Volume 9 | Autumn 2020

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence

ISSN: 2500-9486
DOI: 10.30966/2018.RIGA.9

SELECTIVE LAW ENFORCEMENT ON THE RUNET AS A TOOL OF STRATEGIC COMMUNICATIONS

Milàn Czerny

Abstract

The Russian government's policy regarding the internet is often assessed in binary terms. Writers on the topic suppose that the authorities are either on the path to fully controlling the Russian internet (RuNet), or that they are unable to do so, thus suggesting that the technology poses a serious threat to the Kremlin. However, taking into account Russia's legal culture and its widespread practice of 'selective law enforcement' allows us to gain a more nuanced picture of the Russian authorities' strategic use of the online sphere. This article examines the selective application of internet regulations as a tool of strategic communications directed at different online audiences. We show that selective enforcement of the law allows authorities to delineate the boundaries of permissible political speech, shaping citizens' online behaviour while avoiding the potential backlash that could arise from imposing large-scale restrictions on internet users in general.

Keywords—*strategic communications, strategic communication, Russia, RuNet, information control, internet regulations, Russian law*

About the Author:

Milàn Czerny is an MPhil student in Russian and East European Studies at St Antony's College, University of Oxford. He holds a BA degree from the department of War Studies, King's College London.

Introduction

An analysis of the literature dealing with Russia's information legislation reveals that the Kremlin's control over the internet through legal regulations is generally assessed from two different perspectives. On the one hand, certain analysts have raised concerns that Russia's adoption of numerous internet regulations over the years will inevitably lead the Kremlin to follow in China's footsteps by engaging in large-scale filtering of content, blocking dissenting voices, limiting access to Western social media platforms, and isolating the Russian internet (RuNet) from the global internet. The Washington-based analyst Nathalie Duffy characterises Russia's establishment of a legal framework to regulate RuNet as 'an initiative to create a domestic equivalent to the "Great Firewall of China" around web content'.[1] Similarly, some Western scholars believe that Russia's legal regulations would enable the government to detach 'the Russian Internet from the global infrastructure' and to empower 'the Kremlin to cut off the country's Internet from the rest of the world'.[2] By contrast, others deem Russia's imposition of legal regulations to be merely 'futile efforts': 'the government has not been able to establish absolute control over Russia's information space' nor 'completely silence independent voices contradicting the Kremlin's official narrative'.[3] Maria Kravchenko, a researcher at the Russian non-governmental organisation SOVA, stresses that the Russian government has failed to 'stop distribution of information' and to filter content as users can access material deemed illegal through 'multiple other channels'.[4]

While these contradictory views paint opposing pictures of the government's ability to control RuNet, both perspectives presuppose that the Russian government is seeking to implement regulations systematically to block internet access for all dissenting voices. This assumption obscures the reality that 'the Russian legal realm is much more law in action than law on paper'.[5] This is

1 Natalie Duffy, 'Internet Freedom in Vladimir Putin's Russia: The Noose Tightens', *American Enterprise Institute*, 12 January 2015, p. 30.
2 Julien Nocetti, 'Russia's "Dictatorship-of-the-law" Approach to Internet Policy', *Internet Policy* Review, 4(4), (2015), p. 2; Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, 'The Digital Dictators. How Technology Strengthens Autocracy', *Foreign Affairs,* 6 February 2020; Mari Ristolainen, 'Should "RuNet 2020" Be Taken Seriously? Contradictory Views About Cybersecurity Between Russia and the West', *Journal of Information Warfare*, 16(4), (2017): 113–13.
3 Natalya Kovaleva, 'Russian Information Space, Russian Scholarship, and Kremlin Controls', *Defence Strategic Communications*, 4(1), (2018), p. 158.
4 SOVA Center for Information and Analysis is a Moscow based non-profit organisation that deals with issues related to xenophobia in Russia, relations between the churches and secular society, and government misuse of counter-extremism measures; Maria Kravchenko, 'Russian Anti-Extremism Legislation and Internet Censorship', *The Soviet and Post-Soviet* Review, 46(2), (2019), p. 164.
5 Aryna Dzmitryieva, 'How the Law Really Works: The New Sociology of Law in Russia', *Economic Sociology—The European Electronic* Newsletter, 13(2), (2012), p. 18.

to say that, in Russia, rather than laws being implemented consistently and universally, they are selectively enforced against a limited number of individuals or organisations for the benefit of extra-legal interests.[6] Selective application of the law allows those in power to single out a target that can be made into an example. This not only contains the immediate threat (if there is one) but sends a clear message to sympathisers that unless they keep their own online behaviour in check they risk experiencing similar treatment. This practice helps the regime delineate the informal rules of political conduct in Russian society without resorting to overt, large-scale repression. Beyond a limited number of authors who have raised questions about Russia's selective enforcement of its internet regulations, this practice has received scant attention in the literature.[7] This article seeks to provide a richer interpretation of the intent of Russian internet regulations by examining when they are implemented, how they are enforced, against whom, and how this helps the Russian government.

The sources available to answer these questions are the legislation itself and court decisions accessible in public databases. It also relies on reports produced by the independent Russian NGO Agora, a widely recognised organisation dealing with Russian legal issues, which tracks the enforcement of legislation.

Selective enforcement of internet regulations in Russia constitutes a fundamental tool of Strategic Communications for the Kremlin. Strategic Communications can be defined as 'a holistic approach to communication based on values and interests that encompasses everything an actor does to achieve objectives in a contested environment'.[8] Russian authorities exert control over online information to ensure domestic stability and the regime's legitimacy. We will analyse the selective application of legislation as a tool of strategic communications directed at three different audiences active on RuNet: internet intermediaries,[9] non-systemic opposition voices, and common citizens.[10]

6 Håvard Bækken, *Law and Power in Russia: Making Sense of Quasi-Legal Practices* (New York: Routledge, 2018); Vladimir Gel'man, 'The Politics of Fear: How the Russian Regime Confronts Its Opponents', *Russian Politics & Law*, 53 (5/6), (2015): 6–26; Yelina Kvurt, 'Selective Prosecution in Russia-Myth or Reality', *Cardozo Journal of International and Comparative* Law, 15(1), (2007): 127–68.

7Andrei Soldatov, 'The Taming of the Internet', *Russian Social Science Review*, 58(1), (2017): 39–59; Jaclyn A. Kerr, 'The Russian Model of Internet Control and Its Significance', *Lawrence Livermore National Lab*, (2018): 1–7.

8 Neville Bolt and Leonie Haiden, NATO Strategic Communications Terminology (Riga: NATO Strategic Communications Centre of Excellence, 2019) p. 46.

9 Internet intermediaries are service providers that enable people to use the internet by giving access to, hosting, transmitting, and indexing content, products, and services. This includes search engines and social media platforms.

10 The term 'non-systemic opposition' in Russia refers to activists who seek a radical change of the regime and engage in political protests while holding no official office. By 'common citizens' I mean individuals who might take part in certain protests around local issues or declining living conditions but are not public figures; they do not engage in more organised political actions or seek to hold an official role.

The evolution of Russia's regulation of RuNet

In the 1990s and early 2000s, it was widely believed that the internet was too dynamic a technology to be controlled, and that trying to do so would be like 'trying to nail jello to the wall', in the words of America's former President Bill Clinton.[11] However, in the years that followed, states began to assert their power over the online-sphere through various means. China managed to build a resilient centralised network to ensure control over communication; France was one of the first countries to impose legal regulations in the internet realm (see the *Yahoo Case* of 2000).[12] Nowadays, virtually all states have asserted some degree of control over the activities of internet users located in their territories. The European Union (EU) implemented the General Data Protection Regulation (GDPR) in 2018 to regulate users' data and the privacy of European internet users. The United States—once a fierce proponent of internet freedom—is trying to assert its control over foreign platforms such as TikTok by threatening to ban them or impose a change in ownership.[13]

Russia represents a specific case in this worldwide trend of growing control over the digital arena. To grasp how RuNet is shaped by the authorities one must look at how legal regulations are enforced in practice rather than at the 'law on paper'.[14] To understand this pattern and the driving forces behind the adoption of regulations in Russia, it is necessary to follow the evolution of the government's approach to the internet.

