State regulation of online speech in Russia: The role of internet infrastructure owners

Liudmila Sivetc

Abstract

This article analyses recent developments in regulatory practices applied by the Russian government to online speech. The article relies on internet infrastructure-centric theories developed in the US legal scholarship by Lawrence Lessig and Jack Balkin, among others, and applies these theories to the Russian setting in a novel way. According to these theories, governments prefer indirect regulation of online speech by controlling the internet infrastructure to direct regulation by law. Indirect regulation is realized through cooperating between states and owners of the internet infrastructure. This article argues that this theoretical framework can be applied for analyzing regulation in Russia as well. The article looks at how Roskomnadzor, a government executive agency in the sphere of telecommunications, cooperates with owners of the Russian internet infrastructure. The article reveals that this cooperation may bring drastic implications to the right to freedom of expression enjoyed by Russian online mass media and internet users.

Keywords: Russian internet, internet infrastructure, cooperative speech regulation, free speech, online mass media

INTRODUCTION

The collapse of the Soviet Union in 1991 and the adoption of a new constitution in 1993 became signs of a new era in the Russian history. Article 2 of the 1993 Constitution declared human rights the highest value and obliged the state to protect them. According to Article 29, everyone has the right to freedom of thought and expression, and the right to be free from censorship. The level of protection of free expression was further increased in 1998 when Russia became a member of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 10 of ECHR especially stipulates that the right to freedom of expression shall be enjoyed 'without interference by public authority'. However, whether or not Russia fulfills this standard in practice is a disputable issue.[1] In fact, it appears that the current government

[1] Regarding the fulfillment of standard set in ECHR, there are two opposite views. Some authors assess Russia's attitude to judgments of the ECtHR as promising little for freedom of expression. See, for

is actively seeking for different ways to limit the freedom of expression as far as possible.

Article 10 of ECHR prohibits a state from interfering in free expression, but it does 'not prevent states from requiring the licensing of broadcasting, television or cinema enterprise.' The Russian government has utilized this possibility by introducing strict licensing rules in all of these spheres. A special government agency in the field of telecommunications and media—Roskomnadzor[2]—has been appointed to issue licenses and supervise their fulfillment. At the same time, the Russian government has an intense presence in the mass media market by controlling the most popular television channels directly, or through tycoons loyal to the Kremlin.[3] The control became even stronger in February 2016 when Article 2 of Federal Law № 305-FZ of 2014 prohibited foreign companies from entering the domestic mass media market. Furthermore, Article 19.2 of this Law does not allow foreign companies to possess more than 20 percent of a Russian company that owns a Russian mass media company. Thus, foreign companies are prevented from influencing Russian media not only directly but also indirectly.

Nevertheless, many researchers have noticed that the Russian segment of the global internet, known as RuNet, has for a long time remained a free zone for expressing oneself.[4] At least until 2012, RuNet was open for discussions according to

---

instance, Anton Burkov, '*The Impact of the European Convention on Human Rights on Russian Law'*. (Ibidem Press 2007); Laurence Helfer, 'Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime' (2008) Eur J Int'l L 19, 133; William Pomeranz, 'Uneasy Partners: Russia and the European Court of Human Rights' (2012) Human Rights Brief 19, 19; Tatyana Beschastna, 'Freedom of Expression in Russia as It Relates to Criticism of the Government' (2013) Emory Int'l L Rev 27, 1132–33. Other authors suppose that ECHR and judgments of the ECtHR have a significant potential to improve the protection of freedom of expression in Russia. See, for instance, Jeffrey Kahn, 'Building Bricks: Human Rights in Today's Emerging Economic powers. Freedom of Expression in Post-Soviet Russia' (2013–2014) UCLA J Int'l L & For Aff; 18, 21–3; Robert Ahdieh and Forrest Flemming, 'Toward a Jurisprudence of Free Expression in Russia: the European Court of Human Rights, Sub-national Courts, and Intersystemic Adjudication' (2013–2014) UCLA J Int'l L & For Aff 18, 39–41.

[2] The full name is the Federal Service for Supervision of Communications, Information Technology, and Mass Media or shorter in Russian 'Roskomnadzor'. Roskomnadzor is part of the Ministry of Telecom and Mass Communications. Roskomnadzor was founded in 2008 and consists of the central office in Moscow and 71 regional offices.

[3] Katja Lehtisaari, 'Market and Political Factors and the Russian Media' (2015) Oxford Reuters Institute for Study of Journalism <http://reutersinstitute.politics.ox.ac.uk/sites/default/files/Market%20and%20political%20factors%20and%20the%20Russian%20media%20-%20Katja%20Lehtisaari.pdf> accessed 10 December 2017; Carolina Pallin, 'Internet control through ownership: the case of Russia' (2017) Post Soviet Affairs 33, 1.

[4] See, for instance, Bruce Etling and others, 'Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization' (2010–2011) Berkman Center for Internet & Society of Harvard University <https://dash.harvard.edu/handle/1/8789613> accessed 4 December 2017; Karina Alexanyan and others, 'Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere' (2012) Berkman Center for Internet & Society of Harvard University <https://papers.ssrn.com/sol3/papers.cfm?abstract _id=2014998> accessed 4 December 2017; Sharyl Cross, 'Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the 'Reset'' (2013) Journal of Strategic Security 6, 14; Jaclyn Kerr, 'The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States' (2014) Center for International Security and Cooperation of Stanford University, Social Science Seminar Series 2, 24; Andrey Tselikov, 'The Tightening Web of Russian Internet Regulation' (2014) Berkman

Freedom House Report.[5] As concluded in a study conducted by the OpenNet Initiative, the regulation of the internet in Russia was done minimally and very subtly, without obvious signs of state censorship.[6]

However, as is well-known, the internet facilitates not only the expression of political opinion, but also may be used for disseminating hate speech, child pornography, extremist and terrorist materials. With this backdrop, Russian officials declared in 2011 that Russia needed to find its own balance between the protection of freedom of expression and combating unlawful online speech.[7] Consequently, RuNet became the target for state regulation. Since 2012, several laws have been introduced to intensify control over online speech. This development attracted a lot of criticism and was labeled as 'legal haste'[8] or even 'blitzkrieg'[9] against online free expression. Among the most criticized have been two laws that empowered Roskomnadzor to blacklist websites and require internet service providers to block such websites. Federal Law № 139-FZ of 2012 gives the agency power to blacklist websites containing child pornography, advocacy of drug abuse, and advocacy of committing suicide. Federal Law № 398-FZ of 2013 gives the same power regarding websites publishing extremist speech. Henceforth, these two laws are referred as Blacklist laws.

The quality of introduced Blacklist laws has been criticized both in Russian and foreign press and academia mainly because of the vagueness of what constitutes prohibited speech.[10] These definitions have created a danger of abuse by officials, and therefore suppressed online speech on a larger scale. Website blocking became one of

---

Center for Internet & Society of Harvard University, 1 <http:/srrn.com/abstract=2527603> accessed 10 December 2017; Julien Nocetti, 'Russia's "Dictatorship-of-the-Law" Approach in Internet Policy' (2015) Internet Policy Review 4, 2; Pallin (n 3) 16.

It worth noting, that, although RuNet was free from governmental control, it was not free from state surveillance. Deep packet inspection of traffic was already available for law enforcement agencies through SORM system. See details in Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State' (2013) World Policy Journal 30.

[5] Freedom House, 'Freedom in the World 2015, Country Report: Russia' *(Freedom House)* <https://freedomhouse.org/report/freedom-world/2015/russia> accessed 4 December 2017.

[6] Robert Deibert and Rafal Rohozinski, 'Beyond Denial' in Robert Deibert and others (eds) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010) 7.

[7] Cross (n 4) 16.

[8] Nocetti (n 4) 2.

[9] Alexey 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> accessed 4 December 2017.

