This is an Accepted Manuscript of a book chapter published by Routledge in Freedom of Expression in Russia's New Mediasphere on 14 November 2019, available online: https://doi.org/10.4324/9780429437205.

2 The blacklisting mechanism: new-school regulation of online expression and its technological challenges

Liudmila Sivetc

Introduction

The global expansion of the internet has given rise to new opportunities to publish and access information. However, internet technologies have not only enhanced but also stifled free expression (Lessig 2006; Drezner 2010; Balkin 2014). The same technologies that empowered people to publish for a world-wide audience also enabled states to censor content in novel ways (Balkin 2014). One of these novel ways to restrain the freedom of expression consists of including, in regulation, a new agency – internet service providers – who host online content and/or connect internet users with corresponding websites. Some states see these providers as the best-placed party to block online content in accordance with notifications issued by officials (Deibert et al. 2010). As non-compliance with blocking notifications leads to liability, providers act as collateral censors: they prefer to remove notified content without considering its possible value for the public. Balkin (2014) defines this practice as the 'new school of speech regulation'. He stresses that old-school regulation was based on penalising unlawful content *post ante* as the result of court proceedings. In contrast, new-school regulation relies on penalising allegedly illegal content *ex ante* as the result of administrative procedures.

This new type of regulation has been applied in Russia since 2012 in the form of website blacklisting and blocking (henceforth the "blacklisting mechanism"). The blacklisting mechanism relies on two Federal Laws, No. 139-FZ (2012) and No. 398-FZ (2013). These laws have empowered the Federal Service for Supervision of Communications, Information

Technology and Mass Media (henceforth "Roskomnadzor") to include without court oversight websites containing prohibited information in a special register (henceforth "the Blacklist")[1] and to order internet service providers to block these websites from internet users. The first law introduced the blacklisting of the following kinds of illegal information: child sexual abuse images, information on producing and acquiring drugs, information on illegal gambling and information on ways of committing suicide. The second law expanded the legal basis for website blacklisting to those containing calls for extremist activities,[2] public rallies and unsanctioned public meetings. In 2017, a new category was added on this list: materials published by foreign NGOs that have been designated as 'undesirable' organisations in Russia (Federal Law No. 327-FZ 2017).

Internet companies, for instance Yandex and Wikipedia, have challenged these laws for denying access to information (Yandex Official Blog 2012; Turovsky 2015). In its report 'Freedom on the Net 2015', Freedom House (2015) negatively assessed the laws and consequently changed Russia's Press Freedom Status from 'partly free' to 'not free'. Researchers have criticised the blacklisting mechanism because the laws define various kinds of illegal information in such a vague manner that arbitrary enforcement becomes possible (Favret 2013; Tselikov 2014; Nocetti 2015). Furthermore, researchers have highlighted that the absence of preliminary court overview may allow officials to use the blacklisting mechanism for political purposes: blocking opposition websites even if they do not contain illegal information.

Even though the blacklisting mechanism has seriously endangered freedom of expression, the relevant legal basis, consisting not only of the blacklist laws but also of the bulk of subordinate legislation, has remained underexplored (Jackson 2016). This chapter aims to fill this gap in the literature. Moreover, this chapter hopes to throw some light onto the relationship of censorship,

legality and technology in contemporary Russia. I will explain the blacklisting mechanism as a new-school regulatory tool in the section 'Managing the Blacklist'. In addition, I will ask why blacklisting does *not* always lead to actual blocking. In the section 'Technological Weaknesses of Blacklisting Mechanism', I discuss two side-effects: over-blocking and malicious blocking. I argue that over-blocking presents an inevitable consequence of coopting internet providers to censor online. Moreover, I stress that malicious blocking questions the future of the blacklisting mechanism as an adequate solution from a technological standpoint.

As a result, I will address one of this book's central questions of whether digital technologies have provided new ways to circumvent state control as follows. On the one hand, digital technologies and the blacklisting mechanism have made it easier for the state to censor online content; yet, on the other, the effects of censorship have not only surpassed the intentions of the legislator, but also have undermined the efficiency of the blacklisting mechanism.

This chapter refers to freedom of expression as the fundamental human right to hold opinions and to disseminate ideas, as well as to receive and impart information in every lawful manner accepted in a democratic society, as provided for by Article 10 of the European Convention for the Protection of Human Rights (ECHR).

Managing the Blacklist

The Blacklist: scale of suppression

The Blacklist appeared in Russia in November of 2012. By August 2017, Roskomnadzor reported that the agency blacklisted approximately 275,000 web resources (Smitiuk 2017). According to official statistics published by Roskomnadzor (Report 2017,64), the agency blacklisted 88,500 websites and web pages in 2016. This figure increased dramatically in

comparison with 2015, when the Blacklist contained 49,700 websites (Report 2016, 59). This growth was, in part, due to an increase in the number of websites blacklisted for advocacy of suicide, from almost 2,600 in 2015 to almost 6,200 in 2016, and for information on illegal gambling, from 1,000 in 2015 to almost 18,200 in 2016. Yet, the main reason for the growth was the influx of websites blacklisted for extremist speech,[3] from 5,000 in 2015 to more than 26,000 in 2016 (Report 2017, 64, 66). Thus, websites containing extremist speech constituted almost one-third of the Blacklist in 2016. It is important to note that Roskomnadzor takes over half of websites off the Blacklist after they remove the banned content (as is discussed below).[4]