Russia was not among the first to impose legal regulations on the internet. The initial lack of early control led to the establishment of multiple connections between RuNet and the global internet; users became accustomed to accessing foreign online services. In the early 2000s, rather than trying to ensure control over the online space, the Russian state supported the development of IT businesses and the country's greater integration into the global digital economy by constructing cross-border fibre-optic cables and encouraging internet use.[15] The growing number of citizens who had access to the internet, enjoyed a large degree of online freedom. Russia online was characterised by its dynamic

11 Bill Clinton, 'Clinton's Words on China: Trade Is the Smart Thing', remarks at the Paul H. Nitze School of Advanced International Studies, 8 March 2000.
12 Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (New York: Oxford University Press, 2006): 1–10.
13 Justin Sherman, 'Trump's Un-American Failure to Protect Internet Freedom', *Wired,* 22 October 2020.
14 Dzmitryieva, 'How the Law Really Works'.
15 Marcus Alexander, 'The Internet and Democratization: The Development of Russian Internet Policy', *Demokratizatsiya*, 12(4), (2004): 607–27.

blogosphere, online political debates, cultural discussions, and communications with Russian-speaking bloggers in Ukraine, Armenia, and Israel.[16] Following the *Kursk* submarine disaster and the Beslan tragedy in the early 2000s, the Kremlin increased its control over all information channels, but RuNet largely remained a 'networked public sphere' and 'an alternative to broadcast and print media'.[17]

However, toward the end of the decade, the government began to characterise the internet as an arena of 'information war' waged by the West that posed an existential threat to Russian society and to the Putin regime.[18] To combat the use of information 'to influence the public psyche and destabilise a country from the inside', the Russian government laid the foundations for increased regulation of the internet. In December 2008, after weaponising the internet during the Georgian war, the Kremlin created ROSKOMNADZOR (the Federal Service for Supervision of Communications, Information Technology, and Mass Media) to monitor and implement Russian legislation in the field of communications and information technologies.[19] Initially, this organisation remained passive, as President Dmitry Medvedev, nicknamed the 'blogger-in-chief', promoted the use of social networks and the development of the digital economy.[20] However, once Medvedev's term in office was over, there was a clearly discernible shift in government regulations regarding the internet.

Putin's return to the presidency in 2012 led to large-scale protests in Moscow's Bolotnaya Square. Tens of thousands of users relied on Facebook pages created by leaders of the non-systemic opposition for mobilisation and coordination.[21] Social media were also considered central in the so-called Arab Springs taking place around the same time.[22]

16 Natalja Konradova, Henrike Schmidt, and Katy Teubener (eds), *Control + Shift: Public and Private Usages of the Russian Internet* (Norderstedt: Books on Demand, 2006).
17 Masha Lipman, 'Constrained or Irrelevant: The Media in Putin's Russia', *Current History*, 104(684), (2005): 319–24; Bruce Etling, Karina Alexanyan, John Kelly, Robert Faris, John Palfrey, and Urs Gasser, 'Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization', *Berkman Center Research Publication*, (2010), p. 33; Gregory Asmolov and Polina Kolozaridi, 'The Imaginaries of RuNet: The Change of the Elites and the Construction of Online Space', *Russian Politics,* 2(1), (2017), p. 18.
18 Ofer Fridman, 'The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse', *Defence Strategic Communications*, 2(2), (2017): 61–86.
19 Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War', *Security Dialogue*, 43(1), (2012): 3–24; Russian Federation, Presidential Administration, '*On Public Administration Issues in the Field of Communication, Communication Technologies and Mass Media*', Decree № 1715, Moscow, 3 December 2008.
20 Daphne Skillen, *Freedom of Speech in Russia: Politics and Media from Gorbachev to Putin* (London: Routledge, 2017), p. 50.
21 Asmolov and Kolozaridi, 'The Imaginaries of RuNet'.
22 Ibid.

Protests inside and outside Russia marked a turning point in the development of the government's policies towards the internet.[23] Indeed, social movements relying on social media and support from the United States through Secretary of State Hillary Clinton's promotion of the Internet Freedom Agenda, heightened the politicisation of online information as a fundamental threat to the stability of Russian society and the Russian government.[24] This politicisation, according to Ofer Fridman, was aimed at 'preparing the ground for corresponding legislation intended to minimise the perceived threat of external influence on Russian society'.[25]

In the summer of 2012, Konstantin Malofeev, a proponent of Russia's 'anti-Westernism', and lawmaker Elena Mizulina promoted Federal Law № 139-FZ.[26] This piece of legislation called for the creation of a registry of websites containing materials deemed harmful to children's 'health and development'. ROSKOMNADZOR currently requires Internet Service Providers (ISPs) to permanently block access to sites registered on this 'blacklist'.[27] This law was Russia's first step towards greater regulation. As noted by internet governance scholar Milton Mueller: 'emotional appeals to the children have deliberately been exploited as the entering wedge for a broader reassertion of state control over internet content'.[28] Indeed, in December 2013, Federal Law № FZ-398 was adopted to expand the blacklist.[29] It permitted material deemed extremist or threatening to the public order, such as calls for unauthorised protests, to be included in the registry. The law granted the authorities the power to block such content without a court order; now only a request to ROSKOMNADZOR from the Prosecutor-General's office is sufficient to blacklist websites identified as dangerous under the new definition.

The beginning of the war in Ukraine in 2014 and heightened tensions with the West further reinforced the government's politicisation of online information

23 Anna Klyueva, 'Taming Online Political Engagement in Russia: Disempowered Publics, Empowered State and Challenges of the Fully Functioning Society', *International Journal of Communication*, 10, (2016): 4661–80.
24 Hillary Clinton, 'Conference on Internet Freedom', speech at the Hague, 8 December 2011.
25 Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicization* (New York: Oxford University Press, 2018), p. 149.
26 The State Duma, On the Protection of Children from Information Harmful to Their Health and Development and Other Legislative Acts of the Russian Federation, Federal Law № 139-FZ, Moscow, 28 July 2012.
27 An ISP is a company that provides internet access to users by routing internet traffic, resolving domain names, and maintaining the network infrastructure.
28 Milton Mueller, *Networks and states: The global politics of Internet governance* (MIT Press, 2010), p. 190.
29 The State Duma, *On Information, Information Technologies and Protection of Information*, Federal Law № 398-FZ On Amendments to the Federal Law, Moscow, 28 December 2013.

as a major threat to social and political stability.[30] This was reflected in the 2015 National Security Strategy and the 2016 Information Security Doctrine, both of which stressed the risks posed by online information to Russia's 'sovereignty, political and social stability', and 'constitutional order', claiming that some countries were seeking 'to achieve their geopolitical objectives by using information and communication technologies'.[31] Further regulations were thus adopted to respond to this perceived threat of external influence. In 2019, Vladimir Putin signed Federal Law № 90-FZ, which clarifies how to cut RuNet off from the global Internet in the event of an external threat, Federal Law № 31-FZ, which opposes the dissemination of unreliable information, and Federal Law № 30-FZ, which prevents the spread of material deemed disrespectful to the State and to bodies exercising state power.[32]

Thus, while Russia adopted a largely hands-off approach to RuNet in the 2000s, in the 2010s the government increasingly began to regard the unregulated online space as a source of vulnerability that Western powers could exploit to destabilise Russian society. It was this shift that has led many to believe that Russia seeks to 'gain complete control over the Russian population's access to, and activity on, the Internet'.[33] However, because of the connections established early on between RuNet and the global Internet, Russia's technical capacity to isolate has been questioned.[34] But focusing enquiry solely on Russia's technical ability (or lack thereof) to impose large-scale censorship or disconnect RuNet from the global network risks masking the fact that officials have consistently avoided taking such actions.[35] It is highly likely that blocking popular internet platforms, isolating RuNet from the global Internet, and unduly restricting content would

30 Gregory Asmolov, 'Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation', *Internet Policy Observatory*, (2015): p. 9.
31 Russian Federation, *The Information Security Doctrine of the Russian Federation*, Moscow, 5 December 2016; Russian Federation, Presidential Administration, *On the Russian Federation National Security Strategy*, Decree № 683, Moscow, 31 December 2015.
32 The State Duma, *On Amendments to the Federal law "On Communications" and the Federal law "On Information, Information Technologies and Information Protection*", Federal Law № 90-FZ, Moscow, 1 May 2019; State Duma, *On Amendments to Article 15-3 of the Federal Statute on Information, Information Technologies and Protection of Information*, Federal Law № 31-FZ, Moscow, 18 March 2019; State Duma, *On Amending the Federal Act "On Information, Information Technologies, and Protection of Information*, Federal Law № 30-FZ, 18 March 2019.
33 Duffy, 'Internet Freedom', p. 2.
34 Ksenia Ermoshina and Francesca Musiani, 'Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era', *Media and Communication*, 5(1), (2017): 42–53.
35 Dmitry Medvedev, 'Gosudarstvo i internet: poyavilis' novyye instituty'[The State and the Internet: New Institutions Have Appeared'], 18 April 2012; Dmitry Medvedev, 'Razgovor s Dmitriyem Medvedevym'[Discussion with Dmitry Medvedev], Moscow, 5 December 2019; Vladimir Putin, 'Zasedaniye Soveta Bezopasnosti' [Security Council Meeting], Moscow, 1 October 2014; Vladimir Putin, 'Direct Line with Vladimir Putin', Moscow, 20 June 2019.

undermine the legitimacy of the government.[36] Consequently, Russia has sought to reach a balance between controlling RuNet and limiting overt, widespread restrictions on internet use.

The selective enforcement of Internet regulations helps the government achieve this balance. The authorities can communicate the boundaries of tolerated behaviour to various audiences active on RuNet by targeting a limited number of users to serve as examples in order to shape online behaviour. This scheme is in line with the broader mechanisms of control practiced in Russia long before the advent of the internet.[37] As Sarah Oates argues, it is necessary to analyse the control of online communication in Russia within the context of its national political system and cultural patterns.[38] Therefore, our investigation into Russia's 'selective enforcement' of internet regulations examines the logic of such a practice and the ways it is enabled by Russia's 'legal culture'.