[10] See, for instance, Rebecca Favret, 'Comment: Back to the Bad Old Days: President Putin's Hold on Free Speech in the Russian Federation' (2012-2014) Rich J Global L & Bus 12; Tselikov (n 4); Ольга Караулова, 'Пресса России: Закон Лугового обжалован в Страсбурге' (*BBC*, 11 March 2015) <http://www.bbc.com/russian/russia/2015/03/150311_rus_press> accessed 4 December 2017; Елена Мухаметшина, 'Заблокированные за освещение «болотного дела» интернет-издания считают, что блокировка равноценна закрытию' (*Ведомости*, 11 March 2015) <https://www.vedomosti.ru/newspaper/articles/2015/03/10/blokirovka-bez-granits> accessed 4 December 2017.

the main reasons for Freedom House to change Russia's status in 2015 from 'partly free to 'not free'.[11]

In spite of new, drastic implications for online free expression, studies on post-2012 speech regulation are scarce.[12] This article aims at filling this gap. Yet, the purpose is not to investigate all aspects of the relevant legislation rather to offer a novel, expository perspective on speech regulation. This perspective includes in the analysis not only regulatory schemes introduced by Blacklist laws, but also regulation set beyond law. Therefore, while sharing expressed in the previous research concerns about the vagueness of legal definitions, this article steps outside of positivist thinking and a purely legal dogmatic analysis. To assess online speech regulation with realism, this article relies on internet infrastructure-centric theories developed among others by Lessig[13] and Balkin.[14] According to these theories, governments have changed speech regulation practices from direct control by law to indirect regulation by controlling internet infrastructure. As internet infrastructure is mainly privately owned, the implementation of new control practices requires infrastructure owners to be involved in regulation.[15] This article argues that this theoretical framework, created for the research of US government regulatory practices, can be applied to analyzing regulation regarding RuNet as well. Therefore, the general objective is to test this framework as one to which online speech regulation in Russia may correspond. The framework is explained in the section 'Internet infrastructure-centric theories.' The subsequent section 'Three cases involving Roskomnadzor' answers the main research question: how do owners of the Russian internet infrastructure assist Roskomnadzor in regulating speech published by online mass media and what implications for online free expression does this cooperative regulation bring? This section presents a study depicting three cases: the case of Novaya Gazeta, the case of Grani,Ru, and the case of Netoscope. In each case, the article answers three specific questions. First, what role do infrastructure owners play in the relevant regulatory scheme? Second, can this scheme serve as an example of new-school regulation? Third, what implications does this scheme bring for online free expression? The analysis of these implications from the perspective of national and international law is outside the scope of this article.

INTERNET INFRASTRUCTURE–CENTRIC THEORIES

The internet has enhanced opportunities for self-expression. Internet users can publish content on free-of-charge online speech platforms. This content has the potential to gain

[11] Freedom House, 'Freedom on the Net 2015. Russia' *(Freedom House)* <https://freedomhouse.org/report/freedom-net/2015/russiaFreedom House> accessed 4 December 2017.
[12] Camille Jackson, 'Legislation as an Indicator of Free Press in Russia' (2016) Problems of Post-Communism 63, 355.
[13] Lawrence Lessig, *Code version 2.0* (Basic Books 2006).
[14] Jack Balkin, 'Old-School/New-school Speech Regulation' (2014) Harvard L Rev 127.
[15] According to Jack Balkin, in addition to public-private cooperation, characteristic features of new regulatory practices are digital prior restraints and collateral censorship. Yet, this article focuses only on the first feature—public-private cooperation.

popularity with a nearly world-wide audience. However, illegal speech has received the same advantage. It has posed new problems for governments. Since many internet users act anonymously and can be outside a state's jurisdiction, liability rules and court injunctions may become inefficient.

Some scholars adhering to ideas of cyber libertarianism even declare that decentralized online speech cannot be regulated at all.[16] As stated by John Gilmore, the internet 'interprets censorship as damage and routes around it.'[17] According to the opposite approach, cyber-paternalism,[18] governments can indirectly control online activities by affecting internet architecture. Lessig describes how code, which shapes the internet, affects our experiences of cyberspace. Code, rather than legal acts, has become the most effective regulatory tool or new law in the digital era. When governments realized this potential of code, they started actively regulating the private internet industry. As a result, the industry began encoding products in such a way that governments could obtain indirect control over online content.[19] This approach replaces Gilmore's declaration on a cyberspace without censorship with Balkin's statement that the internet interprets censorship 'as design requirements and builds them into system.'[20]

The revealed vulnerability of the internet to be regulated has led some scholars adhering to cyber-realism to question whether the internet contributes more to free expression or to the governmental control of it.[21] As emphasized by Drezner, the internet has put technological tools not only in the hands of citizens but also in hands of governments.[22] As summarized by Deibert, Palfrey, Rohozinski, and Zittrain in the research conducted within the OpenNet Initiative, many governments started utilizing firewalls and other technological tools to prevent undesired speech from being accessed.[23] However, whether or not technological tools have become the main regulatory practice is disputable. According to Morozov, to suppress free expression, governments rely more on 'sociopolitical' tools. Sociopolitical tools are applied mainly offline in forms of smearing, violent attacks and criminal charges against speakers. In

---

[16] See, for instance, David Post, 'Governing Cyberspace' (1996) Wayne Law Review 22; John Barlow, 'Censorship 2000' (*OnTheInternet*, October 2000) <https://www.isoc.org/oti/articles/1000/barlow.html> accessed 4 December 2017.

[17] Philip Elmer-DeWitt and David Jackson, 'First nation in Cyberspace' *TIME* (New York, 6 December 1993) 62.

[18] See, for instance, James Boyle, 'Faucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' (1997) U Cin L Rev 66; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999); Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (OUP 2006); Andrew Murray, *Information Technology Law, The Law and Society* (2nd edn, OUP 2013).

[19] Lessig (n 13) 5–7, 24.

[20] Balkin (n 14) 2305.

[21] Daniel Drezner, 'Weighing the Scales: The Internet's Effect on State-Society Relations' Brown Journal of World Affairs 16; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2011); Balkin (n 14).

[22] Drezner (n 21).

[23] Deibert and Rohozinsky (n 6) 49.

his opinion, sociopolitical methods can be even more effective than technological ones.[24]

This article acknowledges that sociopolitical tools are exploited in Russia as well. They include arrests of bloggers, patriotic cyber campaigns, and acquisition of media companies by oligarchs loyal to the Kremlin.[25] Such events are usually in the spotlight, while technological tools stay in the shadow. However, this article asserts that the Russian government focuses on technological solutions based on controlling the Russian internet infrastructure.

Interest in the internet infrastructure is connected to a phenomenon that Balkin describes as the merger of two infrastructures: the infrastructure of online free expression is merging with the infrastructure of its regulation. According to him, to secure free speech, it is not enough to prohibit a state from imposing censorship. To be expressed and to be heard by a public, speech needs a certain infrastructure.[26] This infrastructure consists of various media, technologies and institutions to forward the flow of information at any time.[27]

According to Balkin, the main elements of the speech infrastructure relied on by print mass media include the printing press, journalists, delivery chains, and newsstands. This infrastructure cannot be directly blocked by governments, but rather it can be influenced through such tools as fines, civil and criminal charges, and court injunctions. Balkin refers to these tools as 'old-school techniques of speech regulation'. Such old-school tools target publishers, speakers, and traditional technologies of information production and communication. One example is licensing schemes for allowing media to enter the market. At the same time, if governments chose to prevent certain information from becoming public, for example, by intercepting all delivery trucks, it would require enormous efforts and costs. Furthermore, it would be almost impossible to conceal such interference.[28]

Nevertheless, as highlighted by Balkin, the internet has dramatically changed traditional modes of producing and delivering information.[29] Consequently, speech

