DOMAIN NAME SUSPENSION IN RUSSIA – INTERNET-INFRASTRUCTURE-BASED TOOL TO CONTROL FREE EXPRESSION

*Liudmila Sivetc**

1 Introduction

Freedom of expression is essential for a modern democratic society[1] and citizen participation in it.[2] This freedom underpins the public sphere by enabling citizens to voice their opinions.[3] Freedom of expression also enables citizens to develop as individuals.[4] Therefore, a nation-state does not possess "the affirmative right to make information and ideas available to whomever it chooses."[5] Article 10 of the European Convention on Human Rights guarantees everyone the

---

* This article presents an updated and developed part of my doctoral dissertation "*State Control of Online Freedom of Expression by Internet Infrastructure in Russia: Implications for online freedom of expression from the perspective of the new-school speech regulation approach*. TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS SARJA – SER. B OSA – TOM. XXXX | HUMANIORA | TURKU 2021.

1 E. Barendt, *Freedom of Speech*. 2nd ed. New York: Oxford University Press, 2005.

2 J. Barata & M. Bassini, "Freedom of Expression in the Internet: Main Trends of the Case Law of the European Court of Human Rights." In O. Pollicino & G. Romeo (eds.) *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe*, p. 79–101. Routledge, 2016.

3 J. Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy. Studies in Contemporary German Social Thought*. Cambridge, Mass.: MIT Press, 1996.

4 F. Schauer, *Free Speech: A Philosophical Enquiry*, Cambridge University Press, Cambridge, 1982.

5 M. Price, "Public Diplomacy and the Transformation of International Broadcasting" *Cardozo Arts & Entertainment Law Journal*, 2003, 21(1), p. 57.

freedom to receive and impart information and ideas. According to the European Court of Human Rights, it applies not only to the content of information but also to the means of its dissemination, for any restriction imposed on the latter necessarily interferes with that freedom.[6] As the court stated, the Internet has become "one of the principal means [or tools] by which individuals exercise their right to freedom of expression and information."[7]

However, since 2012, Russian State has tightened control over the Russian Internet, "which for a long time provided a space for alternative media and free speech."[8] According to some researchers, Russia set as a goal the achievement of total control over any online activity.[9] As regards online free expression, Russia introduced extensive legislation to intensify state control, a decision that has been criticized as "legal haste,"[10] "blitzkrieg,"[11] and "the occupation of Runet."[12] This process has limited political freedom in the country[13] and led to "a steady decline of freedom of expression in Russia over the past two decades."[14]

---

[6] ECtHR, *Vladimir Kharitonov v. Russia* [2020] App. No. 10795/14, Judgment of 23 June 2020, para *33.*

[7] *Ibid*.

[8] M. Wijermars & K. Lehtisaari (eds). *Freedom of expression in Russia's new mediasphere*. London: Routledge., 2020, p. 1.

[9] G. Asmolov, "Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation" *Center for Global Communication Studies, Internet Policy Observation.* 2015 (2), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1013&context=internetpolicyobservatory; N. Duffy, "Internet Freedom in Vladimir Putin's Russia: The Noose Tightens" American Enterprise Institute, 2015, p. 1, https://www.aei.org/wp-content/uploads/2015/01/Internet-freedom-in-Putins-Russia.pdf.

[10] J. Nocetti, "Russia's "Dictatorship-of-the-Law" Approach in Internet Policy" *Internet Policy Review* November 2015, 4(4), p. 2.

[11] A. Eremenko, "Russia to Make Internet Providers Censor Content – Report" *The Moscow Times*, 2 December 2014, https://themoscowtimes.com/articles/russia-to-make-internet-providers-censor-content-report-41922.

[12] M. Lonkila, L. Shpakovskaya, & Ph. Torchinsky, "The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet," In: M. Wijermars and K. Lehtisaari (eds). *Freedom of expression in Russia's new mediasphere*. London: Routledge, 2020, p. 23.

[13] *Ibid*, p. 18.

[14] M. Wijermars & K. Lehtisaari, *supra 8,* p. 2.

Researchers connect "the most visible element of this decline" to the state control over the media.[15] This article focuses on the less visible element: the state control of the Russian Internet infrastructure, "which researchers less frequently identified as an issue correlated with endangering free expression."[16]

The infrastructural dimension of exercising this right has been highlighted in *Balkin*'s new-school speech regulation approach. Balkin refers to the Internet infrastructure rather than to the Internet as the means of exercising the right to online freedom of expression. Under the new-school speech regulation, he understands controlling online free expression indirectly: regulating the Internet infrastructure rather than the speakers. Nevertheless, this indirect regulation by infrastructure has direct effects on online speech because it can be expressed and accessed only through the Internet infrastructure. By co-opting/cooperating with Internet infrastructure owners, the government implements new-school regulation by inserting filters to sort out and block unwanted content. These new-school tools are non-transparent and work in the background.[17]

Filtering and blocking of websites in Russia relies on the two Blacklist Laws (Law no. 139-FZ of 2012 and no. 398-FZ of 2013).[18] The Blacklist Law of 2012 introduced the blocking of websites containing images of child sexual abuse, drug propaganda, or information on committing suicide. The Blacklist Law of 2013 set up the blocking of websites containing calls for extremist activity, public rallies, and unsanctioned public actions. These websites are included on a black-

---

[15] M. Wijermars & K. Lehtisaari, *supra 8*, p. 3.

[16] L. Sivetc, "Controlling free expression "by infrastructure" in the Russian Internet: The consequences of RuNet sovereignization" *First Monday*, 2021, 26(5), https://doi.org/10.5210/fm.v26i5.11698.