Selective law enforcement in Russia

Selectivity in applying the law against political or business opponents is an infamous phenomenon in Russia.[39] However, it is only recently that the practice of 'selective law enforcement' has been conceptualised in depth. Håvard Bækken defines selective law enforcement as a 'mechanism of repression aimed at enforcing informal rules of political conduct through selective legal acts'.[40] He emphasises that the practice is marked by the penetration of informal, unwritten interests in the legal realm to suspend the application of the law or to employ it instrumentally. The law is not applied universally according to the letter of official legal documents and procedures. The selection of persons whom should be indicted is negotiated outside public view based on informal power structures (the judgement of officials as to who may actually pose a threat or obstacle to their exercise of power) to advance extra-legal interests and to communicate through legal means which behaviours will not be tolerated. In states adhering

36 Asmolov, 'Welcoming the Dragon'; 'Julie Fedor and Rolf Fredheim, '"We Need More Clips About Putin, and Lots of Them:" Russia's State-commissioned Online Visual Culture', *Nationalities Papers*, 45(2), (2017): 161–81.
37 Tatiana Borisova and Jane Burbank, 'Russia's Legal Trajectories', *Kritika: Explorations in Russian and Eurasian History*, 19(3), (2018): p. 469–508; Vladimir Gel'man, 'The Unrule of Law in the Making: The Politics of Informal Institution Building in Russia', *Europe-Asia Studies*, 56(7), (2004): 1021–40; Ella Paneyakh, 'Neformal'nyye instituty i ispol'zovaniye formal'nykh pravil: zakon deistvuyushchii vs zakon primenyayemyi' [Informal institutions and the use of formal rules: acting law vs law in action], *Politicheskaya nauka*, 1, (2003): 33–52.
38 Sarah Oates, *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere* (Oxford: Oxford University Press, 2013).
39 Alena V. Ledeneva, *Can Russia Modernise?: Sistema, Power Networks and Informal Governance* (Cambridge: Cambridge University Press, 2013); Richard Sakwa, *The Crisis of Russian Democracy: The Dual State, Factionalism, and the Medvedev Succession* (Cambridge: Cambridge University Press, 2011).
40 Bækken, *Law and Power in Russia*, p. 2.

to the rule of law, law enforcement is commonly understood as a means of communicating the idea that legal rules apply to all members of a society, while states that practice selective law enforcement blur the boundaries between formal and informal sanctions; the application of the law is based on legally relevant material but extra-legal interests guide the selection of who is singled out for sanction. For instance, Bækken draws attention to electoral legislation in Russia: registration procedures can be selectively enforced to deny participation to opposition candidates based on minor technical violations, while politicians 'leaning on patronal structures and informal support from within the system' do not face similar legal scrutiny.[41] By means of these patterns of enforcement the authorities communicate unwritten rules to the wider public, as citizens easily grasp the double standard and think twice before standing openly against those in power.

Selective law enforcement thus constitutes a powerful tool of communication for those in power. It helps draw boundaries between those within the *systema*, the elites who are allowed to bend or bypass laws, and those on the outside, who must keep their heads down or risk facing the consequences.[42] In the words of Russian political scientist Vladimir Gel'man, the Kremlin has developed a 'politics of fear' in which selective repression plays a 'signalling role, demonstrating to the elites and to ordinary citizens that public displays of disloyalty carry the risk of great losses'.[43] Laws are applied only in a limited number of cases, yet it is precisely the selective enforcement mechanism that communicates to all bystanders that they must respect the unwritten 'rules of the games' to avoid being noticed by the authorities and potentially face legal sanctions. The example of the electoral practices mentioned above shows how the 'rules of the game' encourage citizens to accept without protestation that, while in theory anyone can be an electoral candidate, in practice only individuals close to the regime or at least who do not pose a direct threat to its rule will be allowed to stand for election in most cases. Hence selective law enforcement is practiced only when deemed necessary and public knowledge of the practice continues to shape the political and social landscape long after an example case has been enforced.

It must be emphasised that the functioning logic of selective law enforcement depends on Russia's 'legal culture'—the 'ideas, values, attitudes, and opinions

41 Ibid., p. 138.
42 Ledeneva, *Can Russia Modernise?*.
43 Vladimir Gel'man, 'The Politics of Fear', p. 9.

people in some society [sic] hold with regard to law and the legal system'.[44] Russia's legal culture and the values it embodies form the basis for the selective application of the law to act as a means of strategic communications as we shall see in the examples below.

Russia's leaders understand the law as a fundamental asset of sovereignty that can be manipulated to achieve various objectives, such as limiting political opposition or ensuring control over the economic sphere, rather than as a tool for enforcing healthy constraints.[45] As identified by scholars Tatiana Borisova and Jane Burbank, Russia's legal tradition is marked by 'the primacy of the sovereign as the source of the law' and the instrumentalist approach to the law as a means to advance and protect the interests of Russian elites.[46] Throughout Russia's history, rulers weaponised legislation in cases of 'apparent challenges to principles of Russian sovereignty and rulers who embody it'.[47] Successive Russian leaders have relied on the law to advance their own particular interests, to strengthen and protect their personal power and that of the state, and to avoid social and economic instability. They have employed legislation as a strategic tool of communication to signal and enforce informal rules of political conduct to targeted audiences.

This approach to the law emerged in the Russian Empire and persisted throughout the Soviet Era. Indeed, while important legal reforms under Tsar Alexander II in 1864 introduced principles of equality of all parties under the law, in practice the 'ultimate authority to grant, make, and change law' remained in the hands of rulers.[48] Similarly, following the 1917 revolution, Lenin characterised the law as a weapon and the courts as organs of power.[49] Under Stalin, criminal justice became a crucial tool for instilling terror through the selective prosecution of a very large number of individuals from all walks of life. The 'Moscow Trials', held to prosecute 'Trotskyist-Zinovievist conspirators' between 1936 and 1938, remain the iconic symbol of Soviet selective persecution. A large number of similar but lesser-known show trials took place throughout the 'republics, regions, and even districts of the USSR' so that Stalin could demonstrate his control to all.[50] While Krushchev put an end to the 'crimes of the Stalin Era'

44 Lawrence M. Friedman, 'Is There a Modern Legal Culture?', *Ratio Juris*, 7(2), (1994): p. 118.
45 Anton Oleinik, 'Existing and Potential Constraints Limiting State Servants' Opportunism: The Russian Case', *Journal of Communist Studies and Transition Politics*, 24(1), (2008): p. 184.
46 Borisova and Burbank, 'Russia's Legal Trajectories', p. 501.
47 Ibid., p. 480.
48 Borisova and Burbank, 'Russia's Legal Trajectories', p. 477.
49 Jane Burbank, 'Lenin and the Law in Revolutionary Russia', *Slavic Review*, 54(1), (1995): 23–44.
50 Peter H. Solomon, *Soviet Criminal Justice Under Stalin* (Cambridge: Cambridge University Press, 1996), p. 239.

and adopted the People's Law of 1961, which confirmed that 'all are equal under the law', nevertheless those in power 'used legal actors to cover up their criminal acts, protect friends, or selectively attack rivals'. [51] Under Brezhnev (1964–82), this trend was further reinforced: he left greater room for 'elites' contempt for the constraints of legal rules', while selectively targeting dissenters through high-visibility political trials in his first years in power.[52] The trials of writers Andrei Siniavsky and Yuli Daniel in 1966, and of Alexander Ginzburg and Yuri Galanskov in 1968 signalled the dangers faced by anyone engaged in the publication and dissemination of *samizdat* [dissenting, self-published literature] and *tamizdat* [works published abroad]. In Gel'man's words, such 'surgical repressions of dissenters sent a clear signal to other Soviet citizens: unauthorized public and political activism would cost them dearly'.[53]

The historical trajectory Russia's legal culture has thus set the basis for selective law enforcement under Putin. The turmoil that followed the fall of the Soviet Union under Boris Yeltsin's presidency provided grounds for Putin to push forward legal reforms and the centralisation of power. This brought much-needed stability to the country and improved the provision of justice in mundane or non-political cases.[54] However, the centralisation of justice and changes in law-making also created new opportunities for selective prosecution and further entrenched the seamy side of Russia's legal culture. As William Parlett argues, Putin's legal reforms provided him with a 'a tool for ensuring that he could punish those who did not comply with his informal rules of the game through selective prosecution'.[55] Thus, despite Putin's commitment that law would be restored and imposed according to universalist principles, selective law enforcement remained central to Russia's governance.

This was most notably exemplified in the high-profile prosecution of Mikhail Khodorkovsky. This oligarch likely breached certain laws by relying on tax avoidance schemes and other dubious means to build his wealth in the 1990s, a period characterised by chaos and unaccountable authority in Russia.[56]

51 Bækken, *Law and Power in Russia*, p. 46.
52 Robert Sharlet, 'Soviet Legal Reform in Historical Context', *Columbia Journal of Transnational Law*, 28(1), (1990): p. 6.
53 Gel'man, 'The Politics of Fear', p. 14.
54 Kathryn Hendley, *Everyday Law in Russia* (New York: Cornell University Press, 2017).
55 William Partlett, 'Putin's Artful Jurisprudence', *The National Interest* № 123, (January/February 2013): p. 36.
56 Richard Sakwa, 'Putin and the Oligarchs', *New Political Economy*, *13*(2), (2008): p. 187.