---

[24] Evgeny Morozov, 'Whither Internet Control?' (2011) Journal of Democracy 22.
[25] Tselikov (n 4).
[26] Balkin (n 14) 2297. In note 16 on page 2302, Balkin acknowledges that his ideas about the infrastructure of free speech as a set of interconnected technologies and institutions overlaps with Brett Frischmann's infrastructure theory. Frischmann describes infrastructure as a 'large-scale physical resource made by humans for public consumption' (Brett Frischmann, *Infrastructure: The Social Value of Shared Resources* (OUP 2012) 5) From the perspective of Frischmann's theory, Balkin's infrastructure of free speech may be seen as an infrastructure that is included into a broader meta-infrastructure or the cultural environment.
[27] Jack Balkin, 'The Future of Free Expression in a Digital Age' (2009) Faculty Scholarship Series of Yale Law School Paper 223, 432 <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1222&context=fss_papers> accessed 4 December 2017.
[28] Balkin (n 14) 2297.
[29] The author even uses the term 'revolution' to describe this change.

infrastructure has also changed.[30] Printing technologies have been replaced by digital ones. Distributors have been replaced by telecommunications and broadband companies who own the bottom or the physical layer of the internet infrastructure. Newsstands have been replaced by hosting service companies, cloud services, social media platforms, software applications, and search engines who own the top or the application layer of the internet infrastructure. In the middle of the internet infrastructure there is the central protocols layer with the Domain Name System, internet protocols and standards that make possible the delivering of information. These three layers present the underlying infrastructure for online speech.[31]

Thus, according to Balkin, the internet has become an infrastructure for digital speech. This change has vastly enhanced opportunities to express opinions. Yet at the same time, the change has made free expression more vulnerable to regulation because digital speech depends on the internet infrastructure. This dependence means that setting control of the internet infrastructure leads to setting control over online free expression.[32]

Following Balkin's theory, since the free speech infrastructure and the infrastructure of its regulation have been merging, methods of regulation have also changed. In comparison with old-school regulation, governments do not target directly speakers and owners of media companies to affect what speech is published online. In new conditions, it is possible to regulate speakers and publishers indirectly by leveraging the private power of internet infrastructure owners who are technical intermediaries carrying digital speech to listeners. Therefore, such 'public/private cooperation and co-optation' is one of the main features of new regulation practices named by Balkin as 'new-school speech regulation'. Through trade off and coercion, legal immunities and liability rules, intermediaries are used by governments to control online speech indirectly.[33]

While old-school regulation is mainly based on *post ante* techniques, such as penalizing by courts, new-school regulation is focused on *ex ante* tools, such as filtering and blocking by private intermediaries. In a pre-digital age, governments' attempts to prevent unwanted speech could lead to chilling effects, because of the expectation of possible punishment. New techniques allow governments to prevent undesired speech in a different way, through inbuilt 'digital locks', which routinely, silently and almost

[30] Balkin (n 14) 2305–06. Balkin speaks about the merger of three infrastructures: first, the infrastructure of free expression; second, the infrastructure of speech regulation; and, third, the infrastructure of private and public surveillance. Yet, this paper focuses on the merger of the first and the second infrastructures.

[31] The model of the internet as a structure consisting of several layers is proposed, for instance, by Steve Crocker (William Dutton and Malcolm Peltu, 'The emerging Internet Governance Mosaic: Connecting the Pieces' (2007) Information Polity 12, 65) and Jonathan Zittrain (Jonathan Zittrain, *The Future of the Internet – And How to Stop It* (YUP & Penguin UK 2008)).

[32] The same claim has been expressed in William Dutton and others, *The Changing Legal and Regulatory Ecology Shaping the Internet* (UNESCO Publishing 2011) 15; Laura DeNardis, *Global War for Internet Governance* (YUP 2014) 10. Yet, Balkin's contribution consists in providing an original theory which goes further this claim and provides a framework for understanding of new regulatory practices that became possible due to this phenomenon.

[33] Balkin (n 14) 2298–2310.

invisibly shape online content available for the public. This creates new dangers for the protection of free expression.[34]

Balkin's theory has attracted some criticism. It is not connected with his theoretical basis but challenges Balkin's conclusion that online free expression is endangered. For example, according to Nunziato, new-school regulation can still be adequately answered by using legal doctrines developed for old-school regulation techniques. Besides, the danger of public-private cooperation is overestimated because key online speech intermediaries, such as Google, Microsoft, Yahoo!, and Facebook, have declared their commitment to free speech values. These companies have exposed efforts of several governments to control speech. One example proving the intermediaries' resistance to new practices of regulation is annual transparency reports on requests received from the government and on answers given by intermediaries to such requests.[35]

While taking this criticism into account, the remainder of this article aims to analyze the recent developments in the regulation of free expression in Russia as a change from old-school regulation practices to new-school ones. The following section, after outlining political and legal background, discusses three cases as examples proving this change. A special focus is laid on drastic implications for freedom of expression to which these examples can lead.

THREE CASES INVOLVING ROSKOMNADZOR

Russian internet: political and legal background

In contrast to traditional media, RuNet remained for a long time free from direct state regulation. RuNet might escape the attention of state regulators because of its low penetration rates. In 2008, internet penetration covered only 37 000 000, 26 percent of the population.[36] Nevertheless, internet usage increased rapidly. In 2011, comScore, Inc., a company leading in online platforms measurement analytics, ranked Russians as second in time spent on social networking, due to the facts that 82 percent of internet users, and almost 100 percent of young people between 18 and 24, visited regularly social networks. That same year, the UK ranked eleventh; the USA, thirteenth; and Germany, fifteenth.[37] In 2013, internet penetration in Russia covered already 81 000 000, 57 percent of the population.[38] Also that year, the audience size of the most popular domestic social network, VKontakte, exceeded the audience size of the most popular TV channel, Cannel One.[39]

---

[34] Balkin (n 14) 2340–42.
[35] Dawn Nunziato, 'I'm Still Dancing: The Continued Efficacy of First Amendment and Values for New-School Regulation' (2014) Harvard L Rev 127, 368, 371.
[36] FOM (Фонд Общественное мнение) 'Интернет в России: динамика проникновения. Лето-2016' (*FOM* 18 October 2016) <http://fom.ru/SMI-i-internet/13021> accessed 17 December 2017.
[37] Giles Keir, 'Internet Use and Cyber Security in Russia' (2013) Russian Analytic Digest 134, 2–4.
[38] FOM (n 36).
[39] Keir (n 37).

The increase in the popularity of RuNet coincided with a period of political instability caused by mass unrest during the winter of 2011–2012. Street protests against the results of the December 2011 parliamentary election were almost completely ignored by television, but they were lively discussed on the Russian internet.[40] Therefore, some researchers called RuNet an alternative for the Russian public sphere.[41]

However, the freedom of RuNet was challenged by Blacklist laws. The increased threat of censorship was highlighted by a wide protest campaign[42] initiated in 2012 by such internet companies as Google and Yandex, the latter providing the most popular search engine in Russia, preferred to Google by 62 percent of Russian internet users.[43] For example, Wikipedia placed on its main webpage a poster warning that internet censorship would lead to a world without free knowledge.[44]

Despite interfering in the right to freedom of expression, it appears that Russia's approach does not contradict the international standard stated in Article 10 of ECHR. This article allows restrictions as '(…) prescribed by law and necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals (…)'. Furthermore, Blacklist laws, as stated by the Russian Constitutional Court,[45] do not contradict the Russian Constitution as far as they limit the dissemination of illegal speech. According to part 4 of Article 29 of the Constitution, the advocacy of speech inciting hatred on the basis of race, nationality, religion, language or social status is prohibited. Furthermore, such speech is deemed as a type of extremist activity according to Article 1 of Federal Law № 114-FZ of 2002 and criminalized if speech is disseminated by mass media or via the internet according to Article 282 of Criminal Code. Article 16 of Federal Law on Mass Media № 2124-1-FZ of 2015 stipulates that a media outlet can be shut down by a court after receiving two warnings from Roskomnadzor for publishing extremist speech.

As declared by Roskomnadzor, its activities in the sphere of RuNet are aimed at facilitating free expression and, at the same time, protecting Russian internet users from

---

[40] Alexei Makar'in and Leonid Polishchuk, 'Civic Culture and Political Collective Action in Russia' (2012) <https://www.hse.ru/data/2012/10/25/1245778460/Makar%27in-Polishchuk%20paper.pdf> accessed 4 December 2017.