[17] J. Balkin, "Free Speech is a Triangle" *Columbia Law Rev*iew, 2018, 118(7), p. 2011–2055.

[18] How the website blocking practice correlates with the new-school approach see L. Sivetc. The blacklisting mechanism: New-school regulation of online expression and its technological challenges. *In Freedom of Expression in Russia's New Mediashere*, edited by M. Wijermars and K. Lehtisaari, p. 39–56. BASEES/Routledge series on Russian and East European studies, London and New York: Routledge 2019.

list operated by *Roskomnadzor*[19] – a special executive government agency – which requires Internet service providers to block access to blacklisted websites.[20] Since 2013, new types of harmful content have been covered by the blacklist legislation, ranging from information on the illegal sale of alcohol to the "disrespect" of Russian officials. In 2017, the effectiveness of website blocking was enhanced by the Blacklisting, Anonymization, and Online Browsing Act (Law no. 276-FZ of 2017) requiring, first, that the providers of anonymizing services prevent their users from accessing blacklisted websites and, second, that providers of search engines stop showing links to blacklisted websites.[21]

The Blacklist Laws have attracted criticism mainly because the vague definition of illegal speech might lead to arbitrary censorship by officials.[22] Consequently, in 2015, for the first time, *Freedom House* marked Runet as "not free".[23] This status has remained unchanged since then. In June 2020, the European Court of Human Rights decided that the blacklist legislation regulates free expression in an excessive and abusive manner, as it allows Russian authorities, without

---

[19] The full name of the agency is the Federal Service for Supervision of Communications, Information Technology and Mass Media.

[20] Law no. 139-FZ of 28 July of 2012 "On Amending Federal Law On the Protection of Children from Information Damaging Their Health and Development and on Amending Other Acts of the Russian Federation."

[21] Law no. 276-FZ of 19 July 2017, introducing Article 10.8 in Law "On Information, Information Technologies, and Protecti on of Information." Law no. 276-FZ came into force on 30 July 2017.

[22] See, for instance, R. Favret, "Comment: Back to the Bad Old Days: President Putin's Hold on Free Speech in the Russian Federation" *Richmond Journal of Global Law & Bussiness* 2013(12), p. 299–306; A. Tselikov, "The Tightening Web of Russian Internet Regulation" Harvard University, Berkman Center for Internet & Society 2014, https://cyber.harvard.edu/publications/2014/runet_regulation; P. Johnson, "Homosexual Propaganda' Laws in the Russian Federation: Are They in Violation of the European Convention on Human Rights*?" Russian Law Journal,* 2015, 3 (1), p. 37–61; Nocetti, *supra 10*; E. Sherstoboeva & V. Pavlenko, "Freedom of Expression and Regulation of Extremism in Russia in the Context of the Council of Europe Standards" in *Internet Science. INSCI 2018*, edited by S. Bodrunova, Lecture Notes in Computer Science, vol. 11193, Cham: Springer, 2018, p. 101–115.

[23] Freedom House, "Freedom on the Net 2015. Russia" https://freedomhouse.org/report/freedom-net/2015/russia.

court oversight, to block an entire website rather than only blacklisted content.[24] Moreover, website owners are not able to prevent the blocking by removing or modifying the banned content nor were they provided with procedural safeguards against interference in their freedom of expression.[25] Furthermore, the legislation leaves without remedy the owners of websites that are blocked accidentally due to sharing the same IP address as the blacklisted website.[26]

However, little research has been conducted on non-legal means of filtering and blocking online content that Russia has been using. Previous studies[27] have described and analyzed *the Netoscope* project through which Roskomadzor gained the power to degrade unwanted websites in the lists of search results provided by *Yandex*, the most popular in Russia search engine provider and one of Netoscope partners. This article explains the functioning of another project – *the Authorized Organization Project* – in which Roskomnadzor participates to control the dissemination of online content. This project empowers Roskomnadzor to initiate the suspension of unwanted domain names, which leads to the disconnection of a domain name from the corresponding address on the host server. In contrast to website blocking, domain name suspension cannot be circumvented by using VPNs and consequently presents a more serious threat to online free expression. However, the various reports and indicators of online freedom in Russia have overlooked this practice. For instance, *the Society for the Protection of the Internet,* a Russian Internet freedom watchdog, regularly conducts the "Index of Freedom of the Runet" metrics system, by gathering news on legal, technological, and political events affecting the level of freedom on the Russian Internet. In June 2019, the FSB, a

---

[24] ECtHR, *supra 6*, paras. 38, 43; ECtHR, *OOO Flavus and Others v. Russia* [2020] App. Nos. 12468/15, 23489/15, and 19074/16, Judgment of 23 June 2020, para 38.

[25] ECtHR, *OOO Flavus and Others v. Russia* [2020], para 32, 40.

[26] *Ibid*., paras. 42, 44.

[27] L. Sivetc. State regulation of online speech in Russia: the role of internet infrastructure owners. *International Journal of Law and Information Technology* 27-1/2019, p. 28–44; L. Sivetc and M. Wijermars. The vulnerabilities of trusted notifier-models in Russia: The case of Netoscope. *Media & Communication,* 2021, Volume 9, No 4 (2021): Media Control Revisited: Challenges, Bottom-Up Resistance and Agency in the Digital Age, https://doi.org/10.17645/mac.v9i4.4237.