However, it is widely believed that he was singled out because of his political ambitions, as similar individuals close to the Kremlin did not invite the same legal scrutiny.[57]

Putin relied strategically on legal means to shape and communicate the new 'rules of the game' to oligarchs who became aware that they, like Khodorkovsky, would face sanctions unless they stayed out of politics.[58] Hence, during Putin's first term, 'as in Soviet days, the law was used instrumentally';[59] as Richard Sakwa writes, 'in attacking a few oligarchs he was disciplining the rest'.[60] The Khodorkovsky case demonstrates selective law enforcement logic and reflects enduring trends in Russia's legal culture.

While selectivity in implementing the law has been discussed in terms of Russia's election procedures, tax schemes, and the regulation of NGOs, this practice has been overlooked in our understanding of the Russian government's control over RuNet.[61] Taking into consideration Russia's legal culture and widespread practice of selective law enforcement offers a more nuanced understanding of the Kremlin's strategy of control than the 'traditional' binary assessment of Russia's internet legislation. The following section will show that the Russian government has managed to adapt existing legal patterns to the online sphere.

The selective implementation of internet regulations

We can consider the selective enforcement of internet regulations in Russia and its usefulness as a tool of strategic communications as it relates to three different targeted audiences: internet intermediaries, non-systemic opposition, and common citizens.

Internet Intermediaries as a Targeted Audience

Internet intermediaries, i.e. search engines, content hosts, and social media platforms, are a focal point of control for governments, as these actors manage internet users' communications and have access to their data.[62] The

57 Jonathan D. Greenberg, 'The Kremlin's Eye: The 21st Century Prokuratura in the Russian Authoritarian Tradition', *Stanford Journal of International Law*, 45(1), (2009): 1–50.
58 Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (London: William Collins, 2020), p. 200.
59 Richard Sakwa, *Putin: Russia's choice.* (New York: Routledge, 2007), p. 150.
60 Sakwa, 'Putin and the Oligarchs', p. 189.
61 Håvard Bækken, 'Selections Before Elections: Double Standards in Implementing Election Registration Procedures in Russia?', *Communist and Post-Communist Studies*, 48(1), (2015): 61–70; Stephen Fortescue, *Russia's Oil Barons and Metal Magnates: Oligarchs and the State in Transition* (New York: Palgrave Macmillan, 2006), p. 162; Maria Tysiachniouk, Svetlana Tulaeva, and Laura A. Henry, 'Civil Society Under the Law 'On Foreign Agents': NGO Strategies and Network Transformation', *Europe-Asia Studies*, 70(4), (2018): 615–37.
62 Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

Kremlin's decision to forbid access to the professional social networking website LinkedIn based on Federal Law № 242-FZ[63] exemplifies the practice of selective implementation. This piece of legislation requires internet intermediaries that process and collect the personal data of Russian citizens to store this information on servers physically located in the territory of the Russian Federation. Failure to comply can lead to the imposition of a fine and the decision to block services. The law introduced a new blacklist, the *Registry of Violators of the Privacy of Individual Personal Information*, which allows ROSKOMNADZOR, following a court order, to block access to websites that process personal data in violation of Russia's data protection laws. The Kremlin adopted this law in 2014 in response to public outrage provoked by Edward Snowden's revelation concerning the existence of a global surveillance programme conducted by the US National Security Agency (NSA). Following the revelations, Sergey Zheleznak, a Russian MP, underlined the need to 'seriously protect both the information of our citizens and the information of our country' by requiring Western internet intermediaries that collect and analyse information on Russian users to relocate the servers that store this information onto Russian soil.[64] According to Zheleznak, this would allow Russia to protect its 'digital sovereignty' and prevent US government surveillance.[65]

Despite the arguments of Russian officials, this measure does nothing to increase users' privacy. Legal scholars Anupam Chander and Uyên P. Lê stress that data localisation laws may, in fact, ease the logistical burdens of foreign intelligence companies by creating a 'honey pot' as users' information is centralised in one country.[66] The Snowden case was considered to be merely an excuse for Russia to increase its control over data and its surveillance potential.[67] By moving their servers onto Russian soil, Western platforms would be more vulnerable to censorship as they would have to follow Russian legislation to continue operating.[68] The adoption of the law also raised concerns that it would lead to the 'end of Facebook' or the 'end of Twitter' for Russian users, as the government obtained

63 The State Duma, *On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks*, Federal Law № 242-FZ, Moscow, 21 July 2014.
64 Sergey Zheleznak, 'My dolzhny obespechit' «tsifrovoy suverenitet» nashey strany' [We must ensure the 'digital sovereignty' of our country], *Ekonomika i Zhizn'*, 19 June 2013.
65 Ibid.
66 Anupam Chander and Uyên P. Lê, 'Data Nationalism', *Emory Law Journal*, 64(3), (2014): 677–740.
67 Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: Public Affairs, 2015).
68 Tatevik Sargsyan, 'Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security', *International Journal of Communication*, 10, (2016): 2221–37.

a legal tool to shut down foreign social media by including them in a registry.[69]

Russian internet activist Ivan Begtin does not see Federal Law № 242-FZ as a protection but as 'yet another tool for controlling the Internet', which reveals that Russia is 'moving very fast down the Chinese path'.[70] Following the adoption of the law, investigative journalist Andrei Soldatov warned that Russia may succeed in 'splintering the web' and 'breaking off from the global internet'.[71]

However, five years after adopting the law, these bleak predictions were not realised, as the law has been only selectively enforced. It went into force in September 2015 and ROSKOMNADZOR began to verify the compliance of Western internet intermediaries in 2016. In August 2016, the Taganskiy District Court of Moscow ordered ROSKOMNADZOR to include only one site, the professional social-networking platform LinkedIn, in the *Registry of Violators of the Privacy of Individual Personal Information* and to take measures to limit access to the platform, as it had failed to relocate its servers.[72] In November 2016, Russian users could no longer access the platform. By 2020, however, only a few Western companies had decided to comply with the law, and, aside from LinkedIn, ROSKOMNADZOR has blocked none of the other internet intermediaries that have yet to respect the legislation. Three years after LinkedIn was blocked, the social media platforms Twitter and Facebook were fined 3 000 RUB (42 USD) each.[73] They were then granted an additional nine months to transfer the data of Russian citizens onto servers within the territory of the Russian Federation. It was only later that ROSKOMNADZOR began administrative proceedings to impose a 4 million RUB (55,000 USD) fine against each of the two social networks.[74] The imposition of such small penalties, compared to the costs of complying with the law and to the radical step taken against LinkedIn, is unlikely to provoke any changes in Facebook or Twitter's data localisation. Similarly, Google has yet to store Russian users' data on servers inside Russia, but it has not faced any sanctions for its non-compliance with the legal requirements.[75] Thus, as summarised by Leonid Volkov,

69 Andrey Tselikov, 'The Tightening Web of Russian Internet Regulation', *Berkman Center Research Publication*, № 2014/15, (2014): 1–20.
70 Maria Makutina, 'Tsifrovoy suverenitet' [Digital sovereignty], *Gazeta.ru*, 19 June 2013.
71 Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State', *World Policy Journal,* 2 March 2015.
72 Russian Federation, Taganskiy District Court, 'Case decision № 02-3491/2016', Moscow, 4 August 2016.
73 Russian Federation, Taganskiy District Court, 'Case decision № 12-0513/2019', Moscow, 8 May 2019.
74 Russian Federation, Taganskiy District Court, 'Case decision № 12-0449/2020', Moscow, 16 March 2020.
75 Google Data Center Locations, 2020; Tatyana Lokot, 'Google Denies Russian Media Claims on Data Localization Move', *Global Voices,* 13 April 2015.

a co-founder of the Russian organisation Internet Protection Society: '[T]here was absolutely no difference between how LinkedIn and how Facebook stored and dealt with the personal data of their Russian users. The only thing that made a difference was politics.'[76]

This prompts the question of why only LinkedIn was selected and how that decision helps the Russian government control RuNet. Volkov argues convincingly that LinkedIn was carefully selected by ROSKOMNADZOR: '[Linkedin is] a big brand, with an even bigger one behind it (Microsoft)'. So 'it was chosen to scare off larger players'.[77] According to this interpretation, the Kremlin selectively implemented Law № 242-FZ against LinkedIn, not to force other intermediaries to comply with server localisation requirements but to communicate a message concerning the necessity of cooperating with the authorities. In a manner reminiscent of the Khodorkovsky case, blocking LinkedIn signalled to other social networking platforms that they could face similar sanctions should they oppose the government. The implicit message was that they must comply with certain requests from the Kremlin and suppress specific undesired content—for instance, calls for unauthorised protests or 'information expressing clear disrespect for the official state symbols of Russia'—if they wish to stay out of trouble.[78] Following the selective enforcement of the law against LinkedIn, Western internet firms 'started to express more willingness to engage in dialogue with Russian regulators' and comply with certain of their demands.[79] In recent years, Western firms' transparency reports indicate a sharp rise in requests sent by Russian authorities to restrict access or remove content and in the positive answers given by companies to such requests.[80]