[41] Alexanyan and others (n 4); Nocetti (n 4).

[42] Алла Забровская, 'Новый Закон Угрожает Свободному Интернету' (*Google Russia Official Blog*, 12 July 2012) <https://russia.googleblog.com/2012/07/blog-post.html?spref=bl> accessed 4 December 2017; Yandex, 'О Законопроекте № 89417-6' (*Yandex Official Blog*, 10 July 2012) <https://www.yandex.ru/blog/company/48073> accessed 4 December 2017.

[43] Yandex is used by 62 percent of Russian internet users, and Google is used by 27.6 percent. See details in Matthew Bodner, 'Russia Presents new State-Owned Search Engine Called Sputnik' (*The Moscow Times*, 22 May 2014) <https://themoscowtimes.com/articles/russia-presents-new-state-owned-search-engine-called-sputnik-35706> accessed 4 December 2017.

[44] Даниил Туровский, 'Как Устроен Роскомнадзор' (*Meduza.io* 13 March 2013) <https://meduza.io/feature/2015/03/13/kak-ustroen-roskomnadzor> accessed 7 December 2017.

[45] Конституционный Суд РФ, определение по делу N1759-O от 17.07.2014 (Russian Constitutional Court, Ruling N1759-O in the case of Kharitonov).

dangers connected to global cyberspace.[46] Among the main dangers are the abuse of freedom of the press and dissemination of violent extremist speech.[47]

Roskomnadzor and online mass media monitoring: *Novaya Gazeta* case

One of the main tasks of Roskomnadzor is controlling the mass media, both printed and published online. Roskomnadzor oversees that the media follow requirements prescribed in mass media law and do not publish certain kinds of content.[48] According to Alexandr Zharov, the Head of Roskomnadzor, every week the agency checks publications made by five thousand mass media outlets.[49]

To monitor publications made online by mass media, Roskomnadzor utilizes a special system developed by a private company named DataCenter. This system identifies prohibited content by using a vocabulary of five million key words, phrases, and images. When a threat is detected, the system informs an official. She then checks the suspicious publications. The analytical center is situated in the Main Radio Frequency Center, an enterprise founded and controlled by Roskomnadzor. The system was adopted in December 2011 as an experiment in 19 Russian regions.[50] By the end of 2016, the scope of monitoring was extended to all Russian regions.[51]

If Roskomnadzor concludes that a suspicious publication represents unlawful speech, the agency sends a warning notification to the relevant publisher. The publisher is expected to remove the identified content. In 2013, Roskomnadzor sent 23 warning notifications for publications suspected in extremism.[52] In 2014, the number of notifications was 35,[53] in 2015—39,[54] and in 2016—11.[55] Nevertheless, a publisher can challenge a warning notification in court, and if their case is won, they may keep the speech in question available on their website. Winning a suit also has another, practical consequence: the invalidation of a warning notification. This is important because receiving two uncontested warning notifications within twelve months means that Roskomnadzor can lodge court proceedings in order to shut down a publisher's

[46] Roskomnadzor, 'Public Report 2015' 9 <http://rkn.gov.ru/docs/docP_1485.pdf> accessed 17 December 2017.
[47] ibid 8.
[48] Article 4 of Federal Law № 2124-1 On Mass Media sets out that mass media shall not publish certain kinds of information.
[49] Юлия Воронина and Татьяна Шадрина, 'Цензура.net' (*Российская Газета*, 17 February 2016) <https://rg.ru/2016/02/17/zharov-absoliutnaia-svoboda-predpolagaet-absoliutnuiu-otvetstvennost.html> accessed 4 December 2017.
[50] Виталий Петров, 'Контрольная дата: интернет-СМИ будет мониторить специальный аппарат' (*Российская Газета*, 11 November 2011) <http://www.rg.ru/2011/11/03/control.html-> accessed 4 December 2017.
[51] Roskomnadzor, 'Public Report 2016' 62 (Roskomnadzor's Official Website, 18 April 2017) <https://rkn.gov.ru/docs/doc_1646.pdf> accessed 17 December 2017.
[52] Roskomnadzor, 'Public Report 2013' 65–66 (Roskomnadzor's Official Website, 25 April 2014), <https://rkn.gov.ru/docs/docP_1154.pdf> accessed 17 December 2017.
[53] Roskomnadzor, 'Public Report 2014' 22 (Roskomnadzor's Official Website, 23 April 2015) <https://rkn.gov.ru/docs/doc_1240.pdf> accessed 17 December 2017.
[54] Roskomnadzor (n 46) 56.
[55] ibid 58.

business.[56] In 2015, at least two online mass media companies were closed by the Supreme Court in such a manner.[57]

On 9 September 2014, Novaya Gazeta, one of the main mass media companies in opposition to the Russian government, published an article on its website, novayagazeta.ru, entitled *If We Are Not the West, Then Who Are We?*[58] This article criticizes a view expressed by some Russian officials that Russians should not adopt Western values, but rather should follow their own national traditions. The article compared this official position with ideas expressed by Adolf Hitler in *Mein Kampf*. The author, Iulia Latynina, known in Russia for severe criticism of the Kremlin, argued that Russian culture became development-oriented and began fulfilling its potential only after becoming the part of European cultural traditions. Without importing Western values, Russia would have stayed a retrograde, Asian-like state. Without being brought up in accordance with European culture, millions Russian emigrates would not have been able to adopt so easily in the West. If Russians had not felt close to Europeans, Russians would have rather moved to China, something only a few have done. Yet, the dependence of Russian culture on other cultural traditions does not make Russians deficient in comparison with other peoples. The development of mixed nations in cultural terms is a norm. The article concluded that there is no 'pure Russian nation'. Furthermore, a 'pure' nation that had developed limited to its own cultural elements could hardly be found anywhere.[59]

On 10 October 2014, Roskomnadzor sent a warning notification to Novaya Gazeta. Roskomnadzor informed that Latynina's article contained several sentences using unlawful extremist speech. The agency also warned that the publisher was responsible for the breach of Law № 2124-1 of 2015 on Mass Media and Law № 114-FZ of 2002 on Counteraction against Extremist Activity.[60]

The first set of specified sentences was the only one in the article that contained words 'Hitler', '*Mein Kampf',* and 'fascism'. The author wrote half a year after a mass protest in Kiev, the capital of the Ukraine that,

> Russian officials, members of the Russian Parliament, discovered the existence of a special "Russian culture" that resists the spiritual impoverishment of Europe. However, they have found nothing new. Hitler, in *Mein Kampf*, already opposed strict Nordic culture to present depravity and spiritual impoverishment. This is an ordinary trick used

[56] This procedure is provided for by Article 16 of the Law on Mass Media.
[57] First, Chinovnic.ru was closed following the judgment of the Supreme Court № АКПИ15-1021 of 13 October 2015; second, 66.ru was closed following the judgment of the Supreme Court № АКПИ15-1022 of 20 October 2015.
[58] The English translation of this article under the title '*If Russia isn't the West, then what is she?'* is available at< http://euromaidanpress.com/2014/10/13/if-russia-isnt-the-west-then-what-is-she-full-text-of-article-accused-of-extremism-and-censored-in-russia/> accessed 17 December 2017.
[59] Юлия Латынина, 'Если мы не Запад, то кто мы?' (*Novaya Gazeta*, 9 September 2014) <http://www.novayagazeta.ru/arts/65180.html> accessed 17 December 2017.
[60] Таганский районный суд города Москвы, Решение по делу № 2- 4369/2014 от 22.01.2015, 2 (*Roskomnadzor v Novaya Gazeta* [2015] Tagansky Raionnyi Sud goroda Moskvy).