Russian security service, joined the Authorized Organization Project through *National Computer Incident Response & Coordination Center (NCRCC),* empowering the FSB to trigger domain name suspension and thereby censor online freedom of expression. Although this event was covered in the Russian press,[28] the Society for the Protection of the Internet did not include it when calculating its Index for June 2019. Consequently, the censorship practice by domain name suspension appears to be overlooked by this Internet freedom watchdog as a factor affecting Internet freedom. In my view, this omission may make the researcher question whether the "Index of Freedom of the Runet" adequately assesses the level of Internet freedom. The same criticism relates to international indexes, for instance, those prepared by Freedom House.[29]

Thus, this article aims at filling the gap in understanding of how Russia can control online free expression through the Runet infrastructure and do it by relying on cooperation agreements with owners of this infrastructure rather than by clear legal frameworks. The rest of the article proceeds as follows. The next part discusses the control-through-infrastructure approach and explains new perspectives on controlling freedom of expression that this approach emphasizes. Then, Part 3 explains the governance of the critical point of the Runet infrastructure – Runet Domain Name System. Part 4 unfolds practices of domain name suspension implemented through the Authorized Organization Project and analyzes the implications of these practices for online free expression.

---

[28] See, for instance, D. Sherstoperov & D. Moiseev, "FSB Will Receive Powers to Undelegate" ["ФСБ Получит Разделегирующие Полномочия"], *Kommersant.ru*, 6 August 2019, https://www.kommersant.ru/doc/4053073; INTERFAX.RU, "The Structure of the FSB Received the Right to Demand Website Blocking" ["Структура ФСБ Получила Право Требовать Блокировок Сайтов"], 8 August 2019, https://www.interfax.ru/russia/671716.

[29] Freedom House, "Freedom on the Net 2020. Russia." https://freedomhouse.org/country/russia/freedom-net/2020.

2 Internet control through infrastructure

Studies on free speech on the Russian Internet usually focus mostly on content regulation and much less on the regulation of the Russian Internet infrastructure.[30] This may be explained by the lack of understanding of how online speech regulation is intertwined with Internet infrastructure regulation.

It is often assumed that the Internet, due to its open architecture design, resists "any form of centralized control."[31] The open design means the absence of a central point connecting information flows inside the Internet infrastructure.[32] Therefore, the decentralized design shields online speech from regulation.[33] Following *Gilmore*, the Internet "interprets censorship as damage and routes around it."[34] In contrast, the cyber-paternalists[35] highlight that, although the open ar-

---

[30] I. Stadnik, "Control by Infrastructure: Political Ambitions Meet Technical Implementations in RuNet." *First Monday*, 26 (5), https://doi.org/10.5210/fm.v26i5.11693.

[31] P. Vargas-Leon, "Tracking Internet Shoutdowns Practices: Democracies and Hybrid Regimes" In *The Turn to Infrastructure in Internet Governance,* F. Musiani, D. Cogburn, L. DeNardis & N. Levinson (eds.), Basingstoke: Palgrave Macmillan, 2016, p. 167.

[32] M. Mueller, *Ruling the Root: Internet Governance and the Tamimg of Cyberspace*. Cambridge, MA: MIT Press, 2004.

[33] See, for instance, D. Post, "Governing Cyberspace" *Wayne Law Review* 1996, 43(1), p. 155–171; J. Barlow, "Censorship 2000" *OnTheInternet*, October 2000) https://www.isoc.org/oti/articles/1000/barlow.html; D. Johnson & D. Post, "Law and Borders – The Rise of Law in Cyberspace" *Stanford Law Review*, 1996, 48(5), p. 1367–1402; H. Henry & Jr. Perrit, "Jurisdiction in Cyberspace" *Villanova Law Review*, 1996, 41(1), p. 2–128.

[34] Ph, Elmer-DeWitt & D. Jackson, "First nation in Cyberspace" *TIME*, 6 December 1993, p. 62.

[35] See, for instance, J. Boyle, "Faucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors" *University of Cincinnati Law Review,* 1997, 66, p. 177–205; L. Lessig, *Code and Other Laws of Cyberspace* New York: Basic Books, 1999; J. Goldsmith & T. Wu, *Who Controls the Internet: Illusions of a Borderless World*, UK: Oxford University Press, 2006; A. Murray, *Information Technology Law, The Law and Society* (2nd ed.) UK: Oxford University Press, 2013; M. Geist, "Cyberlaw 2.0" *Boston College Law Review*, 2003, 44(2), p. 323–358; J. Hughes, "The Internet and the Persistence of Law" Boston College Law Review, 2003, 44(2), p. 359–396; M. Birnhack & N. Elkin-Koren, "The Invisible

chitecture has posed a new challenge for regulators, it has not protected them from attempting to control the Internet. Achieving this goal means having control not only over a technological architecture, but also over an economic resource,[36] an instrument for setting political agendas,[37] and a basis for enabling the operation of water, electricity, gas, and other critical distribution networks.[38] Last but not least, control over the Internet means controlling a communication medium, through which flow not only Internet traffic data but also information in the form of text, video, and audio messages.[39] Communication occurs through the Internet infrastructure designed to deliver the information file, split into packets, via multiple routes throughout the plethora of networks to the addressee. Therefore, some scholars have referred to the Internet infrastructure as a means of placing governmental control over communications via the Internet: changes in the infrastructure design usually lead to changes in the communication process via this infrastructure.[40]

When cyberspace is coded or architectured to be regulated, the government can leverage these design pre-settings to affect online

---

Handshake: The Reemergence of the State in the Digital Environment" *Virginia Journal of Law & Technology*, 2003, 88(2), p. 2–57; J. Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence" *European Journal of International L*aw, 2002, 11(1), p. 135–148; N. Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory" *California Law Rev*iew, 2000, 88(2), p. 395–498; J. Goldsmith, "Against Cyberanarchy" University of Chicago Law Review, 1998, 65(4), p. 1199–1250; J. Reidenberg, "Governing Networks and Rule-Making in Cyberspace" *Emory Law Journal*, 1996, 45.

