threat-oriented view towards the internet, driven by concerns for its national security in the digital sphere. Russia has been facing various security concerns, such as potential cyberattacks, dependency on foreign digital technologies, and the dominance of Western and Chinese digital mobilities in global technology. Big American-owned

companies, such as Google and Facebook, carry a potential risk for the domination of the Russian digital sphere. Vladimir Putin viewed the information revolution, particularly the expansion of domestic internet access, as part of U.S. expansionism in the post-Soviet space, especially in Russia, during the 2000s. This was a time when Russia struggled to regain its full sovereignty and faced external pressure. Initially, officials accepted some online criticism and viewed RuNet's expansion as economically advantageous. In an effort to curb "extremism" the first legal limits on the internet were placed in 2002–2003.

Additionally, the monitoring system SORM–II was further developed to monitor online interactions. However, the Arab Spring of 2011 greatly concerned Russian authorities, as demonstrators had coordinated their actions using digital tools. Concerned that comparable movements could pose a threat to their system, the Kremlin and law enforcement intensified their scrutiny of the political use of digital platforms (Internet Policy Review, 2020). Vladimir Putin has come to seriously consider the internet's foreign policy as the establishment of a new U.S.-led hegemonic framework in the context of intense information campaigns over the events in Ukraine and what he views as the decline of a "morally decadent" West that would use the platform to subvert Russian society and culture. Consequently, Russia expanded several laws and regulations, aiming to strengthen its power over Internet infrastructure, communications' privacy, and online content, such as 2016 "Yarovaya amendments" on forced data retention, 2017 law prohibiting VPNs and Internet anonymizers, and law of identification of messaging application users, 2019 "sovereign internet" law, and 2019 law on previously installed applications [9].

Many in Russia were encouraged by these global events to seek significant political reforms following ten years of Vladimir Putin's administration, which was marked by the state guaranteeing improving living standards for citizens in exchange for political freedoms. Legislators have defended these regulations as necessary for safeguarding state security, the integrity of the Russian internet, and the privacy of its users. These actions, however, actually render broad censorship and surveillance possible, introduce ambiguous content-blocking techniques, and threaten the privacy and security of online interactions. Russia's strict digital regulations, intended to ensure digital sovereignty and internet control, significantly restrict citizens' liberties, particularly the right to free speech.

References

1. Alexander, M. (2004). The Internet and democratization: The development of Russian Internet policy. *Population, 8*(6), 607–627. https://doi.org/10.3200/DEMO.12.4.607-627
2. Allerson, E. (2022). Internet censorship in Russia: The sovereign internet laws and Russia's obligations under the European Convention on Human Rights. *Minnesota Journal of International Law, 31*(1), 233–258. https://minnjil.org/wp-content/uploads/2022/06/Allerson_v31_i1_233_258.pdf
3. Amnesty International. (n.d.). *Russia 2023 report*. https://www.amnesty.org/en/location/europe-and-central-asia/eastern-europe-and-central-asia/russia/report-russia/
4. Bezrukov, A. O., Mamonov, M. V., Suchkov, M. A., & Sushentsov, A. A. (2021). Russia in the digital world: International competition and leadership. *Russia in Global Affairs,* (2), 64–85. http://doi.org/10.31278/1810-6374-2021-19-2-64-85
5. Committee to Protect Journalists. (2015, February 19). *In Russia, media regulator uses warnings to restrict the press*. https://cpj.org/2015/02/in-russia-media-regulator-uses-warnings-to-restric/
6. Duffy, N. (2022). Internet freedom in Vladimir Putin's Russia: The noose tightens. *American Enterprise Institute*. https://www.aei.org/research-products/report/internet-freedom-vladimir-putins-russia-noose-tightens/
7. Epifanova, A., & Dietrich, P. (2022). *Russia's quest for digital sovereignty*. DGAP Analysis, 1. German Council on Foreign Relations. https://doi.org/10.60823/DGAP-22-36557-en
8. Freedom House. (2023). *Russia: Freedom on the Net 2023 country report*. https://freedomhouse.org/country/russia/freedom-net/2023#footnote1_1ax0qsg
9. Human Rights Watch. (2017, July 18). *Online and on all fronts: Russia's assault on freedom of expression*. https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression
10. Kerr, J. (2019). The Russian Model of Digital Control and Its Significance. In N. D. Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order* (pp. 62–74). Air University Press. http://www.jstor.org/stable/resrep19585.14
11. Kratasjuk, E. (2006). Construction of 'reality' in Russian mass media news on television and on the internet. In H. Schmidt, K. Teubener, & J. Konradova (Eds.), *Control + Shift: Public and private usages of the Russian Internet* (pp. 34–50). Norderstedt: BOD-Verlag. https://search.gesis.org/publication/gesis-solis-00377169

12. MacKinnon, R. (2012). *Consent of the networked: The world-wide struggle for Internet freedom*. New York, NY: Basic Books. https://scalar.usc.edu/works/uiuc-macs410-media-information-ethics-/media/PDF_ConsentofNetworked_PrefIntroC1C2C3.pdf
13. Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29–41. https://doi.org/10.17645/mac.v5i1.808
14. Meserole, A. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. Brookings Institution. https://policycommons.net/artifacts/3527460/exporting-digital-authoritarianism/4328250/
15. Nisbet, E. C. (2015, February). *Benchmarking public demand: Russia's appetite for Internet control.* Center for Global Communication Studies / Russian Public Opinion Research Center. https://repository.upenn.edu/handle/20.500.14332/37496
16. Nocetti, J. (2015). Russia's "dictatorship-of-the-law" approach to internet policy. *Internet Policy Review, 4*(4). https://doi.org/10.14763/2015.4.380
17. Ognyanova, K. (2015). In Putin's Russia, Information Has You: Media Control and Internet Censorship in the Russian Federation. In M. Merviö (Ed.), *Management and Participation in the Public Sphere* (pp. 62–79). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-4666-8553-6.ch003
18. Orlova, A. V. (2020). "Digital sovereignty" anonymity, and freedom of expression: Russia's fight to re-shape internet governance. *UC Davis Journal of International Law & Policy, 26*(2), 225–248. https://jilp.law.ucdavis.edu/sites/g/files/dgvnsk15346/files/2024-05/26UCDavisJIntlLPoly225.pdf
19. Petrova, M., Fossato, F., Indina, T., Dokuka, S., & Asmolov, G. (2013). *Ranking digital rights report: Russia* (Unpublished report). Moscow: Center for the Study of New Media and Society.
20. Pollicino, O., & Soldatov, O. (2018). Striking the balance between human rights online and state security concerns: The Russian way in a comparative context. *German Law Journal, 19*(1), 85–112. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203724
21. U.S. Department of State. (2024). *2023 Country Reports on Human Rights Practices: Russia* (Bureau of Democracy, Human Rights, and Labor). https://www.ecoi.net/de/dokument/2108736.html
22. Xue, D., Mixon-Baca, B., Valdik S.S., Ablove, A., Kujath, B., Crandall, J. R., & Ensafi, R. (2022). *TSPU: Russia's decentralized censorship system*. In *IMC '22: Proceedings of the 22nd ACM Internet Measurement Conference* (pp. 179–194). https://doi.org/10.1145/3517745.3561461
23. Xue, D., Ramesh, R., Valdik S.S., Evdokimov, L., Viktorov, A., Jain, A., Wustrow, E., Basso, S., & Ensafi, R. (2021). Throttling Twitter: An emerging censorship technique in Russia. In *IMC '21: Proceedings of the 21st ACM Internet Measurement Conference* (pp. 435–443). https://doi.org/10.1145/3487552.3487858