Selective enforcement has thus helped the Kremlin find a sweet spot where they both have the means to pressure Western internet intermediaries and at the same time can fulfil Russian citizens' demands for access to Western services and thus avoid a potential popular backlash. Indeed, despite widely publicised threats, the Russian government has not cut access to platforms such as YouTube, Twitter, or Facebook, which have been used primarily by hundreds

76 Leonid Volkov, 'Why Are Western Internet Companies Cooperating with the Putin Regime to Censor the Web?', *Open Democracy*, 9 April 2018.
77 Ibid.
78 ROSKOMNADZOR, 'Po trebovaniyu ROSKOMNADZORA YouTube ogranichil dostup k roliku s oskorbitel'nymi deystviyami v adres gosudarstvennogo flaga Rossii' [At the demand of ROSKOMNADZOR YouTube limited access to an offensive video against the national flag of Russia], 19 August 2019.
79 Alexander Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?', *Computer Law & Security Review*, 32(1), (2016): p. 145.
80 Google, 'Transparency Report: Government Requests to Remove Content, 2020; Twitter, 'Transparency Report: Russia Removal Requests', 2020.

of thousands of apolitical Russian citizens for entertainment and routine communications since the mid-2000s. According to internet activist and media scholar Ethan Zuckerman's 'cute cat theory of digital activism', governments have little interest in blocking popular platforms used by citizens for non-political activities, as this would risk undermining the regime's stability and legitimacy.[81] In contrast to imposing sanctions on LinkedIn, which was, according to Volkov, used only by a limited number of people who were 'part of the white-collar audience and unlikely to march in the streets against internet censorship', the closure of popular Western platforms would likely alienate much of the population, politicise those most affected, and fuel opposition against the government.[82] Hence, the selective application of the law has helped the government limit loss of legitimacy and communicate to Western platforms that they must cooperate with the Kremlin.

Non-Systemic Opposition as a Targeted Audience

In addition to internet intermediaries, the government has also focused its activities on controlling non-systemic opposition to government policies in the online sphere. The following section examines the selective application of the law directed at this second audience. An analysis of the authorities' decision to block an online voting project launched by dissenters will show how the government uses this tool to signal to its most vocal critics the boundaries of tolerated online political activities, and to circumscribe the behaviour and aspirations of the opposition's wider audience on RuNet.

In November 2018, the leader of the non-systemic opposition, Alexei Naval'ny, launched his new online project, the 'smart voting' strategy website, *2019.vote*, designed to predict the candidate most likely to win in an election against a member of the governing party United Russia (UR), based on opinion polls and previous election results, in each single-member district (SMD). The goal was for all citizens registered on the website to gather their votes for the endorsed candidate and defeat UR. Naval'ny's smart voting sought to 'leverage digital technologies to circumvent problems of coordination and to exploit the vulnerabilities of the hybrid political system'.[83] However, a few weeks following the launch of *2019.vote* in December 2018, ROSKOMNADZOR filed a lawsuit

81 Ethan Zuckerman, 'Cute Cats to the Rescue?', in *From Voice to Influence: Understanding Citizenship in a Digital Age*, D. Allen and J. S. Light, (Chicago: Chicago University Press, 2015): 131–54.
82 Volkov, 'Why are Western Internet Companies Cooperating'.
83 Jan Matti Dollbaum, 'Outsmarting Electoral Authoritarianism? Alexey Naval'ny's "Smart Voting" in Moscow and Beyond', *Russian Analytical Digest,* № 239, 26 September 2019: p. 7

to include the smart voting website in the *Registry of Violators of the Privacy of Individual Personal Information* and to block access to it because Naval'ny's election technology platform allegedly did not meet the legal requirements for the protection of online personal data. As previously mentioned, Federal Law № 242-FZ requires websites to store Russian citizens' data on Russian territory and allows ROSKOMNADZOR to suspend access to sites that violate data privacy laws. The text of the court's official decision stated that Naval'ny's website relied on two services to evaluate website traffic and analyse user behaviour (Google Analytics and Yandex Metrica), 'whose servers are located in the United States'.[84] The court also added that the website did not notify users that their personal information was being collected, did not ask users for their consent, and did not include a document declaring a privacy policy.[85] Based on these violations of Federal Law № 242-FZ, ROSKOMNADZOR included *2019.vote* in the registry, which led to the website being blocked.

This legal decision constitutes a clear case of selective law enforcement. We demonstrated above that the requirement for storing Russian citizens' data on servers located in Russia has been only selectively implemented. According to this criterion, a large share of websites available to Russian users should be included in the registry. Furthermore, Russian bloggers revealed that the government's official websites were committing similar privacy 'violations' to those of Naval'ny's project.[86] For instance, as their source codes verify, the website of the State Duma relies on Yandex Metrics, and the website of the Presidential Administration of the Russian Federation employs Yandex services and the Google Analytics system.[87] Both of these official Russian government websites rely on services 'whose servers are located in the United States', do not include a privacy policy document, and do not warn users about data collection nor ask for their consent to collect personalized information. Similarly, while UR has published a privacy policy document, its website does not ask users if they allow Facebook to process their personal data, despite the social media platform collecting and storing their personalised statistics and analytics on servers located in the US.[88] These sites remain accessible, despite violating the

84 Russian Federation, Tagansky district court, 'Case Decision № 02-4261/2018', Moscow, 19 December 2018.
85 Ibid.
86 Alexander V. Litreev, 'Zakon dlya vsekh yedin—ROSKOMNADZOR i sayt «Umnoye Golosovaniye»' [The law is the same for everyone—ROSKOMNADZOR and the site "Smart Voting"], Alexander V. Litreev's Blog on *Medium*, 19 December 2018.
87 Russian Federation, *State Duma Page Source Code*, 2020; Russian Federation, *Server of the State Bodies of the Russian Federation Page Source Code*, 2020.
88 Russian Federation, *Edinaya Rossiya Page Source Code*, 2020.

same laws that led to the shutdown of Naval'ny's political project.

The selective application of Law № 242-FZ against Naval'ny's project allowed the Kremlin to limit the opposition's capacity to promote an anti-UR voting scheme before the elections and thus its capacity to threaten the state's grip on power. This selective implementation of the law communicated that, while Naval'ny's popular YouTube videos were left untouched, if the regime feels threatened it can always use existing legislation to limit any meaningful online projects launched by the opposition.

Naval'ny's position can be compared to that of LinkedIn in the previous example. As the most popular figure of the non-systemic opposition, Naval'ny constitutes a 'convenient symbol' the authorities can target to communicate messages to the opposition's audience concerning acceptable political behaviour. As Gel'man explains, selective enforcement of the law against political opponents serves to 'keep the opposition isolated and limits its capacity to grow: [It] is aimed […] not so much at punishing the regime's enemies (although these purposes are present in some cases), but at preventing the spread of hostile activity beyond the (usually very narrow) circle of direct opponents'.[89] Indeed, while the opposition and its supporters may succeed in bypassing the blocking of their website through technical means, those who are contemplating joining the non-systemic opposition can grasp the double standard at play, interpret the decision to block Naval'ny's website as politically motivated, and thus be discouraged from joining the non-systemic opposition due to fear of sanctions. The precise impact of this practice on citizens' willingness to join the opposition cannot be estimated, as citizens who have been thus deterred refrain from voicing their opinions. Still, Gel'man suggests that 'under those circumstances, the circle of dissenters remained narrow and had no real opportunity to expand their ranks'.[90] Using selective law enforcement to limit projects that might influence election results allows the regime to minimise the impact of the non-systemic opposition's online activities and to communicate, to precisely the audience most likely to challenge it, state-sanctioned values associated with 'managed democracy', in which elections constitute a means to reinforce the regime's legitimacy rather than an opportunity for citizens to contest the leadership of the incumbent.

Citizenry as a Targeted Audience

89 Gel'man, 'The Politics of Fear', p. 9.
90 Ibid., p. 14.

In 2018–19 there was growing discontent in the Russian countryside and the people began voicing their demands for political change. This led more citizens to publish their criticisms of the government and local authorities on social media.[91] Consequently, the government decided to employ selective legislation also towards ordinary citizens to shape their online behaviour. The pattern of enforcement of Federal Law № 30-FZ[92] exemplifies the use of selective implementation of the law to control the third audience, the common citizens.

Federal Law № 30-FZ prohibits the dissemination of online information considered to be 'indecent expressions and obvious disrespect towards society, the state, official state symbols and the constitution of the Russian Federation, and bodies exercising state authority in the Russian Federation'. For posting such content, violators face fines of up to 100 thousand RUB (1,400 USD) and 300 thousand RUB (4,200 USD) in the case of a repeated offence. Additionally, following a request from the Prosecutor General, ROSKOMNADZOR may demand the deletion of information considered to be indecent.