[36] S. Braman, "Internet Policy" In M. Consalvo & S. Ess (eds.) *The Handbook of Internet Studies*, Hoboken, HJ: Wiley-Blackwell, 2010, p. 137–167.

[37] G. Lotan & E. Graeff, "The Revolutions were Tweeted: The Information Flows During the 2011 Tunisan and Egyptian Revolutions" *International Journal of Communication*, 2011, 5, p. 1375–1405

[38] R. Radanovsky & A. McDougal, *Critical Infrastructure: Homeland Security and Emergency Preparedness*. Boca Raton FL: CRC Press/Taylor and Francis Group, 2010.

[39] G. Giacomello. *National Governments and Control of the Internet: A Digital Challenge*. London, England: Routledge, 2005.

[40] F. Musiani, D. Cogburn, L. DeNardis, N. Levinson (eds.), *The Turn to Infrastructure in Internet Governance*, Basingstoke: Palgrave Macmillan, 2016; P. Vargas-Leon, *supra 31*.

conduct.[41] For instance, *Reidenberg* acknowledges that governments can seek to "re-engineer" the Internet infrastructure to "facilitate state enforcement of legal and policy decisions" and lays a special focus on co-opting Internet service providers and "the power of technological instruments," such as filters and packet interceptors.[42] Reidenberg refers to these technical, infrastructure-based instruments as "ex ante means to assure that policy decisions are enforced."[43] Balkin also refers to infrastructure-based regulation as ex ante means. In the pre-digital years, governments used post ante regulation tools: court injunctions, fines, civil and criminal charges. Balkin calls this control "old-school speech regulation." Nevertheless, governments could not physically restrict the print speech infrastructure, for instance delivery chains, by installing roadblocks on streets to intercept all delivery trucks, because this would be costly to implement and impossible to conceal.[44] The situation has changed as content and users have migrated to online spaces. This is rooted in the change in speech infrastructure.[45] Online media and digital speech rely on Internet technologies, telecommunications, and broadband companies to deliver information packages to hosting servers and clouds, where Internet users can access the digital content. The functioning of this digital speech infrastructure is enabled by the Internet protocols and standards that govern the Internet.[46] Thus, the Internet infrastructure is used as an infrastructure for digital speech. The infrastructural change has not only enhanced the opportunities for speakers to reach out to their audiences, but also provided governments with new ways to regulate. Regulating speakers by regulating the digital speech infrastructure itself, that is, the Internet infrastructure, has

---

[41] L. Lessig, *Code and Other Laws of Cyberspace* New York: Basic Books, 1999, p. 514.

[42] J. Reidenberg, "States and Internet Enforcement" *University of Ottawa Law & Technology Journal*, 2003–2004, 1, p. 216.

[43] *Ibid.*, p. 218.

[44] J. Balkin, "Old-School/New-school Speech Regulation" *Harvard Law Review*, 2014, 127(8), p. 2297.

[45] *Ibid.*, p. 2305–06.

[46] W. Dutton & M. Peltu, "The Emerging Internet Governance Mosaic: Connecting the Pieces" *Information Polity* 2007;12(1–2), p. 63–81; J. Zittrain, *The Future of the Internet – And How to Stop It* Yale University Press & Penguin UK, 2008.

introduced "new-school" speech regulatory practices. In contrast to the old-school practices, new-school regulation does not aim to control the speakers directly. Rather, the new-school tools control the speakers indirectly by affecting the speech infrastructure. As the speech infrastructure is owned by private Internet companies, governments have to address them in order to leverage their private power over the users of their services. For instance, Reidenberg points out to Internet service providers as owners of "gateway" hubs in the Internet infrastructure located under a state jurisdiction to be used as government proxies to "re-centralize access" to online content.[47] The cooperation between governments and infrastructure owners is usually non-transparent, which creates new challenges for the protection of online free expression.

The Internet-infrastructure-centric approaches depict the Internet infrastructure as a system that consists of several layers. For instance, *Crocker* offers a thick-thin-thick layered model.[48] The model consists of three layers: the bottom, thick layer of telecommunications carrier protocols and standards, forwarding digital data through wired and wireless infrastructure; the middle, thin layer of core infrastructure, necessary to route data to the addressees; and the top, thick layer of application protocols enabling the functioning of various applications. In the logical layer, there are critical Internet resources: the Domain Name System, Internet protocols, and the standards for storage and transmission of information.[49] The Domain Name System serves as a database to allow a website to be found on the net by connecting the unique domain name of a website to a corresponding numerical combination or a unique address at which this website exists. Therefore, the system can be used as a choking point to implement censorship.[50] If governments receive control over the Domain Name System, this would enable them to control Internet connectivity and decide what

---

[47] Reidenberg, *supra 42*, p. 223.

[48] Dutton & Peltu.

[49] M. Mueller. Networks and States: the Global Politics of Internet Governance. Cambridge, MA: MIT Press, 2010.