> by fascism: under the pretense of liberation of the nation from "alien culture," to free the nation from any culture at all and to immerse it in the days and habits of barbarism.[61]

The second set contained a claim that

> [O]nly three contemporary developed nations—Jews, Chinese, and Indians—could claim their own way of cultural formation during thousands of years. While all others—a graft, crossbreed, mudblood.[62]

Novaya Gazeta concealed notified sentences on its website with black covers, over which were written 'Censorship. Concealed following Roskomnadzor's requirement before a final court judgment'. Then, Novaya Gazeta challenged the notification before courts, but eventually lost the case on 4 August 2015.[63] The court disagreed with the applicant's argument that the warning notification was unlawful because it was based on the incorrect assessment of the speech in question. An expert assessment submitted by Novaya Gazeta had concluded that neither the notified sentences nor the article contained unlawful speech. Yet, the court preferred another assessment that favored Roskomnadzor. It was made by an independent expert who had confirmed that the notified sentences did exhibit extremist speech.[64]

Nevertheless, the article is still accessible on Novaya Gazeta's website. Although the black covers are still in place, they hide approximately eight percent of the whole text and do not change the meaning of the article.

From the perspective of Balkin's theory, the case of *Novaya Gazeta* represents an example of an old-school regulation practice in which Roskomnadzor interacted with a publisher. The RuNet infrastructure was not used as a regulatory tool. Owners of the physical layer—internet access and hosting service companies—did not cooperate with the state agency. Rather, they were involved only as technical intermediaries which carried Roskomnadzor's warning notification to the publisher. The latter had an opportunity to react to this notification by concealing the notified sentences. Thereby, the publisher realized the goal of notification—the removal of unlawful speech by the website owner. Moreover, this goal was achieved without undue over-blocking, because the majority of the article in question was left accessible to the public. When readers access the article, they are informed that some parts have been concealed at the requirement of Roskomnadzor. If RuNet users want to know what content has been covered up, they can find it in the court rulings published online.

Roskomnadzor and online speech blocking: *Grani.Ru* case

[61] *Roskomnadzor v Novaya Gazeta* [2015] 3.
[62] ibid 2.
[63] On 2 January 2015, Novaya Gazeta lost proceedings in Tagansky District Court of Moscow; on 28 April 2015, it lost in appeal in Moscow City Court; on 4 August 2015, it lost in cassation in Moscow City Court.
[64] *Roskomnadzor v Novaya Gazeta* [2015] 6, 7.

In October 2012, Roskomnadzor was empowered to conduct a special list (henceforth the Blacklist), which includes websites with certain illegal content: child pornography; advocacy of drugs and suicide; and illegal gambling.[65] The aim is to force website owners to remove prohibited speech from listed websites or make it inaccessible to RuNet users. However, if website owners do not react to Roskomnadzor's notifications, which is forwarded to them via relevant hosting providers, within three days,[66] blacklisted speech is blocked by internet access providers. The latter are obliged to install special software for that purpose and check updates to the Blacklist.[67] By the end of 2015, more than four thousand internet access providers received special authorization from Roskomnadzor to get automatic access to a database with blacklisted websites.[68]

In 2015, 49 000 websites and web pages were included on the Blacklist. Of those, 31 000 were blocked. Nevertheless, 30 000 were removed from the list and unblocked because the blacklisted content had been deleted.[69] In 2016, the number of blacklisted websites and web pages exceeded 88 500.[70] Of those, approximately 48 700 were unblocked.[71]

Usually, instead of getting access to a blocked website or a page, a RuNet user sees a notice saying that access to that particular web resource has been blocked following state bodies' requirements.[72]

Alexandr Zharov, the Head of Roskomnadzor, has declared that there was no intent to build a Chinese-like firewall or eradicate all kinds of illegal content. Only certain types of content are targeted. Furthermore, he has recognized that the full blocking of blacklisted content is impossible to achieve because of various ways to circumvent blocking. Internet users who really want to access blacklisted content can avail themselves of different technical tools, like VPN-services, anonymizer software, and proxy servers. Consequently, Zharov has stressed that Roskomnadzor applies Blacklist laws to minimize traffic to blacklisted websites and prevent the average internet user from stumbling on prohibited speech when surfing on RuNet.[73] Zharov has

---

[65] Russian Government, Regulations on Roskomnadzor, para 5.1.7, adopted by Order N 228 of 16 March 2009 and amended by Order N 1100 of 26 October 2012.
[66] Federal Law № 398-FZ On Amending the Federal Law on Information, Information Technologies and on the Protection of Information, 28 December of 2013, Article 15.1.7.
[67] Roskomnadzor, Order 01.11.2012, Temporary Regulations on Performing the State Function on Creating, Framing and Operating the Unified Automatic Information System 'Single Register of Domain Names, URL addresses and IP Addresses Which Identify Internet Websites with Information Dissemination of Which Is Prohibited in Russia', paras 46–48.
[68] Roskomnadzor (n 46) 15.
[69] Roskomnadzor (n 46) 59.
[70] Roskomnadzor (n 51) 64.
[71] ibid 65.
[72] Туровский (n 44).
[73] АнастасияГолицына and Елизавета Брызгалова, 'Интервью – Александр Жаров, глава Роскомнадзора' (*Ведомости*, 1 August 2014) <http://www.vedomosti.ru/newspaper/articles/2014/08/01/zablokirovat-informaciyu-v-internete-navsegda-nevozmozhno> accessed 4 December 2017.

also acknowledged[74] that after being blocked, a website may receive additional attention because of an outcry in Russian mass media and the blogosphere. According to his estimation, such additional attention declines after seven to ten days because of the following two factors. On the one hand, media coverage is shrinking, and, on the other hand, more and more websites on which blacklisted content has been replicated are being included on the list. As a result, the audience of a blocked website becomes smaller in size than it was when the website was initially blocked. After a month, as Zharov claims, only 10 percent of the audience persists in trying to circumvent blocking.[75] Thus, if these figures are correct, it may be concluded that the practice of blacklisting makes prohibited content inaccessible to 90 percent of RuNet users.

According to Roskomnadzor, when the blocking procedure was introduced, the agency did not specifically check whether a certain listed website had been blocked by a certain access provider. Omissions were detected during regular routine inspections. Then, special officials were engaged to verify whether a blacklisted website could be accessed via the connection offered by a certain access provider. Yet, this solution soon became inefficient because the number of blacklisted websites to be checked reached 100 000. Roskomnadzor decided to solve this problem by creating a technical tool. The agency connected its own system, 'Ревизор' ('Controller' in English) to providers' networks. This system employs ten thousand robots send more than 120 000 000 requests in an hour to blacklisted websites. If a request has been forwarded by a provider to a blacklisted website, the system signals to an official who checks why the website is not blocked.[76]

If an access provider has failed to block blacklisted websites, Roskomnadzor can bring administrative proceedings before a court, and a provider can be fined.[77] In 2015, Roskomnadzor lodged 501 such proceedings and won 443 of them.[78] One example of when Roskomnadzor lost was in a case where a provider had fulfilled the blocking requirement 24 days in a month. Yet, six days that same month, blocking had not taken place. A court decided that such a breach was too insignificant to place liability on a provider.[79]

Since 1 February 2014, Roskomnadzor's blacklisting power has been enhanced by Federal Law № 398-FZ of 2013. This law empowers Roskomnadzor to include on the Blacklist websites containing calls for mass unrest, committing extremist activities or

---

[74] Alexandr Zharov, Interview (*Russia24*, 11 March 2015)
<http://rkn.gov.ru/press/interview/news30896.htm> accessed 4 December 2017.
[75] Ibid.
[76] Воронина and Шадрина (n 49).
[77] The liability is set in part 3 of Article14.1 of the Code of Administrative Procedure. The ground of the liability is the breach of license conditions. Sanctions include a warning or a fine in the amount of 30 000–40 000 rubles (approximately € 500). Yet, on 22 February 2017, the Code was amended by Federal Law № 18-FZ. The law introduced a new article, 13.34, that provides for a new offence in case of non-implementing Roskomnadzor's requirement about blocking. Fines for internet access providers arose to 50 000–100 000 rubles (approximately € 1000–2000).
[78] Roskomnadzor (n 46) 61.
[79] Арбитражный суд Ярославской области, решение по делу № А82-12025/2016 от 28.10.2016 (*Roskomnadzor v Yaroslavl'-GSM* [2016] Arbitrazhnyi Sud Yaroslavskoi Oblasti).

participating in public meetings conducted in violation of the law. In such cases, the Prosecutor General and her Deputies require Roskomnadzor to begin blacklisting. In contrast to the blacklisting procedures introduced earlier, Roskomnadzor does not notify website owners about blocking, but contacts access providers so that blacklisted content is blocked immediately.