The Blacklist is not limited to domestic websites, that is, those registered in the .ru and .рф top-level domains; it also contains foreign websites. This stretches out Russian jurisdiction to content placed abroad yet accessible in Russia, although the enforcement with regard to foreign companies is problematic. For instance, in 2016, Roskomnadzor (ibid., 65) blacklisted almost 2,300 web pages placed on YouTube.com, 1,800 on Twitter.com, 342 on LiveJournal.com and 60 on Facebook.com. Yet, most of all blacklisted web pages, almost 19,600 (ibid., 65), were placed on VKontakte.com, the most popular online social platform in Russia. In contrast to VKontakte, its competitor Odnoklassniki (OK.ru) had only 554 blacklisted web pages (ibid., 65). These figures, plus the comparison of the number of blacklisted web pages placed on VKontakte, 19,600, with the total number of websites and web pages blacklisted in 2016, 88,500, lead one to the conclusion that this online social platform might be the main target of the blacklisting campaign.

Notably, these statistics cannot explain the scale of suppression, because the original content can be blacklisted many times. Recurrent blacklisting occurs if Roskomnadzor claims that blacklisted

content has been re-created or mirrored[5] on another website. In this case, Roskomnadzor includes such mirror-websites in the Blacklist (Rules for the Federal Agencies 2017, para 11).

Blacklisting procedures: the turn to new-school regulation

The so-called 'old-school regulation' blocks content *post ante*: courts penalise sites for illegal content and this may, secondarily, discourage others from publishing similar types of (prohibited) materials. In contrast, new-school regulation blocks content *ex ante*: officials coopt internet service providers to block allegedly illegal content, before the question of whether websites should be penalised is decided by the courts. These two types of regulation apply through the blacklisting mechanism. The Blacklist contains websites to be blocked according to court rulings and websites to be blocked according to notifications issued by officials without any preliminary court oversight. Thus, judiciary and administrative decision-making receive the same weight: judgements confirming that the content in question *is* unlawful and officials' conclusions assuming that the content *may* be unlawful leads to the same result – blacklisting and blocking. This unjustifiably elevates notifications within the legal hierarchy while degrading old-school regulation.

The role of new-school regulation in the blacklisting mechanism strengthened in March of 2017. Instead of introducing court oversight for administrative decision-making, officials' notifications were set under limited control by a special commission. This Commission consists of officials from federal agencies and representatives from internet companies. They provide for preliminary expert opinions (Rules on the Blacklist 2017, para 10). The Commission controls blacklisting in a limited manner because the Commission only advises but does not rule on whether or not the content in question is to be blocked. Moreover, Roskomnadzor summons the Commission only if the agency decides that an expert opinion is needed (Order for the Expert Commission 2017,

paras 4–6). Thus, the blacklisting mechanism has been enlarged by adding a new administrative procedure that helps Roskomnadzor to blacklist rather than safeguards content from dangers of *ex ante* regulation.

Administrative decision-making within the blacklisting mechanism is supported by the Information System of Immediate Interaction,[6] which works automatically in a 24-hour manner (Rules on the Blacklist 2017, paras 2–4). Roskomnadzor sits in the centre of the system, accumulating signals on illegal content sent by courts, the Prosecutor Generals' Office, three federal agencies and internet users (ibid., para 5). A court can rule to blacklist any illegal content, the dissemination of which has been deemed by it a criminal or administrative offence. In contrast, the others can flag only certain types of prohibited information. The Prosecutor General's Office sends notifications about websites that contain calls for public rallies and unsanctioned public actions, as well as information on activities of extremist organisations and 'undesired' NGOs. The Ministry for Internal Affairs flags websites containing drug propaganda.[7] The Federal Service for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor) sends notifications about websites containing information on ways of committing suicide. The Federal Tax Service, finally, flags websites informing on illegal gambling.

Roskomnadzor not only accumulates and processes all notifications but also actively contributes to identifying unlawful online materials. For example, the agency filters online content for images of child sexual abuse. In addition, it monitors online content published by Russian mass media for articles advocating drugs and suicide (ibid.).

Internet users can also contribute to blacklisting. They can send notifications to Roskomnadzor directly by filling a special electronic form on Roskomnadzor's official website. According to

Alexandr Zharov (2015), from November of 2012, when blacklisting was introduced, to March of 2015, Roskomnadzor examined approximately 165,000 notifications sent by users. Zharov says that of those, two-thirds were rejected as ill-founded. Yet, notably, these figures should not be interpreted as confirming that internet users' contribution is insignificant. Bearing in mind that the number of notifications sent by users has increased from 95,600 in 2015 (Report 2015,59) to almost 140,000 in 2016 (Report 2016,64), the acceptance of only one-third of notifications means that internet users significantly contributed to blacklisting.