[50] H. Klein, ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy, *The Information Society*18, 2002, p. 193–207.

digital speech is allowed to pass on to online platforms at the application layer.[51]

3 Domain Name System of Runet

The Runet Domain Name System (henceforth the Runet DNS) is governed by *the Coordination Center for the top-level domains RU and РФ*. It is a non-profit organization that was founded in 2001 in accordance with the multistakeholder model, which understands Internet governance as a common task for several stakeholders: the technological community of Internet developers, the private sector companies, the civil society, and states.[52] Initially, the Coordination Center had four co-founders. The Internet users were represented by *the Regional Public Center of Internet Technologies* (Региональная организация «Центр Интернет Технологий» *(РОЦИТ))*[53] and the Internet service providers by *the Union of Internet Operators (*Союз Операторов Сети Интернет (СОИ)).[54] The Russian government was represented indirectly by the *RIPN Network Information Center* (Российский НИИ развития общественных сетей (РосНИИРОС)), created by the state for technical support of the Russian Internet backbone, the Runet DNS, and the Internet exchange points.[55] The fourth cofounder, *the Association of Documental Telecommunications* (Общественно-государственное объединение «Ассоциация документальной электросвязи» (АДЭ)), was created by the state as an umbrella organization for the ICT sphere.[56] Among its members are telecommunication companies, like *MegaFon, Telecom*, and *Vimpelcom*; software developers, for instance, *Kaspersky Lab;* and other commercial organizations, for

---

[51] Mueller, *supra 49*; L. DeNardis, Internet Points of Control as Global Governance, GIGI Internet Conference Papers, Paper NO.2, August 2013, L. DeNardis, Global War for Internet Governance New Haven: Yale University Press, 2014.

[52] W. Dutton, "Multistakeholder Internet governance?" *World Bank*, 2015, https://pubdocs.worldbank.org/en/591571452529901419/WDR16-BP-Multistakeholder-Dutton.pdf.

[53] http://www.rocit.ru.

[54] http://www.soi.ru.

[55] http://www.ripn.net.

[56] http://www.rans.ru.

example, Yandex. In addition to t commercial companies, there are state scientific centers, including *the Russian Academy of Science* and *the Institute of State and Law*. The members also include governmental bodies such as the Ministry of Telecom and Mass Communications, the Ministry of Internal Affairs, and the Federal Security Service (FSB). Thus, it can be inferred that the fourth cofounder represented both the private sector and the state. Consequently, the cofounders can be depicted under the following scheme:

(1)+(1)+(1)+(1)
or
(one civil society actor – the Regional Public Center of Internet Technologies) + (one private sector actor – the Union of Internet Operators) + (one state actor – RIPN Network Information Center) + (one public-private actor – the Association of Documental Telecommunications).

In 2015, the number of cofounders was enlarged by adding two stakeholders. First, *the Ministry of Telecom and Mass Communications* (renamed in 2018 as *the Ministry of Digital Development, Communications, and Mass Media),* which had already participated indirectly through the *Association of Documental Telecommunications*, became the fifth stakeholder. Thus, for the first time, the Russian government intervened directly in the governance of the Runet DNS. Second, *the Institute for Internet Development* became the sixth stakeholder.[57] This organization was founded in 2015 to study the international trends in the development of the global Internet industry, and to offer strategic development programs for the governance of Runet. The Institute has five co-founders. Only one of them represents the Internet users, the already mentioned *Regional Public Center of Internet Technologies.* Two co-founders of the Institute represent the private sector: *the Russian Association for Electronic Communications (RAEC)*, presenting the Russian Internet industry,[58] and *the Media Communication Union,*[59] presenting the Russian Internet media industry. The fourth cofounder is *the Foundation for Developing Internet Initiatives,* a non-government

[57] http://ири.рф.

[58] http://raec.ru.

[59] http://www.np-mks.com.

organization. It was created by a state agency, the Strategic Research Agency for Forwarding New Projects. The president of the Supervisory Council of this agency is Vladimir Putin. Therefore, the fourth cofounder very probably represents the state. The fifth cofounder is a Russian citizen – *Herman Klimenko*. On the one hand, he is a successful IT businessman and, on the other, he was the advisor to President Putin from 2016 to 2018. Klimenko is known as a supporter of the idea that Runet should be tightly regulated by the state.[60] Thus, *the Institute for Internet Development* represents a public-private sector actor who supports the state and the private sector rather than the Runet users. In comparison with *the Association of Documental Telecommunications*, the other public-private actor, *the Institute* is an organization that focuses more on the Internet than on other spheres of communications. As a result, the scheme of sector actors in the Coordination Center was changed in favor of the state by having one cofounder added to represent the state directly and one cofounder to represent both the state and the private sector. Consequently, the new scheme can be depicted as follows:

(1)+(1)+(2)+(2)
or
(one civil society actor – the Regional Public Center of Internet Technologies) + (one private sector actor – the Union of Internet Operators) + (two state actors – RIPN Network Information Center and the Ministry of Telecom and Mass Communications) + (two public-private actors – the Association of Documental Telecommunications and the Institute for Internet Development).

This shift might lead to the Coordination Center being placed under the control of the Russian government. This control can be exercised through the Council of this organization. Formally, the supreme body of the Coordination Center is the General Shareholders' Assem-

[60] D. Turovsky, "RuNet Isolation and Anonymity Ban. What Herman Klimenko Has Done as President Advisor on Internet Issues" ["Изоляция Интернета и Запрет Анонимности. Что Делал Герман Клименко на Посту Советника Президента по Интернету"], *Meduza.io*, 13 June 2018, https://meduza.io/slides/izolyatsiya-interneta-i-zapret-anonimnosti-chto-delal-german-klimenko-na-postu-sovetnika-prezidenta-po-internetu.

bly, which decides on the general guidelines and appoints the Director of the Coordination Center. In practice, however, the power belongs to the Council, which runs the organization on a daily basis. The Council consists of fifteen members: the Director of the Coordination Center, two members appointed by him, and twelve members representing the cofounders (each cofounder has two representatives).[61] Each of the members has one vote. A decision can be adopted only if at least eight members are present[62] and if the decision receives at least eight votes.[63] We can determine that the two stakeholders representing the state and the two stakeholders representing both the state and the private sector jointly always hold a simple majority, namely, eight members and therefore eight votes. Consequently, these votes are sufficient to secure the required quorum and the adoption of a decision. Although any decision adopted by the Council can be quashed by the Board, the power of the latter is limited by the following conditions: firstly, all cofounders must be present[64] and, secondly, the vote must be unanimous.[65] Therefore, the Russian government represented by the Ministry of Telecom and Mass Communications can effectively block the Board's power, so that a decision adopted in coalition with the stakeholders representing the mixed interests can survive.