This piece of legislation was hastily adopted. Deputy Andrei Klishas introduced it in the State Duma in December 2018, and it came into force only four months later, in March 2019. This left no time to respond to criticisms that were repeatedly raised by the Presidential Council for Civil Society and Human Rights (SPCh), the consultative body to the President of the Russian Federation tasked with assisting the presidency in guaranteeing and protecting human rights and freedoms in Russia. The SPCh demanded the rejection of the bill on the grounds that the vague definition of what constitutes 'indecent expressions and obvious disrespect' leaves 'a very high degree of discretion' in the hands of law enforcers. Consequently, 'it can be applied as one desires', and opens the door for violation of the principles of equality under the law.[93] Senators at the Federation Council, the upper house of the Russian Parliament, voted that 'each court, depending on the circumstances, will decide for itself what an indecent form is and what a decent form is'.[94] Such public concern suggests that, from its

91 Andrei Kolesnikov and Denis Volkov, 'Russians' Growing Appetite for Change', *Carnegie Moscow Center*, January 2020.
92 The State Duma, *On Amending the Federal Act "On Information, Information Technologies, and Protection of Information*, Federal Law № 30-FZ, 18 March 2019.
93 Russian Federation, Presidential Council for Civil Society and Human Rights , 'V SPCH raskritikovali zakony o feykovykh novostyakh i oskorblenii vlasti' [SPCh criticizes the law on fake news and on insulting authority], 16 May 2019; Russian Federation, Presidential Council for Civil Society and Human Rights, 'Ekspertnyye zaklyucheniya' [Expert opinions], 11 March 2019.
94 Russian Federation, Federation Council, '454 zasedaniye Soveta Federatsii' [Meeting №454 of the Federation Council], 13 March 2019.

very conception, Law № 30-FZ was designed to be selectively enforced.

Following the first prosecution under Law № 30-FZ, leaders of the non-systemic opposition and their supporters posted hundreds of messages that could potentially be considered illegal according to that piece of legislation.

A cursory look at Russian social media reveals that everyday users post messages that can be considered 'indecent expressions towards bodies exercising state authority in the Russian Federation'. However, according to the Russian NGO Agora, in the first 18 days after Law № 30-FZ came into force, only 45 users in 29 regions were charged.[95] Those fined were generally neither activists nor public figures, but ordinary citizens from rural areas voicing their dissatisfaction with the authorities online because of issues such as declining living conditions. For instance, following a reform increasing the retirement age in Russia, a pensioner from the Krasnodar krai was fined 70 000 RUB (980 USD) for posting 'Vladimir Putin is a state criminal! Thief and impostor Vladimir Putin! Get out!' on the Russian social media platform VKontakte.[96] While the law theoretically applies to a broad range of indecent expressions directed towards state symbols and bodies exercising state authority, up to 80% of the fines imposed have been for posts directed at Vladimir Putin, further demonstrating selectivity in the application of the law.[97]

In several cases, the law was enforced against users who posted messages insulting the authorities in concert with offline protests. For instance, one of the first fines imposed for indecent expression concerned a citizen from the rural oblast of Vologda who insulted Vladimir Putin after taking part in protests against pension reforms.[98] Similarly, the largest proportion of related cases (15%) prosecuted under this law took place in the Arkhangelsk oblast, following protests against the construction of a waste dump.[99] Extra-legal criteria penetrated the legal realm, as the law was selectively enforced against users after they took part in protests. Selective prosecutions for indecent expression

95 Stanislav Seleznev, 'Votum neuvazheniya prezidentu: pervoye polugodiye «zakona Klishasa»' [Vote of disrespect to the president: first six months of the «Klisha's law»], *Agora Report*, 30 September 2019, 1–19.
96 Russian Federation, Dinskoy District Court, 'Resheniye po administrativnomu delu' [Decision concerning an administrative case], Dinskaya, 12 December 2019.
97 Ibid.
98 OVD-info, 'Na zhitelya Vologodskoy oblasti sostavili protokol o neuvazhenii k vlasti' [A protocol for disrespect toward the authorities was drawn up against a resident of the Vologda Oblast], *OVD.info.org,* 15 May 2019; Russian Federation, Verkhoyansky District, 'Press-sluzhba' [Press Service], Verkhovazhye, 6 July 2019.
99 Seleznev, 'Votum neuvazheniya prezidentu', p. 15.

constituted a means to communicate to protesters that they should refrain from engaging in demonstrations and criticisms against the regime.

While there seems to be a degree of coherence and regularity in the selective enforcement of the law, one should be wary of assuming that these patterns are always the result of a coherent pre-determined strategy established by the highest authorities and implemented by lower echelons. Selective law enforcement should not be thought of as always being part of a 'coordinated master plan', but rather as a more or less uncoordinated set of actions that are based on a shared legal culture.[100] The selection of certain citizens may well be arbitrary in certain cases and local authorities may try to instrumentalise the law for their personal interests. For example, the mayor of Troitsk, a town in the Chelyabinsk oblast, has used the law to prosecute an individual who insulted him online.[101] The increase in cases initiated by mayors or governors led the Deputy Minister of Internal Affairs (MVD) to intervene and send recommendations to the heads of the regional branches of the MVD, ordering them to report all cases concerning indecent expressions to the ministry's main directorate and to take control of them personally.[102] This reveals that the highest authorities may not be able to manipulate the law as they desire. In this instance, the government sought to regain control over the legislation following its instrumentalisation by lower echelons of authority.

Despite a temporary loss of control, the selective enforcement of this law directed at common citizens represents a powerful tool of strategic communications used by the state to limit the expression of negative public opinion on RuNet without resorting to heavy-handed censorship by technical means. First, a larger number of users would potentially relate to those prosecuted when the legislation is applied to opinions posted by common citizens rather than in instances involving leaders of the non-systemic opposition. Citizens who identify with those prosecuted are motivated to abstain from online dissent and are thus depoliticised.

Second, it is strategically prudent for the Kremlin to target individuals located in specific regions. The regime might face a bigger risk of backlash when it targets individuals living in Moscow or St Petersburg who have greater opportunities for

100 Bækken, *Law and Power in Russia*, p. 187.
101 Russian Federation, Troitsky City Court, 'Case decision № 5-50/2019', Troitsky, 5 June 2019.
102 Russian Federation, Ministry of Internal Affairs, 'O napravlenii metodicheskikh rekomendatsiy po delam o neuvazhenii k vlasti' [On the direction of methodical recommendations concerning cases of disrespect toward the authorities], № 1/7615, 1 July 2019.

making their voices heard and to contest legal decisions than pensioners isolated in rural towns. Moreover, citizens are more likely to be influenced by cases brought against people from their own regions to whom they can relate, rather than by cases brought against individuals living on the other side of the vast country or enjoying very different socio-economic conditions in Russia's capital.

Because citizens identify with their regional peers the authorities can use local cases to communicate to internet users dispersed throughout Russia that they should refrain from online dissent. The maximum fine for transgressing Law № 30-FZ is up to seven times the average monthly salary in certain area—a clear incentive for users to abstain from insulting the Kremlin.

Third, legal vagueness concerning what constitutes 'indecent expression and obvious disrespect' plays a fundamental role in fostering restraint on the part of Russian citizens. In their study of authoritarian practices on the internet, legal theorists Bryan Druzin and Gregory S. Gordon write: 'the precise ambit of permissible speech is left unclear so as to maximize the range within which people voluntarily restrain their behaviour online, creating a chilling effect on public speech'.[103] The line between legitimate criticism and indecent expression is left ill-defined, creating uncertainty and thus further incentives for citizens to refrain altogether from online criticism directed at the authorities.

Finally, to further ensure that the selective use of the law functions as a means of Strategic Communications, prosecutions for 'indecent expression and obvious disrespect' are often widely publicised in regional newspapers and on television channels under the control of the authorities. For instance, in Krasnodar Krai, 'Kuban News', the official newspaper of the regional administration and the most read in the region, has consistently reported on legal sanctions for 'obvious disrespect', as in the example of the pensioner previously mentioned.[104] Such publicising of selective enforcement serves to amplify the signalling and deterring effect created by selective enforcement of the law.[105] This helps authorities get their message through to a vast audience spread throughout the territory of the Russian Federation. Hence, without large-scale restriction,

103 Bryan Druzin and Gregory S. Gordon, 'Authoritarianism and the Internet', *Law & Social Inquiry*, 43(4), (2018): p. 1431.
104 Kubanskie Novosti, 'Pensioner iz Krasnodarskogo kraya oshtrafovan na 70 tysyach za oskorbleniye prezidenta Putina' [A pensioner from the Krasnodar Kray was fined 70 thousands for insults against President Putin], 25 February 2020.
105 Kirill Rogov, 'The Art of Coercion: Repressions and Repressiveness in Putin's Russia', *Russian Politics*, 3(2), (2018): 151–74.

which has the potential to damage government legitimacy, selectively enforcing Federal Law № 30-FZ against ordinary citizens represents a particularly helpful tool of Strategic Communications for the Kremlin to control and shape this audience's behaviour on RuNet.

Conclusion

The debate that followed the adoption of numerous internet regulations in Russia around 2013, concerning the Kremlin's technical capacity to implement its legislation in full and limit all dissenting speech on RuNet, fails to take into account the more subtle ways in which the authorities shape the online sphere. In accordance with Russia's enduring legal culture, the Kremlin uses legislation selectively as a tool of Strategic Communications to control RuNet, communicating to various audiences the boundaries of tolerated behaviour in the online sphere. Through selective enforcement of existing legislation, the Kremlin 1) signalled to Western intermediaries that they must cooperate with the authorities, 2) suppressed a potentially threatening political project promoted by the non-systemic opposition and surgically delineated the limits of activists' online behaviour, and 3) deterred ordinary citizens from all walks of life throughout the vast territory of Russia from freely expressing their criticisms of the government online. The strategy of selective enforcement allows the government to maintain unrestricted access to the internet for the vast majority of citizens, while simultaneously ensuring their acceptance of the adoption of further regulations and keeping popular backlash to a minimum.[106] In sum, internet regulations are used selectively by the government to achieve its objective of communicating the unwritten 'rules of the game' for online political behaviour to various audiences while limiting the risks of popular backlash in the contested environment that is RuNet.