To illustrate how this mechanism works, let us take an example of when a user sends a notification on child sexual abuse images – the type of prohibited content that Roskomnadzor examines. In this case, the processing of this notification consists of two phases. Firstly, an official in Roskomnadzor conducts an examination within 24 hours (Temporary Regulations 2012, para 10). The official assesses whether all required information has been sent, whether the notified content may be illegal and whether Roskomnadzor has already blacklisted this content (ibid., para 12). If the official has not found the information to be illegal, he/she takes a screenshot of the notified page and attaches it to his decision to reject the notification (ibid., para 13). Secondly, if the official has assessed notified content as supposedly illegal, he/she forwards the notification for further examination to a specialist who is not an official (ibid., para 19). According to Zharov (2015), these specialists worked initially as volunteers for the League for a Safe Internet (*Liga Bezopasnogo Interneta*),[8] a voluntary organisation with a conservative profile and strong state support. Since 2014, specialists have been working for the Main Radio Frequency Centre (*Glavnyi Radiochastotnyi Tsentr*),[9] a state-owned company controlled by Roskomnadzor (Report 2015, 6). This company maintains a department consisting of 20 specialists. In 2016, this department examined more than 11,200 web pages and confirmed the

presence of child sexual abuse images in 95 per cent of the cases (Report 2016, 65). If a specialist has concluded that content is probably illegal, Roskomnadzor issues a decision on including the relevant web resource in the Blacklist.

Blocking procedures: coopted internet service providers

After including a website in the Blacklist, the blacklisting mechanism switches to the blocking phase. To implement blocking, Roskomnadzor coopts internet service providers. At first, Roskomnadzor sends an electronic notification to the relevant internet hosting provider that accommodates the blacklisted recourse. This notification contains a requirement to inform its client of the obligation to remove the banned content. If the website owner has not deleted the blacklisted content within 24 hours, a notification requires the hosting provider to remove the content or block access to it (Law 398, Article 15.1.7). Three days after sending this notification, Roskomnadzor checks whether the requirements have been fulfilled. If neither the website owner nor the hosting provider has reacted, Roskomnadzor orders internet access providers to deny internet users access to the resource (Rules on the Blacklist 2017, para 12).

Foreign hosting service providers usually do not react. Therefore, the blacklisting mechanism focuses on coopting internet access providers who are subjects of Russian jurisdiction, because they own cables and other equipment placed on the Russian soil. Roskomnadzor has involved almost 4,000 internet access providers in the Information System of Immediate Interaction. They have gone through special registration with Roskomnadzor and received access to the Blacklist (Report 2015, 61). These providers are obliged to download the Blacklist and its updates twice a day to keep up with the pace of blacklisting (Rules on the Blacklist 2017, para 13).

Roskomnadzor monitors the implementation of blocking through *Revizor*, an automated system sending access requests to websites that are expected to be blocked. If *Revizor* reveals that an

access provider has failed to block a given website, this provider, in accordance with Article 13.34 of the Code of Administrative Offences, faces significant fines, up to 100,000 roubles (approximately €14,000).

From a technological perspective, blocking provides the state with only limited control over online content. Users can still access a blocked website from abroad or even from Russia by using VPN connections or other circumvention tools. To reinforce the effectiveness of blacklisting, the government has developed legislation to bar circumvention. Federal Law No. 276-FZ (2017) obliges providers of VPN and proxy services to prevent internet users from applying circumvention methods to access banned content. In a case of non-compliance, these providers face the blocking of their online business activities in Russia. The law also obliges providers of online search engines not to display links to blacklisted and blocked websites. Thus, by coopting search engine providers, as well as providers of VPN connection and proxies, the state has significantly strengthened the technological enforcement of blocking.

The blacklisting mechanism coopts providers not only for blocking but also for making the websites available for users again. Roskomnadzor orders providers to restore access to websites only in two situations: when websites remove the banned content and when they win court proceedings against Roskomnadzor for unlawful blacklisting. According to the agency, for the first five years of applying the blacklisting practice, Roskomnadzor ordered the unblocking of almost 178,000 websites out of 275,000 blacklisted for the same period, because of the removal of banned information (Smitiuk 2017). Roskomnadzor has not provided information on how many websites have been unblocked on the basis of court proceedings. My study of cases lodged against Roskomnadzor has not revealed such examples; in other words, it revealed only examples in which website owners lost.[10] Moreover, the number of court proceedings against

blocking by Roskomnadzor is highly insignificant: namely only ten cases were filed between September 2012 and July 2018. Out of those, four cases were lodged regarding websites containing information on Aleksei Navalny, a prominent opposition political activist.[11] Therefore, the statistics and this study allow to conclude that in practice, removing the banned content is the only way to be unblocked.

If the website deletes the banned content, it sends Roskomnadzor the evidence – a screenshot – that the content in question does not exist anymore on the relevant web page (Rules on the Blacklist 2017, para 14b and 14(1)). After receiving this evidence, Roskomnadzor excludes the website from the Blacklist within three days and simultaneously informs providers, so that they can restore access to this website within 24 hours (Rules on the Blacklist 2017, para 15). Thus, coopted providers censor third-party content in both ways: by concealing the banned information from the public and by making it available again.