Thus, the Russian government has the opportunity to decide on the governance of the Runet DNS. Until 2015, the government played the part of an outsider who had to conclude agreements on cooperation with the Coordination Center. After 2015, the state became a powerful insider who may set the rules of the game.

By 2021, the list of cofounders shifted again. In 2019, the Union of Internet Operators, the only actor from the private sector, left the Coordination Center. Furthermore, in 2020, the Russian Federation be-

---

[61] General Shareholders' Meeting of the Coordination Center, "Charter of Non-For-Profit Organization "Coordination Center for Top-Level Domain RU" ["Устав Автономной Некоммерческой Организации Координационный Центр Национального Домена Сети Интернет"], adopted 12 July 2001, in the version of 19 November 2015, para 8.3, https://cctld.ru/about/orgstructure/charter.pdf.

[62] *Ibid*., para 8.13.

[63] General Shareholders' Meeting of the Coordination Center, *supra 62*, para 8.14.

[64] *Ibid*., para 3.1.

[65] *Ibid*., para. 3.5.

came a cofounder instead of the Ministry of Telecom and Mass Communication. The Russian State is represented by Roskomnadzor. Thus, the state has received even more power in controlling the Runet DNS. After this change, the scheme can be depicted as follows:

(1)+(0)+(2)+(2)
or
(one civil society actor – the Regional Public Center of Internet Technologies) + (no private sector actor) + (two state actors – RIPN Network Information Center and the Russian Federation) + (two public-private actors – the Association of Documental Telecommunications, renamed into Russian Association of Networks and Services (RANS) and the Institute for Internet Development).

4 Domain name suspension

4.1 The general order of domain name suspension

Domain name registrations are sold by the domain name registrars encompassing sixty companies in December 2021. Crucially, the Coordination Center can suspend the registration for a domain name accommodated in the .ru and .рф top-level domains.[66] This would lead to the disconnection of a domain name from the corresponding address on the host server. Consequently, a website owner is not deprived of the possession of the suspended domain name but rather precluded from using it. In terms of the Rules of Domain Name Registration (henceforth the Rules), this technique is called the termination of a delegation. To implement a termination, the Coordination Center corrects the

[66] Coordination Center, "Rules of Domain Name Registration in .ru and .рф" ["Правила Регистрации Доменных Имен в Доменах .RU и. РФ"], https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf. The Coordination Center can deny the registration of a domain name in other ways than suspension. For instance, deletion or blocking. Deletion means de-registration, which makes the relevant domain name available for registration by a new owner. In contrast, suspension only precludes the current owner from using the domain name. Blocking of the domain name means not only de-registration for the current owners but also preventing all other from using this domain name in the future.

relevant information in the Main Registry, a database containing names and corresponding addresses. The Main Registry can be presented as a Runet telephone book. From this perspective, if users "dial" the number corresponding to the suspended domain name, they will not be connected to the relevant website. Importantly, in contrast to website blocking, which affects only Runet users, a website with a suspended domain name is inaccessible not only from Russia but also from any point from abroad. To make the blocked website accessible again, the website owners can avail themselves of three options: first, to remove the content that triggered the domain name suspension; second, if they want to keep the banned content, to register a new domain name for this website and place a copy under that name; third, to leave the Runet zone and register the website under the same name but in another top-level domain.

According to the Rules,[67] the termination of a (domain name) delegation can be used under a general and special order. A domain name can be suspended following a general order under two conditions: if a website is involved in unlawful activities and if the termination is required by investigative state agencies or courts. The termination of delegation is inapplicable to mass media websites, websites hosted by foreign providers, social media platforms, and websites with a significant number of users. A third-level domain name (xxx.xxx.xx) can be suspended only after all reasonable means to contact the administrator of the second-level domain have been exhausted or if the administrator has refused to remove the content in question.

4.2 The special order of domain name suspension: the Authorized Organization Project

The special order of domain name suspension is available only to a few, so-called "authorized organizations" that participate in the scheme to which I refer as the Authorized Organization Project. According to

[67] Coordination Center, "Clarification on the Aplication of Paragraph 5.5 of Rules on Registration of Domain Names in .RU and .РФ" ["Разъяснения по Порядку Применения п.п 5 Правил Регистрации Доменных Имен в Доменах .RU и. РФ"], https://cctld.ru/domains/docs/5_5.

the information on the official website of the Coordination Center, this project appeared in 2012 to enhance the security on the Russian Internet.[68] The project allows Internet companies authorized by the Coordination Center to trigger domain name suspension under Article 5.7 of the Rules. The article states that a domain name registrar shall terminate the delegation of a domain name of a website following a request received from an authorized organization. However, this power is limited: an organization can request domain name suspension only if it has found child pornography, phishing, or botnet activity on the website. The technological implementation of the domain name suspension is fulfilled by the partner of the Authorized Organization Project – *the Technical Center "Internet"*, a company founded by the Coordination Center to operate the Main Registry of the Runet DNS.