On 13 March 2014, Roskomnadzor, following a notice sent by the Prosecutor General's Office, required access providers to block the website of Grani.Ru, an oppositional online mass media outlet. On the same day, the website www.grani.ru was blocked. According to the notice, the website published calls to participate in unlawful public meetings, which is attributed to extremist speech. The website published an article[80] about an initiative, 'Strategy-6'. This initiative called for meetings every sixth of the month to support people arrested for participating in mass protest actions held in Moscow on 6 May 2012. Furthermore, the website contained photographs and video files that showed how participants of meetings organized within that initiative did not obey the police and brought public order. The Prosecutor General's Office decided that the article, and a considerable part of other content published on the website, justified such activities. Therefore, the website was accused of promoting participation in unlawful public meetings.[81]

Notably, unblocking is possible under one of the following conditions: first, if a court has ruled that a decision on the inclusion of a website on the Blacklist is invalid; and second, if a website owner has removed blacklisted content or made it inaccessible.[82] Grani.Ru decided to protect its content and consequently lodged court proceedings, but eventually lost on 2 September 2014.[83] Grani.Ru argued that neither the Prosecutor General's Office notice nor the blocking notification sent by Roskomnadzor to internet access providers clarified what content became the reason of blocking: whether it was the article, photo and video files, or some other content. As claimed by Grani.Ru, the Prosecutor General's Office should have specified which web pages contained unlawful speech, and consequently, Roskomnadzor should have ordered to block only those pages, but not the whole website. The court disagreed and stated that the reason of blocking was the fact that a significant part of published materials constituted unlawful speech. The speech in question acquired its unlawful character mainly because of the publisher's biased way of describing events. Readers could receive the wrong impression that participating in the public meetings was not in

---

[80] Grani.Ru, 'На Манежной задержаны участники схода в защиту «болотников»' (*Grani.Ru*, 6 March 2015) available outside the RuNet zone at <http://graniru.org/Politics/Russia/activism/m.226296.html> accessed 4 December 2017.

[81] Таганский районный суд города Москвы, Решение по делу № 2-1343/2014 от 06.05.2015, 6 (*Roskomnadzor v Grani.Ru* [2015] Tagansky Raionnyi Sud goroda Moskvy).

[82] Russian Government, Order N 1101 of 26 October 2012, Rules on Creating, Framing and Operating the Unified Automatic Information System 'Single Register of Domain Names, URL addresses and IP Addresses Which Identify Internet Websites with Information Dissemination of Which Is Prohibited in Russia', para 14a).

[83] On 6 May 2014, Grani.Ru lost proceedings in Tagansky District Court of Moscow; on 2 September 2014, Grani.Ru lost in appeal in Moscow City Court.

breach of law. The court did not conduct its own investigation into whether or not the speech represented unlawful extremist content. Instead, the court said that it 'trusted' a conclusion made by an expert-prosecutor[84] who must be competent in that issue. Regarding blocking the whole website rather than a web page, the court ruled that Law № 398-FZ allows Roskomnadzor to blacklist an 'information resource'. The court interpreted this definition as including both a website and a webpage. Therefore, the court concluded that there was no legal obstacle to blocking the whole website.[85]

As a result, the website of Grani.ru is still blocked. Not satisfied with such an outcome, Grani.Ru brought a complaint before the European Court of Human Rights on the grounds that the applicant's right to freedom of expression had been violated.[86]

Looking at the case of *Grani.Ru* through lenses of Balkin's theory highlights stark contrast to the *Novaya Gazeta* case. In the former case, the Russian government turned to the RuNet infrastructure as a regulatory tool. Although the Blacklist technological solution is aimed at the removal of content from blacklisted websites by their owners, as well as the regulatory scheme in *Novaya Gazeta* case, the Blacklist regulatory scheme takes into account that website owners may ignore their obligation to remove blacklisted content. Therefore, the Blacklist scheme is not targeted at publishers, but rather focused on making blacklisted speech inaccessible by RuNet infrastructure owners without publishers' consent. Moreover, if a website is included on the Blacklist following a notice sent by the Prosecutor General's Office, Law № 398-FZ does not even require Roskomnadzor to contact a website owner about blocking. It is sufficient if a blocking notification is forwarded to the publisher by his hosting provider. As a result, in the case of *Grani.Ru*, the publisher was denied any active role. He was informed after the website had already been blocked and could only challenge the blocking notification *post facto*.

Thus, in comparison with old-school regulation practices, which presuppose the involvement of publishers, the Blacklist regulatory scheme is an example of a new-school regulation practice. This scheme circumvents website owners but still controls content published by them. The inherent feature of the Blacklist regulatory scheme is the co-optation of access providers—owners of the physical layer of the RuNet infrastructure.

Although the cases of *Novaya Gazeta* and *Grani.Ru* are examples of practices belonging to different regulatory schools, these cases can have almost the same consequence for publishers' freedom of expression. As stipulated in Article 16 of Federal Law on Mass Media № 2124-1-FZ of 2015, the second warning notification

---

[84] The expertise was made the day before the Prosecutor General's Office issued the notice. The expert was a prosecutor from the Department of Supervision of Compliance with Laws on Federal Security, Interethnic Relations, Counteraction against Extremism and Terrorism. The expert's conclusion was approved by the head of the Department.

[85] *Roskomnadzor v Grani.Ru* [2015] 5–7.

[86] Application no. 12468/15 OOO FLAVUS v. Russia, lodged 2 March 2015 and joined with four applications in case OOO FLAVUS and the Others v. Russia. The case was pending during the time of writing this article.

received within 12 months can lead to liquidating an online newspaper as an organization. The liquidation occurs if a court adopts a relevant decision following a claim lodged by Roskomnadzor. Such an outcome cannot be triggered by a blocking notification. However, a blocking notification can lead to the shutting down of an online newspaper as a source of information. Although, formally an online newspaper keeps its license and can continue publishing, the blocking of the newspaper's website makes publishing impossible in practice, at least until a court decides that the blocking was illegal. Consequently, even on the first attempt and without a previous court review, Roskomnadzor can prevent the publisher from making its content available to the public. Although consequences for publishers' freedom of expression are dramatic, publishers are not directly contacted by Roskomnadzor, nor do they have a chance to prevent blocking.

Another threat to freedom of expression of online media publishers is that the Blacklist regulatory scheme might become the main tool to regulate websites suspected of publishing extremist speech. This may happen because the Prosecutor General's Office has two options to block online content. First, it can bring proceedings before a court and claim a violation of Federal Law № 114-FZ of 2002 on Counteraction against Extremist Activity. In such a case, extremist content can be blocked following a court decision as a result of a court investigation and balancing the protection of freedom of expression with the protection of public order. Second, the Prosecutor General's Office can send a notice to Roskomnadzor. In that case, allegedly extremist content will be included on the Blacklist and blocked by access providers in a routine, automatic manner. The first option requires much time and effort from the Prosecutor General's Office to achieve blocking. The second approach appears to be a much less demanding practice, which may lead to the same result happening within a single day. Therefore, prosecutors may be inclined to prefer this new-school regulation tool. Moreover, the court in the case of *Grani.Ru* refused to assess the illegality of blacklisted content and fully relied on the conclusion made by the Prosecutor General's Office in its notice to Roskomnadzor. Such limited court investigation conducted after blocking renders online publications more vulnerable to unjustified suppression than if publications were properly assessed during court proceedings held before blocking.