Among coopted providers, internet access providers might be the most severe collateral censors. They are likely to be indifferent about what content they provide to the public because they offer access to the internet as a whole, rather than to a certain website. Therefore, they are the best-placed party to censor collaterally what Roskomnadzor considers the most dangerous type of prohibited content – information relating to extremist activities (Zharov 2015). When the Prosecutor General and her deputies notify Roskomnadzor about websites containing extremist information, the agency immediately orders internet access providers to block these websites. In 2015, the Prosecutor General's Office sent 144 notifications (Report 2016, 60). In 2016, the figure increased to 193 notifications (Report 2017, 66). However, these modest figures triggered a large-scale blocking because not only the notified websites were blocked, but also their

mirrors. For instance, 193 notifications led to the blocking of almost 1,400 mirror-websites and web pages (ibid.).

This immediate blocking deprives website owners of the possibility to escape it by removing the banned content. For instance, in the case of *Grani.Ru v. Roskomnadzor*, the Prosecutor General's Office sent Roskomandzor a notification to block the website grani.ru. The Prosecutor General's Office pointed that one article, and a significant part of another, supported participation in unsanctioned public meetings. Roskomnadzor received the notification on March 13, 2014. The same day, the agency blacklisted www.grani.ru, and internet access providers blocked the website. The website owner challenged the blocking in court but lost the case.[12]

Yet, even if the website owner had won, Roskomnadzor would have unlikely ordered immediate unblocking. In such a case, Roskomnadzor would rather postpone unblocking until it receives a new notification in which the Prosecutor General's Office orders the agency to trigger the unblocking procedure. Roskomnadzor justifies its position by referring to a lacuna in the blacklist laws (Zharov 2015). Article 15.1 of the Law on Information (Law No. 139-FZ 2012) stipulates that Roskomnadzor can exclude a website from the Blacklist after receiving a court ruling. In contrast, Article 15.3 (Law No. 398-FZ 2013), which sets out the order of blocking initiated by the Prosecutor General's Office, does not contain a similar rule. As a consequence, as Zharov claims, Roskomnadzor can exclude a website only after receiving a new, unblocking notification from the Prosecutor General's Office. Although this interpretation has not yet been acknowledged as correct in court practice, it signals that the power of administrative decision-making outweighs judiciary decision-making in the blacklisting mechanism.

The manoeuvre tactic: why blacklisting does not always lead to actual blocking

Although Roskomnadzor is able to enforce blocking through coopted providers, the inclusion in the Blacklist does not necessarily lead to the blocking of a website. For instance, in 2015, only 31,000 websites out of the blacklisted 49,700 were blocked (Report 2016, 59). The main reason for such an outcome is that the banned content was removed before Roskomnadzor ordered internet access providers to block websites. It means that, for example, if Twitter removes the banned content hosted by it, Roskomnadzor excludes twitter.com from the Blacklist and does not require the blocking of this website. Yet, it is likely that Roskomnadzor will not order Twitter to be blocked even if the company fails to remove banned content. This assumption is confirmed by the fact that although Twitter complied only with five per cent of notifications[13] sent by Roskomnadzor during the period from July of 2015 to December of 2015 (Freedom House 2015), Roskomnadzor never blocked twitter.com. Roskomnadzor explains such a situation by saying that it prefers negotiations to blocking large providers (Zharov 2015). It appears that these negotiations allowed Roskomnadzor to persuade Google to comply with 75 per cent of the agency's notifications sent between July 2015 and December 2015 (Freedom House 2015). Moreover, negotiations with Twitter might be a reason why the number of fulfilled notifications has increased: from July to December 2016, Twitter complied with 28 per cent of removal requests; from July to December 2017, with 51 per cent (Twitter 2017).

The Twitter example shows that although the blacklist legislation requires Roskomnadzor to order blocking, the agency does not follow this obligation, or at least postpones its fulfilment in some cases. Instead of blocking, Roskomnadzor applies the manoeuvre tactic: by threatening to block, the agency tries to persuade website owners to delete blacklisted content. Indeed, the perspective of blocking can motivate a website to take into account Roskomnadzor's position and to edit blacklisted content. For example, on April 5, 2013, Wikipedia's article 'Smoking

cannabis'[14] was blacklisted for advocating drug usage (Rothrock 2013). Wikipedia rewrote the article in a manner required by Roskomnadzor, and consequently evaded blocking (Filonov 2013).

The manoeuvre tactic may be efficient because *ex ante* regulation places the burden on website owners to obtain a court ruling to unblock websites (Temporary Regulations 2012, para 72). Notably, challenging the blocking in courts does *not* release blacklisted content. Internet providers restore access only after receiving an entered-into-force court ruling stating that Roskomnadzor wrongly found the content in question unlawful (Temporary Regulations 2012, para 73). Thus, keeping in mind that court proceedings in Russian courts may be extremely time-consuming, legal content mistakenly or purposely blacklisted may remain inaccessible for a long time. Consequently, risk aversion may motivate a website owner to remove blacklisted content rather than to attempt to protect it. My above-mentioned survey of cases (see also note 10) confirms this assumption.