The Coordination Center's reports include some figures to evaluate the effects of domain name suspension by the project. Additionally, the 2015 Report by the Director of the Coordination Center[69] provides statistics regarding one project partner – *Group-IB*. In 2014, this company asked the registrars to terminate the delegation of 1,397 domain names. As a result, 1,160 domain names were suspended; and only 153 of those were unblocked after the content in question had been removed. In 2015, Group-IB asked to terminate the delegation of 1,634 domain names. As a result, the delegation of 1,060 domain names was terminated; and 435 of those were unblocked after their owners removed the objectionable content. These figures may be interpreted in a way that the registrars satisfied only part of the requests sent by Group-IB, because the 2015 Report leaves unclarified what happened with 574 of the requests. It could be speculated that these requests were ignored by the registrars or the Coordination Center and, consequently, did not lead to suspension. However, I assume that these requests were left unanswered because the website owners had removed the content in question by the time the blocking was considered. The latter appears more probable as, following the 2016 Report by the Director of the

---

[68] Director of Coordination Center, "2015 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], https://cctld.ru/upload/files/dir_year_report_2015.pdf.

[69] *Ibid*, p. 11.

Coordination Center,[70] only three requests sent by authorized organizations were left without a response from the registrars. The 2016 Report provides the figures for termination requests in general, without the correlation between the authorized organization and the requests sent by it. According to the statistics, all requests sent by authorized organizations, 2,338 in total, were addressed by the registrars, which led to the suspension of 2,169 domain names and, in 169 cases, to removing the content in question in order to escape blocking.[71] The 2017 Report follows the pattern of the 2016 Report and provides only cumulative figures for all authorized organizations. According to the 2017 Report, the number of termination requests almost doubled in comparison with the previous year, from 2,338 to 5,496, leading to the blocking of 5,256 domain names.[72] In 2018, the numbers did not change significantly, with 5,803 termination requests and 5,633 suspended domains.[73] The next two reports provide, for the first time, not only cumulative figures but figures with the correlation between all of the authorized organizations and the requests sent by them, including the statistics about Roskomnadzor. According to the 2019 Report, the number of termination requests increased to 7,456, leading to the suspension of 6,687 domains.[74] Roskomnadzor sent 11 termination requests.[75] According

---

[70] Director of the Coordination Center, "2016 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], p. 12, https://cctld.ru/upload/files/dir_year_report_2016.

[71] *Ibid.*

[72] Director of Coordination Center, "2017 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], p. 13, https://cctld.ru/upload/files/dir_year_report_2016.pdf.

[73] Director of Coordination Center, "2018 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], p. 16–17, https://cctld.ru/upload/files/dir_year_report_2018.pdf.

[74] Director of Coordination Center, "2019 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], p. 12, https://cctld.ru/upload/files/dir_year_report_2019.pdf.

[75] *Ibid*, p. 16.

to the 2020 Report, 10, 229 termination requests were sent and 8,693 domain names were suspended.[76] Roskomnadzor sent 20 requests.[77]

4.3 New-school regulation by domain name suspension

From 2012 to 2016, the Authorized Organization Project involved only private organizations and companies. However, on June 16, 2016, domain blocking control became available for the government when Roskomnadzor joined the project by receiving the status of an authorized organization.[78] Consequently, the project turned into a new-school speech regulation tool. The government now had the opportunity to leverage the private power belonging to the owners of the DNS critical point of centralized control. In contrast to website blocking, the government had not set out clear legal frameworks for domain name suspension. The government's censorship relied on the private Rules of Domain Name Registration rather than on laws.

The only known example of Roskomnadzor using this capability is dated to 2017. In August 2017, Roskomnadzor reported that it had requested the termination of the delegation for the domain name *dailystormer.ru* because of the extremist speech published on the corresponding website.[79] This website represented a mirror of *The Daily Stormer* website placed in the US jurisdiction. Reportedly, the American counterpart was banished from the USA after Go Daddy, a US domain name registrar, had terminated its services because it had published an article supporting the white nationalist rallies held on August 12–13 that year in the city of Charlottesville, USA.[80] The Daily

---

[76] Director of Coordination Center, "2020 Report" ["Отчет Директора АНО «Координационный центр национального домена сети Интернет» А.А. Воробьева"], p. 13–14, https://cctld.ru/files/yr_report/dir_year_report_2020.pdf.

[77] *Ibid*, p. 20.

[78] Director of the Coordination Center, *supra 70*, p. 11.

[79] Roskomnadzor, "The Delegation of American Neo-Nazi Site in the Ru Domain is Terminated" ["Прекращено Делегирование Американского Неонацистского Сайта в Доменной Зоне .RU"], 17 August 2017, https://rkn.gov.ru/news/rsoc/news48958.htm.

[80] Meduza.io, "Booted from GoDaddy and Google, American Neo-Nazi Website The Daily Stormer Finds a New .RU home" *Meduza.io*, 16 August

Stormer swiftly migrated to the Runet domain name zone, concluded a contract with RU-CERT – the biggest Russian domain name registrar – registered the domain name dailystrimer.ru, and started publishing the same kind of information in Russian. However, RU-CERT terminated the domain name delegation a few days after receiving Roskomnadzor's request, forwarded via the Authorized Organization Project.

4.4 Implications for online freedom of expression

Through the Authorized Organization Project, the government, in cooperation with the private partners, has inserted a digital lock into the center of the Russian Internet infrastructure – the Runet DNS. This control, allowing the government to block unwanted content, has had negative implications for online freedom of expression, both from a legal and technological perspective.

From the legal perspective, online free expression is challenged as private power is leveraged for state censorship purposes. The project allows the government to circumvent the general order set for the termination of delegation that follows requests sent by investigative agencies or courts. The project relies on the special order of domain name suspension prescribed in Article 5.7 of the Rules. Moreover, as the example of the Daily Stormer demonstrates, the government does not follow the special-order rule. The article lists only three grounds for domain name suspension: child pornography, phishing activities, and botnet activity. In disrespect of this rule, Roskomnadzor triggered blocking for allegedly extremist speech, the ground absent from the list. Notably, the Coordination Center and RU-CERT violated the rule, as well, by implementing Roskomnadzor's request. Thus, Roskomnadzor can block online speech not only without any preliminary court review and any obligation to follow the administrative procedures prescribed by law for investigative agencies, but also without the limitations set for the Authorized Organization Project. This allows for the assumption that Roskomandzor can use this power to arbitrarily block any type of online content also in other situations.