This can lead to drastic implications, not only for publishers' free expression, but also for RuNet users' right to seek and receive information. RuNet users cannot access the whole website. A notice on the screen informs visitors that the website in question cannot be accessed because it has been placed on the Blacklist by Roskomnadzor. If the website is searched for via Yandex, the web browser offers a link providing information on the reason for blacklisting. Following this link will allow the user to see that the website was blacklisted on 13 April 2014 in accordance with a decision of the Prosecutor General's Office. To get access to the blacklisted content, users could utilize special software, which, even if free of charge, requires from them specific skills. Another way to get knowledge on what speech triggered blocking could have been reading of the relevant court judgements. However, in contrast to the case of *Novaya*

Gazeta, if users turn to the court rulings in the case of *Grani.Ru*, they will find no citation of the blacklisted content. The rulings contain only general referrals to the article and to other vaguely identified materials. Consequently, readers are not able to form their own opinion. They only can, like the court, 'trust' that the conclusion made by prosecutors was correct.

Roskomnadzor and database with suspicious websites: the case of Netoscope

Netoscope is the name of a private project started in 2012 in order to develop a platform for technical collaboration among interested parties from the internet community. According to information placed on the project's website,[87] Netoscope-partners are domain name registrars accredited in the RuNet zone, and a few private companies from the Russian internet industry, including Mail.Ru Group, Yandex, Rostelecom, Group-IB, Kaspersky Lab, Technical Center 'Internet,' and BI.ZONE. The project is organized by a national domain name registry for the RuNet zone—the Coordination Center for top-level domains RU/РФ.[88].As stated on the project's website, the main goal of Netoscope is to achieve security on the net by combating against malware, spam, phishing, and botnets (networks of zombie computers). The main outcome is a database with websites suspected of targeted activities and websites proved to be involved in such activities. Every internet user has the opportunity to check whether a website is listed in this database. Moreover, users can report that a website is suspicious by pressing a special button on the project's website. After receiving signals, the partners of the project will decide whether or not this website qualifies for inclusion in the database in accordance with criteria known only by the partners.

From 2012 to 2016, more than two million domain names were suspected of unwanted activities and included in the database. In 2016, the number of suspicious domain names was approximately 300 000. The majority of those, 86.3 percent, are websites with malware.[89]

In spring 2014, Yandex started utilizing this database to exclude mentioned websites from its search engine optimization. As a result, such websites appear closer to the end of a search results list.[90]

On 19 April 2016, Roskomnadzor joined Netoscope.[91] The private project thus turned into a form of public-private partnership. An agreement on cooperation was made between Roskomnadzor and the Coordination Center for top-level domain RU/РФ. The agreement represents a very basic, four-page document stating goals of cooperating but lacking any details of it. According to the agreement, Roskomnadzor

---

[87] The website of the project is available at <http://netoscope.ru/en/>.
[88] Coordination Center, 'Report on the Netoscope project 2016' <http://netoscope.ru/upload/iblock/9c3/9c34755b944f30a0187e55a6623a095d.pdf> accessed 4 December 2017.
[89] Coordination Center (n 105).
[90] Director of the Coordination Center, 'Report for 2014' <https://cctld.ru/upload/files/dir_year_report_2014.pdf> accessed 4 December 2017.
[91] Director of the Coordination Center, 'Report for 2016' 12 <https://cctld.ru/upload/files/dir_year_report_2016> accessed 4 December 2017.

collaborates with Netoscope partners in order to prevent the dissemination of unlawful speech on the internet.[92] One of the main targets is to find new ways to restrain the dissemination.[93] To achieve this, the partners can develop and implement any form of cooperation.[94] What forms can be created and how they are regulated, the agreement does not clarify. Yet, the director of the Coordination Center for top-level domain RU/РФ said that websites included on the Blacklist would be added to the Netoscope database, which would allow the partners to react more expeditiously to and combat more efficiently against unlawful content.[95]

This development poses a new puzzle as to how the law could constrain Roskomnadzor's activities within Netoscope. In comparison with the Blacklist regulatory scheme, where Roskomnadzor performs the functions of a state regulatory body and must comply with the Blacklist laws, Roskomnadzor's status in Netoscope is obscure. Although the agreement says generally that the parties must follow all requirements set in the Russian legislation, no clear, overarching legal framework is designated. The yearly report for 2016 issued by the Coordination Center in June 2017 does not clarify the basis and conditions of the cooperation. Thus, the question of whether Roskomnadzor will put in the database only websites included on the Blacklist or non-blacklisted websites as well remains unanswered. It appears that the partner-companies have empowered Roskomnadzor to include a website containing any unwanted speech under the label 'suspicious malware' in the Netoscope database.

From this article's theoretical standpoint, Netoscope is another example of a new-school scheme that does not involve publishers, but allows Roskomnadzor to regulate them indirectly. Balkin explains infrastructure owners' willingness to assist the government in speech regulation in situations where they are not being obliged to do it by law or directly threatened as taking an opportunity 'to ensure an uncomplicated business environment'.[96] This explanation appears to be valid for the case of Russia as well. The private partners of Netoscope may see this cooperation as the inclusion into a group of companies which are close to the Kremlin and therefore receive business preferences.[97]

In comparison with the Blacklist regulatory tool, limited to co-opting internet access providers—owners of the physical layer of the RuNet infrastructure, the Netoscope regulatory scheme is more extensive. The Netoscope scheme is based on cooperating with owners of all three infrastructural layers. In the physical layer,

---

[92] Agreement of 19 April 2016 on cooperation between Roskomnadzor and the Coordination Center for top-level domains RU/РФ, part 1.1 <https://cctld.ru/files/news/rkn_agreement.pdf> accessed 17 December 2017.
[93] ibid 2.1.
[94] ibid 3.2.
[95] Director of the Coordination Center for top-level domain RU/РФ, Andrei Vorobyov, is quoted in 'Roskomnadzor is now taking part in Netoscope project' (*Coordination Center's Official Website* 19 April 2016) <https://cctld.ru/ru/press_center/news/news_detail.php?ID=9692> accessed 17 December 2017.
[96] Balkin (n 14) 2299.
[97] Pallin (n 3) 18.

Roskomnadzor cooperates with Rostelecom, one of the key companies in the internet broadband market with the share of 37 percent.[98] In the application layer, Roskomnadzor cooperates with Mail.Ru Group, the owner of the most popular domestic social media platform VKontakte; with Yandex, the most popular search engine in Russia; and with Group-IB, Kaspersky Lab, BI.ZONE, developers of threat intelligence and antivirus software. In the central protocol layer, Roskomnadzor cooperates with Technical Center 'Internet', a key company in the Russian internet because it operates the Main Registry of RuNet's Domain Name System.[99]

In contrast to the Blacklist regulatory scheme, which application is transparent and prescribed by law, the Netoscope scheme represents an example of cooperation framed under the shade of public-private partner agreements. This endangers free expression because the project provides Roskomnadzor with another solution of how to affect online speech by making unwanted content almost invisible or at least less visible. Roskomnadzor can include in the Netoscope database a website with unwanted content on grounds that are defined by the partners but not by the legislator. Then, Yandex can place this website closer to the end of a search results list. Thereby, the company conceals it from the public, who is usually expected to pay attention only to the top of a list.

Thus, in the Netoscope scheme, the control of the RuNet infrastructure comes to the fore as the primary regulatory tool, while law lags in the background.

There is no clear evidence confirming that Roskomnadzor has used the Netoscope regulatory scheme to affect online speech. Yet both of the websites, www.novayagazeta.ru and www.grani.ru, are already mentioned in the database as 'containing malware at some point in the past.' There is no clarification as to what kind of malware is meant. Yet, it may be supposed that this label applies to anonymizer software which enables an internet user to change his IP address in order to circumvent blocking effective within RuNet. Roskomnadzor was empowered to block such websites in July 2017 by Federal Law № 276-FZ. This rule entered into effect on 1 November 2017.[100] Before this date, an anonymizer-website can appear on the Blacklist only on the ground of a court ruling. By the beginning of 2017, at least twenty courts situated in different parts of Russia[101] issued similarly that anonymizer software must be blocked because it allows internet users to access websites containing illegal extremist speech. These judgments were adopted in a routine manner and almost without investigation. Local prosecutors, after revising whether illegal extremist materials

---

[98] Freedom House, 'Freedom on the Net 2016' Part 'ICT Market' *(Freedom House)* <https://freedomhouse.org/report/freedom-net/2016/russia> accessed 4 December 2017.