The manoeuvre tactic exposes the blacklisting mechanism as a tool of arbitrary enforcement that may first of all be aimed at political activists. Moreover, Roskomnadzor's power to decide on when, and against which, of the blacklisted websites blocking applies, in practice opens the way to corruption.

Technological weaknesses of the blacklisting mechanism

Over-blocking

Coopted internet access providers block websites in three ways: by denying a web request, firstly to a certain web page; secondly to a certain website and thirdly to a server that hosts this website. Consequently, the Blacklist contains numerical addresses of web pages (URLs), addresses of

websites (domain names) and addresses of hosting servers on which websites reside (IP addresses). Blocking on the basis of a URL or domain name presents examples of targeted blocking that leads to blocking only a blacklisted web resource. However, blocking on the basis of an IP address – non-targeted blocking – leads to blocking not only a blacklisted resource but also all other resources hosted under the same IP address on the server. This side-effect is known as over-blocking. It became evident at the very beginning of applying blacklisting practices. For instance, in December of 2012, this side-effect led to the accidental blocking of the website www.digital-books.ru (this example is discussed in more detail later). In April of 2018, when Roskomnadzor was trying to block messaging application Telegram,[15] over-blocking reportedly affected millions of websites because of blocking IP addresses connected with Google (Philipenok 2018) and Amazon (Balashova et al. 2018).

The blacklist legislation allows internet access providers to apply IP-address-based blocking, along with the options of targeted blocking, in two situations. Firstly, IP-address-based blocking may occur when Roskomnadzor includes the relevant IP address in the Blacklist after the website owner or the relevant internet hosting provider has not removed the banned content within three days. Secondly, internet access providers can apply IP-address-based blocking when Roskomnadzor immediately includes the relevant IP address in the Blacklist after receiving notifications from the Prosecutor General's Office (Rules on the Blacklist 2017, para 12).

Opinions regarding the scale of over-blocking differ. According to internet freedom advocates, more than 90 per cent of blocked websites are victims of over-blocking (Tselikov 2014, 4; Freedom House 2016 when referring to Roskomsvoboda's evaluation). In Roskomnadzor's opinion, this figure is grossly exaggerated. According to Zharov (2015), by 2015 only 1,000 owners of accidentally blocked websites contacted the agency, and only two owners filed cases

in courts. In my opinion, the scale of over-blocking must be significant. In 2014, two years after the blacklist law came into effect, Rostelecom, the largest domestic internet service provider with a 37 per cent share of the internet access market (Freedom House 2015), was able to implement only IP-address-based blocking. Rostelecom rejected the targeted-blocking options as too expensive to apply (Golytsina and Bryzgalova 2014). Thus, Rostelecom, as well as other providers applying IP-address-based blocking, over-blocked every time that other websites shared the IP address with a blacklisted website.

Over-blocking dramatically enhances effects of collateral censorship by internet access providers. Although the blacklist legislation coopts them only to censor information on blacklisted web resources, providers censor content on accidentally blocked resources as well. Yet, Roskomnadzor does not acknowledge this problem. The agency assesses over-blocking as hardly problematic because, as it claims, 70 per cent of internet access providers apply targeted blocking instead of the IP-address-based version (Zharov 2015). This figure appears unlikely because the blacklist legislation neither requires nor encourages internet access providers to prefer expensive targeted-blocking options.

Moreover, the interpretation of the blacklist legislation provided by Russian courts also allows internet access providers to apply IP-address-based blocking instead of the targeted-blocking options. Although the question of *who* should be responsible for the consequences of over-blocking is still unsolved, several court rulings have already confirmed that internet providers are non-liable for damage caused by over-blocking. For instance, in the case of *Group IB v. Rostelecom*, decided on July 10, 2014, the Moscow Court of Arbitration found Rostelecom non-liable for the accidental blocking of www.groub-ib.com. Blocking in this case targeted a website that contained information on drugs. When the owner of this blacklisted website and his hosting

provider had not removed the banned content, Roskomnadzor included in the Blacklist two relevant IP addresses. These IP addresses were then blocked by Rostelecom. This blocked 400 other websites placed on the same IP addresses, including www.groub-ib.com. The website owner, Group IB, sued Rostelecom for over-blocking and argued that the blocking in connection with a drug dealers' website caused damage to the company's reputation to the amount of 150,000,000 roubles (more than €2,000,000). However, the court rejected the applicant's claims. In the case of *V. Kharitinov*, decided on July 17, 2014, the Constitutional Court of Russia found Rostelecom non-liable for accidental blocking of the website www.digital-books.ru, containing information on electronic publications. As clarified in the case of *Kharitonov v. Russia*,[16] the website was blocked because it shared an IP address with the website www.rastaman.tales.ru. The latter contained information on cannabis. As neither the website owner nor its US-based hosting service provider, Dreamhost, had removed the content in question, Roskomnadzor placed the relevant IP address on the Blacklist. This IP address was also ascribed by the provider to the website www.digital-books.ru. As a consequence, internet providers accidentally blocked this website. The owner of the website, Vladimir Kharitonov, before referring to the Constitutional Court, challenged the over-blocking in 2013 before civil courts but lost.[17] The Constitutional Court also rejected his claims. The court stressed that it was not blacklisting that caused over-blocking, but rather the ascribing of one IP address to several websites by the hosting provider. Therefore, the issue of compensation should be decided in civil proceeding between the website owner and his hosting provider. Following the Constitutional Court's logic, the provider should have given each web resource its own IP address. However, this is impossible in practice because the number of IP addresses, presenting numerical combinations, is vast but not unlimited. At the same time, the number of web resources in need of IP addresses is constantly