As Strategic Communications is 'a holistic approach to communication based on values,'[107] selective enforcement of RuNet regulations must be conceived holistically as a tool of the Russian government within the broader legal culture, together with other tools at the Kremlin's disposal that might further shape users' behaviour, such as government surveillance or the mass dissemination of pro-government content.[108]

106 Asmolov, 'Welcoming the Dragon'.
107 Bolt and Haiden, NATO Strategic Communications Terminology, p. 46.
108 Jonathon W. Penney, 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study', *Internet Policy Review*, 6(2), (2017): 1–39; Seva Gunitsky, 'Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability', *Perspectives on Politics*, 13(1), (2015): 42–54.

One question remains: how effective is Russia's use of internet regulations as a tool of strategic communications? It is difficult to isolate the effect of this strategy from other dynamics that might protect the legitimacy of the regime and those that might influence the propensity of citizens to oppose the Kremlin both on and offline. In the past decade the Kremlin has successfully employed legal practices to mark and enforce the boundaries of permissible political behaviour, while leaving the online sphere seemingly unrestricted and thus avoiding public backlash. It is perhaps no coincidence that the largest opposition movement coordinated online remains the 2011 Bolotnaya protest, an event that just preceded the introduction of stricter internet regulations on public speech. Contrary to the cyber-utopianist view prevalent in the wake of this protest, few would now argue that the expansion of internet use and Russian citizens' access to foreign social media represent an existential threat to the Russian regime. On the contrary, the case can be made that the Kremlin now benefits from the openness of the online sphere. The regime enhances its legitimacy by leaving 'enough room for a sufficiently wide range of subjects that people can let off steam about government corruption or incompetence' while it can reassert, through the selective use of the law, the boundaries of this 'space of freedom' when its grip on power seems threatened.[109]

Russia's selective enforcement of the law is nothing other than careful management of the online sphere by targeting the few to discipline the rest. While Russia's ability to shape RuNet has been robust so far, small shifts in public perception regarding permissible limits of online expression and the need to respect the rules communicated by the leadership could rapidly 'proliferate into large-scale torrents of uncensored speech'.[110] The future of RuNet depends to a great extent on various audiences' willingness and capacity to break the yoke of fear and boundaries of online political conduct communicated and enforced through selective application of the law.

Acknowledgements

The author is grateful for the support and helpful feedback of Dr Ofer Fridman.

109 Rebecca MacKinnon, 'Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China', *Public Choice*, 134(1/2), (2008), p. 33.
110 Druzin and Gordon, 'Authoritarianism and the Internet', p. 27.

Bibliography

Alexander, Marcus, 'The Internet and Democratization: The Development of Russian Internet Policy', *Demokratizatsiya*, 12(4), (2004): 607–27.

Asmolov, Gregory and Polina Kolozaridi, 'The Imaginaries of RuNet: The Change of the Elites and the Construction of Online Space', *Russian Politics,* 2(1), (2017): 54–79.

Asmolov, Gregory, 'Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation', *Internet Policy Observatory*, (2015): 1–13.

Bækken, Håvard, 'Selections Before Elections: Double Standards in Implementing Election Registration Procedures in Russia?', *Communist and Post-Communist Studies*, 48(1), (2015): 61–70.

_____, *Law and Power in Russia: Making Sense of Quasi-Legal Practices* (New York: Routledge, 2018).

Belton, Catherine, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (London: William Collins, 2020).

Bolt, Neville and Leonie Haiden, *Improving NATO Strategic Communications Terminology*, (Riga, Latvia: NATO Strategic Communications Centre of Excellence, June 2019).

Borisova, Tatiana and Jane Burbank, 'Russia's Legal Trajectories', *Kritika: Explorations in Russian and Eurasian History*, 19(3), (2018): p. 469–50.

Burbank, Jane, 'Lenin and the Law in Revolutionary Russia', *Slavic Review*, 54(1), (1995): 23–44.

Chander, Anupam and Uyên P. Lê, 'Data Nationalism', *Emory Law Journal*, 64(3), (2014): 677–740.

Clinton, Hillary, 'Conference on Internet Freedom', speech at the Hague, 8 December 2011.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War', *Security Dialogue*, 43(1), (2012): 3–24.

DeNardis, Laura, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

Dollbaum, Jan Matti, 'Outsmarting Electoral Authoritarianism? Alexey Naval'ny's "Smart Voting" in Moscow and Beyond', *Russian Analytical Digest,* № 239, September 2019: 5–8.

Druzin, Bryan, and Gregory S. Gordon, 'Authoritarianism and the Internet', *Law & Social Inquiry*, 43(4), (2018): 1427–57.

Duffy, Natalie, 'Internet Freedom in Vladimir Putin's Russia: The Noose Tightens', *American Enterprise Institute*, 12 January 2015, 1–12.

Dzmitryieva, Aryna, 'How the Law Really Works: The New Sociology of Law in Russia', *Economic Sociology—The European Electronic* Newsletter, 13(2), (2012): 13–20.

Ermoshina, Ksenia and Francesca Musiani, 'Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era', *Media and Communication*, 5(1), (2017): 42–53.

Etling, Bruce, Karina Alexanyan, John Kelly, Robert Faris, John Palfrey, and Urs Gasser, 'Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization', *Berkman Center Research Publication*, (2010): 1–46.

Fedor, Julie and Rolf Fredheim, '"We Need More Clips About Putin, and Lots of Them:" Russia's State-commissioned Online Visual Culture', *Nationalities Papers*, *45*(2), (2017): 161–81.

Fortescue, Stephen, *Russia's Oil Barons and Metal Magnates: Oligarchs and the State in Transition* (New York: Palgrave Macmillan, 2006).

Fridman, Ofer, 'The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse', *Defence Strategic Communications*, 2(2), (2017): 61–86.

_____, *Russian "Hybrid Warfare": Resurgence and Politicization* (New York: Oxford University Press, 2018).

Friedman, Lawrence M., 'Is There a Modern Legal Culture?', *Ratio Juris*, 7(2), (1994): 117–31.

Gainous, Jason, Kevin M. Wagner, and Charles E. Ziegler, 'Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections', *Democratization*, 25(2), (2018): 209–26.

Gel'man, Vladimir, 'The Politics of Fear: How the Russian Regime Confronts Its Opponents', *Russian Politics & Law*, 53(5/6), (2015): 6–26.

_____, 'The Unrule of Law in the Making: The Politics of Informal Institution Building in Russia', *Europe-Asia Studies*, 56(7), (2004): 1021–40.

Goldsmith, Jack and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

Google, Google Data Center Locations, 2020.

_____, 'Transparency Report: Government Requests to Remove Content', 2020.

Greenberg, Jonathan D., 'The Kremlin's Eye: The 21st Century Prokuratura in the Russian Authoritarian Tradition', *Stanford Journal of International Law*, 45(1), (2009): 1–50.

Gunitsky, Seva, 'Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability', *Perspectives on Politics*, 13(1), (2015): 42–54.

Hendley, Kathryn, *Everyday Law in Russia* (New York: Cornell University Press, 2017).

Kendall-Taylor, Andrea, Erica Frantz, and Joseph Wright, 'The Digital Dictators. How Technology Strengthens Autocracy', *Foreign Affairs,* 6 February 2020.

Kerr, Jaclyn A., 'The Russian Model of Internet Control and Its Significance', *Lawrence Livermore National Lab*, (2018): 1–7.

Klyueva, Anna, 'Taming Online Political Engagement in Russia: Disempowered Publics, Empowered State and Challenges of the Fully Functioning Society', *International Journal of Communication*, 10, (2016): 4661–80.

Kolesnikov, Andrei and Denis Volkov, 'Russians' Growing Appetite for Change', *Carnegie Moscow Center*, January 2020.

Konradova, Natalja, Henrike Schmidt, and Katy Teubener (eds), *Control + Shift: Public and Private Usages of the Russian Internet* (Norderstedt: Books on Demand, 2006).

Kravchenko, Maria, 'Russian Anti-Extremism Legislation and Internet Censorship', *The Soviet and Post-Soviet* Review, 46(2), (2019): 158–86.

Kvurt, Yelina, 'Selective Prosecution in Russia-Myth or Reality', *Cardozo Journal of International and Comparative* Law, 15(1), (2007): 127–68.

Ledeneva, Alena V., *Can Russia Modernise? Sistema, Power Networks and Informal Governance* (Cambridge: Cambridge University Press, 2013).

Lipman, Masha, 'Constrained or Irrelevant: The Media in Putin's Russia', *Current History*, 104(684), (2005): 319–24.