2017, https://meduza.io/en/news/2017/08/16/booted-from-godaddy-and-google-american-neo-nazi-website-the-daily-stormer-finds-a-new-home-in-russia.

From a technical perspective, domain name suspension brings three threats: the impossibility to circumvent blocking, the impossibility to reuse the domain name on the Russian Internet, and the impossibility to keep a domain name parked, which enhances the negative effects on online free expression from a legal perspective. Firstly, the domain name suspension enables the state to make speech published on a targeted website inaccessible from any point in the world. There is no technological way to access it, except using unofficial and not widely known alternative domain name systems. This threat is more serious than in the case of website blocking. This control, in contrast to the domain name suspension, can be circumvented by using anonymization tools, masking that an access request has been sent from the territory of Russia. Although the Blacklisting, Anonymization, and Online Browsing Act (Law no. 276-FZ of 2017) aims to prevent circumvention by requiring the providers of anonymizing services to guarantee that their services are not used for accessing blacklisted websites, the implementation of these requirements remains questionable, especially by foreign providers, like Tor. Secondly, if a domain name is suspended, it cannot be reused because this domain name's registration, despite terminating the registration, remains valid. Consequently, it precludes a new website with the same domain name from appearing on the Russian Internet. If the owners of the website with the suspended domain name want to make the website available again, the content has to be copied to a website with another domain name. Thirdly, blocked speech can be suppressed further. The suspension of a domain name affects only accessibility rather than the existence of the content. In theory, the content on the website with the suspended name can be preserved, although blocked until this website exists. However, a new practice applied by *Yandex*, a partner of the Authorized Organization Project and one of the biggest hosting providers in Russia, challenges the existence of websites with suspended domain names. Since 2014, Yandex has been refusing to offer its domain name parking service to websites with suspended domain names. This parking is usually offered for domain names that are registered but not delegated, namely, for domain names that have not yet been attached to a certain website. Therefore, the termination of delegation triggered by Roskomnadzor's request may deprive the website with the suspended domain name of the possibility to stay on Yandex's hosting facilities. This means that the content can

be made not only inaccessible, but also physically non-existent unless the owner of the website with a suspended domain name finds a new hosting provider.

Thus, the combination of the government's unrestricted power, already used in an abusive manner, and the impossibility to avoid censorship may have drastic implications for online freedom of expression on the Russian Internet. Nevertheless, the effect of domain name suspension on the availability of online content can easily be detected, in contrast to that of ranking manipulations through Netoscope.

5 Conclusion

The Russian government has turned to the Russian Internet infrastructure as a tool to control online free expression. In addition to the website blocking, already addressed in the scholarly literature, the government has achieved more infrastructure-based control through the Authorized Organization Project. By leveraging the power of this project, the government now has been able to effectively and indirectly control online content. This control relies on domain name suspension. This new-school practice leads to making content inaccessible by detaching the relevant website's domain name from its address. As a tool, domain name suspension relies on the termination of domain name registration. The termination consists of two phases. At first, the domain name registrar in question terminates the registration of a domain name to comply with a request sent by Roskomnadzor. Then, the Coordination Center, through the Technical Center "Internet", a company controlled by it, disconnects this domain name from the corresponding numerical address in the Main Registry, the "telephone book" of the Russian Internet. Consequently, users, not only from Russia but also from abroad, cannot assess the website. Although domain name suspension though the Authorized Organization Project should be limited to child pornography, phishing, and botnet activities, the example of The Daily Stormer website demonstrates that the Russian government does not adhere to these limitations and may use the scheme to block any type of unwanted content. In addition to arbitrary censorship, domain name suspension control is technologically highly efficient. The efficiency originates from the impossibility for users to circumvent do-

main name suspension, even via a VPN (virtual private network), unless by turning to alternative domain name systems run by volunteers. The efficiency of domain name suspension is further enhanced by the impossibility for owners of websites to re-register a suspended domain name in the Runet zone. Furthermore, Yandex, a large hosting provider, can banish a website with a suspended domain name by refusing to keep its domain parked. Bearing these threats in mind, a website will probably remove any content that is undesired by the Russian government. And, if owners of websites want to keep banned content online, they can move it on a website with another domain name, although there is no guarantee that this website's domain name will not be swiftly blocked, as well. Alternatively, a website can be migrated from the Russian Internet to another top-level domain in which the blocked-in-Russia domain name can be registered again.

Importantly, while website blocking is based on a clear legal framework, the Authorized Organization Project relies on non-transparent public-private arrangements. Non-transparency, as one of the main threats to free expression, has been highlighted by the new-school regulation approach. Critics of the approach have suggested that this problem could be solved if the infrastructure owners would disclose the government attempts to leverage their private power to control speech and report all requests to remove content.[81] This suggestion is valuable for the Russian setting, as well. The partners of the Authorized Organization Project should disclose whenever the government uses the projects to affect content. However, the close cooperation with the government as a partner might bring into question such disclosures as a reliable source of information. Therefore, the implementation of domain name suspension by the government via the project has seriously endangered free expression on the Russian Internet.

---

[81] D. Nunziato, "I'm Still Dancing: The Continued Efficacy of First Amendment and Values for New-School Regulation" *Harvard Law Review,* 2014; 127(8), p. 376–372.