growing. Consequently, hosting providers have to accommodate multiple websites under the same IP address. Thus, this decision in no way contributes to solving the problem of over-blocking. Moreover, it indirectly supports the practice of IP-address-based blocking and therefore the accidental collateral censorship.

Roskomnadzor advises owners of accidently blocked websites to change hosting provider and consequently receive a new IP address that is not on the Blacklist (Zharov 2015). However, I agree with Kharitonov (2017) who dismissed this advice and rightly emphasised that it is unjustified to place any burden to unblock information on websites that publish lawful content. Although changing a hosting provider encumbers accidentally blocked websites, changing a hosting provider appears to be the only way left for them because even the targeted-blocking options do not always prevent over-blocking. For example, when a user is surfing a website created in accordance with the secure HTTP Web protocol (HTTPS), his/her request is encrypted in such a manner that an internet provider cannot distinguish to what website or web page on the server this request is sent. Consequently, a provider is unable to apply the targeted-blocking options. A provider has to choose whether to apply the IP-address-based blocking to escape fines for under-blocking, or to find new, more sophisticated and expensive technologies to escape over-blocking. The latter is unlikely because providers are non-liable for over-blocking following *Group IB v. Rostelecom* and the case of *V. Kharitinov.*

Not only providers, but also Roskomnadzor may be uninterested in the application of more sophisticated technologies to prevent over-blocking. Indeed, the threat of over-blocking may strengthen Roskomnadzor’s manoeuvre tactic in negotiations with website owners. For instance, in March of 2015, Roskomnadzor blacklisted five web pages of Lurkmore, a humoristic online encyclopaedia, which could have caused the blocking of the entire website because it was

created in accordance with HTTPS standards. Roskomnadzor informed the website owner on the danger of over-blocking. The owner reacted by removing the blacklisted content (Khomak 2015). Thus, the technological problem of over-blocking caused by encrypting has added a new argument to Roskomnadzor's manoeuvre tactic. Nevertheless, the example of YouTube, a HTTPS-based web resource that Roskomnadzor constantly criticises for hosting prohibited content but does not block, shows that the over-blocking argument is not always persuasive.

Malicious blocking

Although over-blocking suppresses freedom of expression, this side-effect is unlikely to be capable of undermining the blacklisting mechanism as such. Rather, over-blocking highlights the point that web technologies have not been developed to enforce website blocking. While it is disputable whether or not the internet should be adjusted to website blocking or *vice versa*, another side-effect of blocking can challenge the blacklisting mechanism as an adequate regulatory tool. This is the susceptibility of the blacklisting mechanism to manipulation for malicious purposes.

One way to trigger malicious blocking is to place illegal content on a victim-website. For example, in November of 2014, an anonymous user posted information on committing suicide on www.github.com, a popular website for open source software developers. It led to the website's blacklisting and blocking on December 2, 2014. After blocking, GitHub made the banned content inaccessible for Russian internet users. Consequently, the website was excluded from the Blacklist and unblocked on December 5. Interestingly, Zharov (2015) acknowledged that the agency knew that GitHub became a victim of the malicious-blocking attack, but this understanding could not prevent blocking.

More recently, a new way of malicious blocking has been discovered (Berg 2017). It consists in attaching an IP address of a victim-website to the domain name of a blacklisted website. The procedure of attaching is simple: the owners of a blacklisted website update the information submitted when they had registered their website. This information includes the domain name and the IP address of a server on which this website is hosted. The owner just adds one or several new IP addresses of servers that are unconnected to her/his website but host victim-websites. This new information, without checking, enters WHOIS database used by Roskomandzor for blacklisting. After that, new IP addresses appear on the Blacklist and become blocked by internet access providers. In the period of May to June of 2017, this new strategy triggered a wave of malicious blocking that reportedly affected thousands of victim-websites. For instance, this wave affected the websites of Telegram, a popular online messenger; Meduza.io and Lenta.ru, popular online media outlets; as well as Wikipedia, Booking.com and, ironically, Roskomnadzor's own website (Ser'gina 2017).

Roskomnadzor reacted to this new technological problem by sending to internet service providers the so-called white lists containing IP addresses that cannot be blocked in any event (Sal'manov 2017). However, this solution is not only incapable of eliminating the problem but also shows how weak the blacklisting mechanism is from the technological perspective. The massive blacklisting and blocking machine driven by several federal agencies and thousands of internet providers stumbled when, as was reported in the press, a few human rights activists used the same internet technologies on which the blacklisting mechanism relies to undermine it.