Litreev, Alexander V., 'Zakon dlya vsekh yedin— ROSKOMNADZOR i sayt «Umnoye Golosovaniye»' [The law is the same for everyone– ROSKOMNADZOR and the site "Smart Voting"], Alexander V. Litreev's Blog on *Medium*, 19 December 2018.

Lokot, Tatyana, 'Google Denies Russian Media Claims on Data Localization Move', *Global Voices,* 13 April 2015.

MacKinnon, Rebecca, 'Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China', *Public Choice*, 134(1/2), (2008): 31–46.

Makutina, Maria, 'Tsifrovoy suverenitet' [Digital sovereignty], *Gazeta.ru*, 19 June 2013.

Medvedev, Dmitry, 'Gosudarstvo i internet: poyavilis' novyye instituty' [State and the Internet: new institutions have appeared'], 18 April 2012.

_____, 'Razgovor s Dmitriyem Medvedevym' [Discussion with Dmitry Medvedev], Moscow, 5 December 2019.

Mendras, Marie, *Russian Politics: The Paradox of a Weak State* (London: Hurst Publishers, 2012).

Mueller, Milton, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010).

Natalya, Kovaleva, 'Russian Information Space, Russian Scholarship, and Kremlin Controls', *Defence Strategic Communications*, 4(1), (2018): 113–35.

Nocetti, Julien, 'Russia's "Dictatorship-of-the-law" Approach to Internet Policy', *Internet Policy* Review, 4(4), (2015): 1–19.

Oates, Sarah, *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere* (Oxford: Oxford University Press, 2013).

Oleinik, Anton, 'Existing and Potential Constraints Limiting State Servants' Opportunism: The Russian Case', *Journal of Communist Studies and Transition Politics*, 24(1), (2008): 156–89.

OVD-info, 'Na zhitelya Vologodskoy oblasti sostavili protokol o neuvazhenii k vlasti' [A protocol for disrespect toward the authorities was drawn up against a resident of the Vologda Oblast], *OVD.info.org,* 15 May 2019.

Paneyakh, Ella, 'Neformal'nyye instituty i ispol'zovaniye formal'nykh pravil: zakon deĭstvuyushchiĭ vs zakon primenyayemyĭ' [Informal institutions and the use of formal rules: acting law vs law in action], *Politicheskaya Nauka*, 1, (2003): 33–52.

Partlett, William, 'Putin's Artful Jurisprudence', *The National Interest* № 123, (January/February 2013): 35–45.

Penney, Jonathon W., 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study', *Internet Policy Review*, 6(2), (2017): 1–39.

Putin, Vladimir, 'Direct Line with Vladimir Putin', Moscow, 20 June 2019.

_____, 'Zasedaniye Soveta Bezopasnosti' [Security Council Meeting], Moscow, 1 October 2014.

Ristolainen, Mari, 'Should "RuNet 2020" be Taken Seriously? Contradictory Views About Cybersecurity Between Russia and the West', *Journal of Information Warfare*, 16(4), (2017): 113–13.

Rogov, Kirill, 'The Art of Coercion: Repressions and Repressiveness in Putin's Russia', *Russian Politics*, 3(2), (2018): 151–74.

ROSKOMNADZOR, 'Po trebovaniyu ROSKOMNADZORA YouTube ogranichil dostup k roliku s oskorbitel'nymi deystviyami v adres

gosudarstvennogo flaga Rossii' [At the demand of ROSKOMNADZOR YouTube limited access to an offensive video against the national flag of Russia], 19 August 2019.

Russian Federation, Dinskoy District Court, 'Resheniye po administrativnomu delu' [Decision concerning an administrative case], locality of Dinskaya in Krasnodar Krai, 12 December 2019.

_____, *Edinaya Rossiya Page Source Code*, 2020.

_____, Federation Council, '454 zasedaniye Soveta Federatsii' [Meeting № 454 of the Federation Council], 13 March 2019.

_____, Ministry of Internal Affair, 'O napravlenii metodicheskikh rekomendatsiy po delam o neuvazhenii k vlasti' [On the direction of methodical recommendations concerning cases of disrespect toward the authorities], № 1/7615, 1 July 2019.

_____, Presidential Administration, '*On public administration issues in the field of communication, communication technologies and mass media*', Decree № 1715, Moscow, 3 December 2008.

_____, Presidential Adminsitration, *On the Russian Federation National Security Strategy*, Decree N 683, Moscow, 31 December 2015.

_____, Presidential Council for Civil Society and Human Rights, 'V SPCH raskritikovali zakony o feykovykh novostyakh i oskorblenii vlasti' [SPCh critizes the law on fake news and on insulting authority], 16 May 2019.

_____, Presidential Council for Civil Society and Human Rights, 'Ekspertnyye zaklyucheniya' [Expert opinions], 11 March 2019.

_____, *State Duma Page Source Code,* 2020.

_____, *Server of the State bodies of the Russian Federation Page Source Code*, 2020.

_____, Tagansky District Court, 'Case Decision № 02-3491/2016', Moscow, 4 August 2016.

_____, Tagansky District Court, 'Case Decision № 02-4261/2018', Moscow, 19 December 2018.

_____, Tagansky District Court, 'Case Decision № 12-0513/2019', Moscow, 8 May 2019.

_____, Tagansky District Court, 'Case Decision № 12-0449/2020', Moscow, 16 March 2020.

_____, *The Information Security Doctrine of the Russian Federation*, Moscow, 5 December 2016.

_____, Troitsky City Court, 'Case Decision № 5-50/2019', town of Troitsky in Chelyabinsk oblast, 5 June 2019.

_____, Verkhoyansky District, 'Press-sluzhba' [Press Service], district of Verkhovazhye in Vologda oblast, 6 July 2019.

Sakwa, Richard, 'Putin and the Oligarchs', *New Political Economy*, *13*(2), (2008): 185–91.

_____, *The Crisis of Russian Democracy: The Dual State, Factionalism, and the Medvedev Succession* (Cambridge: Cambridge University Press, 2011).

Sargsyan, Tatevik, 'Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security', *International Journal of Communication*, 10, (2016): 2221–37.

Savelyev, Alexander, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?', *Computer Law & Security Review*, 32(1), (2016): 128–45.

Seleznev, Stanislav, 'Votum neuvazheniya prezidentu: pervoye polugodiye «zakona Klishasa»' [Vote of disrespect to the president: first six months of the «Klishas law»], *Agora report*, (September 2019): 1–19.

Sharlet, Robert, 'Soviet Legal Reform in Historical Context', *Columbia Journal of Transnational Law*, 28(1), (1990): 195–234.

Sakwa, Richard, *Putin: Russia's choice.* (New York: Routledge, 2007).

Sherman, Justin, 'Trump's Un-American Failure to Protect Internet Freedom', *Wired,* 22 October 2020.

Skillen, Daphne, *Freedom of Speech in Russia: Politics and Media from Gorbachev to Putin* (London: Routledge, 2017).

Soldatov, Andrei and Irina Borogan, 'Russia's Surveillance State', *World Policy Journal,* 2 March 2015.

_____, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: Public Affairs, 2015).

Soldatov, Andrei, 'The Taming of the Internet', *Russian Social Science Review*, 58(1), (2017): 39–59.

Solomon, Peter H., *Soviet Criminal Justice Under Stalin* (Cambridge: Cambridge University Press, 1996).

The State Duma, *On Amendments to the Federal law "On communications" and the Federal law "On information, information technologies and information protection*", Federal Law N 90-FZ, Moscow, 1 May 2019.

_____, *On the Protection of Children from Information Harmful to Their Health and Development and Other Legislative Acts of the Russian Federation*, Federal Law N 139-FZ, Moscow, 28 July 2012.

_____, *On Amendments to the Federal Law, "On Information, Information Technologies and Protection of Information"*, Federal Law N 398-FZ, Moscow, 28 December 2013.

_____, *On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks*, Federal Law N 242-FZ, Moscow, 21 July 2014.

_____, *On Amending the Federal Act "On Information, Information Technologies, and Protection of Information"*, Federal Law N 30-FZ, 18 March 2019.

_____, *On Amendments to Article 15-3 of the Federal Statute on Information, Information Technologies and Protection of Information*, Federal Law N 31-FZ, Moscow, 18 March 2019.

Tselikov, Andrey, 'The Tightening Web of Russian Internet Regulation', *Berkman Center Research Publication*, № 2014/15, (2014): 1–20.

Twitter, 'Transparency Report: Russia Removal Requests', 2020.

Tysiachniouk, Maria, Svetlana Tulaeva, and Laura A. Henry, 'Civil Society Under the Law 'On Foreign Agents': NGO Strategies and Network Transformation', *Europe-Asia Studies*, 70(4), (2018): 615–37.

Volkov, Leonid, 'Why are Western Internet Companies Cooperating with the Putin Regime to Censor the Web?', *Open Democracy*, 9 April 2018.

Zheleznak, Sergey, 'My dolzhny obespechit' «tsifrovoy suverenitet» nashey strany' [We must ensure the "digital sovereignty" of our country], *Ekonomika i Zhizn'*, 19 June 2013.

Zuckerman, Ethan, 'Cute Cats to the Rescue?', in *From Voice to Influence: Understanding Citizenship in a Digital Age*, D. Allen and J. S. Light, (Chicago: University Press, 2015): 131–54.