[99] The company is owned by the Coordination Center for top-level domains RU/РФ.

[100] Federal Law № 276-FZ of 19 July 2017 On Amendments to Federal Law on Information, Information Technologies and on the Protection of Information.

[101] This practice was adopted, for example, by Kalininskii District Court of Ufa, Republic of Bashkortastan (four judgments adopted on 18 October 2016); Sarapulskii District Court, Udmurtskaia Republic (five judgments adopted on 10 May 2016); Alsheevskii District Court, Republic of Bashkortastan (10 judgments adopted on 21 September 2016); Court of Anapa, Krasnodarskii Krai (ten judgments adopted on 25 February2016).

enlisted by the Ministry of Justice[102] are accessible through using a number of anonymizer-websites, lodged proceedings as a package of suits against these websites. Then, a court issued a package of similar judgments, which ordered Roskomnadzor to include these anonymizer-websites on the Blacklist.

For example, in April 2015, a popular anonymizer, NoBlock, was placed on the Blacklist and blocked following a court judgment.[103] The owners of NoBlock reacted by changing the name to NoBlockMe and moving the content from the blocked website, noblock.ru, to a new website, noblockme.ru.[104] However, in August 2016, noblockme.ru was required to be blocked by a court again.[105] In another example, the most popular Russian anonymizer, Cameleon, was added to the Blacklist following a court judgment in July 2016.[106] It affected more than two million internet users who visited cameleo.ru monthly.[107]

In fact, all three of the above-mentioned anonymizer-websites are contained in the Netoscope database as websites on which malware was detected at some point in the past.[108]

Since the partners of the project can include websites in the database on their own initiative, Roskomnadzor possesses the same power. Consequently, the agency could add a website in the database because of anonymizer software even before it was empowered by Federal Law № 276-FZ of 2017 to add such a website to the Blacklist. Moreover, it appears that Roskomnadzor's power to affect online speech by the Netoscope scheme has never been limited to websites with anonymizer software. The partnership agreement can allow the agency to label as 'malware' any content that Roskomnadzor assesses harmful.

Supposing that Roskomnadzor, because of anonymizer software or because of any other 'malware' of the agency's own choice, changed the status of novayagazeta.ru from containing malware in the past to containing malware at present, what implications for freedom of expression of online media publishers can this bring? The main threat is

---

[102] The special list of websites with illegal extremist content was introduced by Article 13 of Federal Law № 114-FZ On Combating Extremist activities of 2002. The list is formed according to court judgments that certain online materials represent illegal extremist speech and operated the Ministry of Justice. The list is available at <http://minjust.ru/ru/extremist-materials/>

[103] Анапский городской суд Краснодарского края, решение по делу № 2-1303/2015 от 13.04.2015 (*Anapa Prosecutor's Office* [2015] Anapskii Gorodskoi Sud Krasnodarskogo Kraia).

[104] Владимир Зыков, 'Роскомнадзор внёс в чёрный список крупнейший российский анонимайзер' (*Известия*, 26 July 2016) <http://izvestia.ru/news/623836> accessed 4 December 2017.

[105] Кировский районный суд города Саратова Саратовской области, решение по делу № 2-7756/2016 от 08.08.2016 (*Saratov Prosecutor's Office* [2016] Kirovskii Raionnyi Sud goroda Saratov Saratovskoi Oblasti).

[106] I have concluded that the blocking of camaleo.ru (a website on which the anonymizer in question was placed) was done according to one of five judgments adopted by Sarapulskii District Court, Udmurtskaia Republic on 10 May 2016. Which of these judgements is the relevant one is hard to say because all of them are written in a similar manner and in each of them the name of an anonymizer-website to be blocked was removed from the text.

[107] Зыков (n 104).

[108] I did the checking on 6 February 2017. Cameleo.ru is also mentioned as a website disseminating spam at some point in the past.

the utilizing of the database by Yandex to exclude websites from its search engine optimization. It could be expected that the company would put the website closer to the end of the list of search results and, therefore, will effectively prevent it from attracting attention. Thus, the publisher would still publish, but readers would not, with all likelihood, read its publications. Moreover, in contrast to situations like in the cases of *Novaya Gazeta* and *Grani.Ru*, the publisher may never know that its speech has been regulated, but the publisher still has to bear the consequences of regulation. Although an online newspaper will not be closed as a source of information, as in the case of applying the Blacklist tool, the publisher's ability to forward its content to readers will be negatively affected. In these circumstances, it becomes especially important who assesses content as unlawful. In the case of *Novaya Gazeta*, the conclusion on unlawful character of the published content was made by an independent expert. In the case of *Grani.Ru*, a similar conclusion was made by an expert, although unlikely independent due to his post at the Prosecutor General's Office. In contrast to these cases, in the case of Netoscope, such a conclusion can be made by Roskomnadzor itself. Thus, online media publishers may more easily become victims of the agency's abuse. In spite of these drastic implications for publishers' freedom of expression, nontransparent mechanisms of regulation within Netoscope leave unclear the issue of how publishers can challenge them. Therefore, this scheme is potentially more dangerous for freedom of expression than the Blacklist scheme, because publishers are left unprotected.

Applying the Netoscope regulatory scheme can lead to drastic implications not only for publishers' free expression, but also for RuNet users' right to seek and receive information. In this case, content is not blocked but placed far from RuNet users' eyes by Yandex. Users are not aware of this. They only see the result formed with help of technological tools working invisibly. Yandex may argue that a private company should not inform its consumers as to what algorithms it uses to create search results lists. Yet, since Roskomnadzor joined the project and received power to affect search results, this argument should be re-evaluated, if not rejected.

CONCLUSION

The case study analysis proves the main argument of this article that the Russian government has changed regulatory practices by turning from direct, old-school speech regulation to indirect, new-school regulation. Indeed, the case of Novaya Gazeta and especially the case of Netoscope show that the government realized this indirect regulation by co-opting owners of the RuNet infrastructure.

The exposition of ideas expressed in the previous internet infrastructure-centric research in the new, Russian context enables this article to offer three theoretical contributions. First, the article has demonstrated that the internet infrastructure-centric framework can apply to study online speech regulation across multiple jurisdictions. Second, the case of Netoscope shows that the idea of cooperative regulation should be expanded from regulation by cooperating with a certain owner of one infrastructural layer to regulation by multi-partnership cooperating among owners of all infrastructural

layers. Third, the case of Netoscope shows that the main criticism to the theory of new school of speech regulation is invalid in the Russian context. This criticism emphasizes that a new state power received through co-opting/cooperating with internet infrastructure owners can be counteracted by online speech platform providers, for example Google or Facebook, who have started to report governments' requests to remove content.[109] Even if such reports include all requests received and provide with true information, it is unlikely that this counteraction measure can be efficient in Russia. On the Russian internet market, the popularity of Google and Facebook is less than of Yandex and VKontakte, domestic providers. At the same time, both Yandex and VKontakte, the latter through its owner Mail.Ru Group, cooperate with the Russian government in the Netoscope project. Therefore, even if these providers reveal the Russian government's requests to remove speech, their information can hardly be reliable.

In these conditions, insights introduced by the internet infrastructure-centric theories appear extraordinarily powerful and pessimistic for the freedom of expression in RuNet. The study shows that both mass media's right to freedom of expression and users' right to seek and receive information have been endangered by the move to regulating in assistance with RuNet infrastructure owners. Yet, although the internet infrastructure-centric framework serves as an efficient intellectual tool to reveal new threats to online free expression, this framework appears underdeveloped from a normative perspective. Therefore, solutions on how to safeguard online free expression from internet infrastructure-based censorship might be suggested by other theories. Moreover, these solutions might be found by conducting empirical research. For instance, it should be explored how Russian media professionals have reacted to the regulation by co-opted infrastructure owners.

[109] Nunziato (n 35).