Conclusion

This chapter has provided new insight into the relationship of censorship, legality and technology in contemporary Russia. This relationship is affected by new-school forms of regulation. The

blacklisting mechanism, a tool of new-school regulation, has made content regulation more efficient. The mechanism has enabled the state to coopt internet providers to collaterally censor online content. The extensive and well-developed system of administrative procedures regulates online content *ex ante* and without preliminary court oversight, which brings the danger of politically motivated blocking. This danger is caused not only by vague legal definitions, in particular extremism, as suggested in previous research, but also by the manoeuvre tactic applied by Roskomnadzor selectively, as discussed in this chapter. Moreover, this chapter brings to the fore new threats rooted in blocking technologies – over-blocking and malicious blocking. Lawful content suffers from over-blocking because internet service providers apply IP-address-based blocking instead of making a certain web page inaccessible. Consequently, they block all websites sharing the same IP address. Furthermore, even when internet providers apply targeted blocking of web pages, providers have to switch to IP-address blocking because they cannot see to what HTTPS web page a user sends a request for access. As the web address in these requests is encrypted by HTTPS technologies, providers have to block access to the relevant IP address, thereby making all content placed on it unavailable. Additionally, almost every website may become a victim of malicious blocking. This may occur because a user has purposely published unlawful content or because the owner of a blocked website has deceived the blacklisting mechanism by misinforming providers that the IP address of the victim-website is also shared by this blocked website.

These side-effects not only have surpassed the intentions of the legislator but also have undermined the efficiency of the blacklisting mechanism. The fundamental flaws of the mechanism were once again highlighted by the extensive collateral damage caused by Roskomnadzor's attempt to block Telegram in April 2018. Fixing the blacklisting mechanism

requires the Russian government to change the very internet technologies on which website blocking relies. This change is highly difficult to implement because these internet technologies are controlled not by Russia but by the global internet community, including, for instance, the Internet Engineering Task Force (IETF) and the Internet Society. The absence of national control over global internet technologies as well as costs and limitations of the blacklisting mechanism may put the future of website blocking in doubt. If the Russian government finds that the blacklisting mechanism is no more inefficient to regulate online content, the government might shift to other approaches. For instance, it may intensify pressure on internet hosting providers, such as VKontakte.

References

Balashova, Anna, Mariia Kolomychenko, and Ivan Kuranov. 2018. "Popal Pod Razdachu: Kak iz-za Telegram v Rossii Blokiruiut Adresa Amazon." *RBK*, 16 April. https://www.rbc.ru/technology_and_media/16/04/2018/5ad4b5c59a794739885fa03a.

Balkin, Jack M. 2014. "Old-School/New-school Speech Regulation." *Harvard Law Review* 127, no. 8: 2296–2342.

Berg, Evgenii. 2017. "Aktivisty Vospol'zovalis' Uiazvomost'iu v Rabote Roskomnadzora i Teper' Blokiruiut Chuzhie Saity. Kak Eto Ustroeno?" *Meduza.io*, 9 June. https://meduza.io/feature/2017/06/08/aktivisty-vospolzovalis-uyazvimostyu-v-rabote-roskomnadzora-i-teper-blokiruyut-chuzhie-sayty-kak-eto-ustroeno.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Drezner, Daniel W. 2010. "Weighing the Scales: The Internet's Effect on State-Society Relations." *Brown Journal of World Affairs* 16, no. 2 (Spring/Summer): 31–44.

Favret, Rebecca. 2013. "Comment: Back to the Bad Old Days: President Putin's Hold on Free Speech in the Russian Federation." *Richmond Journal of Global Law & Business* 12 (Spring): 299–315.

Filonov, Dmitrii. 2013. “Stat’ia iz Vikipedii o Kurenii Marikhuany Budet Iskliuchena iz ‘Chernogo Spiska’.” In *RAPSI-Russian Legal Information Agency*, April 8. rapsinews.ru/incident_news/20130408/266952801.html.

Freedom House. 2015. “Freedom on the Net 2015, Russia.” https://freedomhouse.org/report/freedom-net/2015/russia.

Freedom House. 2016. “Freedom on the Net 2016, Russia.” https://freedomhouse.org/sites/default/files/FOTN%202016%20Russia.pdf

Golytsina, Anastasiia, and Ekaterina Bryzgalova. 2014. “Interv’iu – Aleksandr Zharov, Glava Roskomnadzora.” *Vedomosti*, 1 August. https://www.vedomosti.ru/newspaper/articles/2014/08/01/zablokirovat-informaciyu-v-internete-navsegda-nevozmozhno.

Jackson, Camille. 2016. “Legislation as an Indicator of Free Press in Russia.” *Problems of Post-Communism* 63, no. 5–6: 354–366.

Kharitonov, Vladimir. 2017. “Tochka.” Interview by Aleksandr Pliushchev. *Ekho Moskvy*, 17 September. Audio, 12:48. https://echo.msk.ru/sounds/2056054.html.

Khomak, Dmitrii. 2015. “Sozdatel’ ‘Lukomor’ia’ Obvinil Roskomnadzor v Shantazhe.” *Meduza.io*, March 10, 2015. https://meduza.io/news/2015/03/10/sozdatel-lurkomorya-obvinil-roskomnadzor-v-shantazhe.

Lessig, Lawrence. 2006. *Code Version 2.0*. New York: Basic Books.

Nocetti, Julien. 2015. “Russia’s ‘Dictatorship-of-the-Law’ Approach in Internet Policy.” *Internet Policy Review* 4, no. 4: 1–19. https// doi.org 10.14763/2015.4.380.

Philipenok, Artem. 2018. “Pol’zovateli Soobstchili o Problemakh s Dostupom k Google v Rossii.” *RBK*, 22 April. https://www.rbc.ru/society/22/04/2018/5adbbb5e9a79470489910377.

Roskomnadzor. 2015. “Report (2015) by Roskomnadzor for 2014.” https://rkn.gov.ru/docs/doc_1240.pdf.

Roskomnadzor. 2016. “Report (2016) by Roskomnadzor for 2015.” http://rkn.gov.ru/docs/docP_1485.pdf.

Roskomnadzor. 2017. “Report (2017) by Roskomnadzor for 2016.” https://rkn.gov.ru/docs/doc_1646.pdf.

Rothrock, Kevin. 2013. "Wikipedia's Suicide Mission against Russian Censors." *Global Voices*, Posted 9 April 2013. Accessed 10 October 2018. https://advox.globalvoices.org/2013/04/13/wikipedias-suicide-mission-against-russian-censors/.

Sal'manov, Oleg. 2017. "Roskomnadzor Razoslal Belye Spiski Saitov." *Vedomosti*, 9 June. https://www.vedomosti.ru/technology/blogs/2017/06/09/693751-belie-spiski-saitov.

Ser'gina, Elizaveta. 2017. "Roskomnadzor Zapodozril Politicheskikh Aktivistov v Organizatsii Lozhnykh Blokirovok." *Vedomosti*, 15 June. https://www.vedomosti.ru/technology/articles/2017/06/15/694430-roskomnadzor-lozhnih-blokirovok.

Smitiuk, Iurii. 2017. "Roskomnadzor za Piat' Let Zablokiroval okolo 275 tys. Resursov s Zapreshchennoi Informatsiei." *TASS*, 27 July. http://tass.ru/politika/4445476.

Tselikov, Andrey. 2014. *The Tightening Web of Russian Internet Regulation*. Cambridge, MA: The Berkman Klein Center for Internet & Society at Harvard University.

Turovsky, Daniil. 2015. "Kak Ustroen Roskomnadzor." *Meduza.io*, 13 March. https://meduza.io/feature/2015/03/13/kak-ustroen-roskomnadzor.

Twitter. 2015. "Transparency Report. Removal Requests – July to December 2015." https://transparency.twitter.com/en/removal-requests.html.

Twitter. 2017. "Transparency Report. Russia Removal Requests." https://transparency.twitter.com/en/countries/ru.html.

Yandex Official Blog. 2012. "O Zakonoproekte No. 89417-6." Posted 10 July. Accessed 10 October 2018. https://www.yandex.ru/blog/company/48073.

Zharov, Aleksandr. 2015. "Rossiia 24: Interv'iu Rukovoditelia Roskomnadzora Aleksandra Zharova Telekanalu 'Rossiia 24'." Interview Published on the Official Website of Roskomnadzor, Text, 11 March. http://rkn.gov.ru/press/interview/news30896.htm.

International materials cited

Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 1953.

General Policy Recommendation no. 15 on Combating Hate Speech adopted by the European Commission against Racism and Intolerance (the ECRI) on December 8, 2015.

The Shanghai Convention on Combating Terrorism, Separatism and Extremism of 2001.

Russian laws cited

Federal Law No. 114-FZ of 2012.

Federal Law No. 139-FZ of 2012.

Federal Law No. 398-FZ of 2013.

Federal Law No. 276-FZ of 2017.

Federal Law No. 327-FZ of 2017.

Order on the Unified Information System (2015) "O poriadke funktsionirovaniia informatsionnoi sistemy vzaimodeistviia." Adopted by Roskomnadzor's Order N 912 of 12.08.2013 and amended by Order 47 of 13.05.2015.

Order for the Expert Commission (2017) "Poriadok deiatel'nosti ekspertnoi komissii po voprosam priznaniia informatsii zhapreshchennoi k rasprostraneniiu na territorii Rossiiskoi Federatsii." Adopted by Roskomnadzor's Order N 161 of 16.08.2017.

Regulations on Roskomnadzor (2012) "Polozhenie o federal'noi sluzhbe po nadzoru v sfere sviazi, informatsionnykh tekhnologii i massovykh kommunikatsii." Adopted by Russian government's Order N 228 of 16.03.2009 and amended by Order N 1100 of 26.10.2012.

Rules on the Blacklist (2017) "Pravila sozdaniia, formirovaniia i vedeniia edinoi avtomatizirovannoi informatsionnoi sistemy 'Edinyi reestr domennykh imen, ukazatelei stranits saitov v informatsionno-telekommunikatsionnoi seti 'Internet' i setevykh adresov, pozvoliaiushchikh identifitsirovat' saity v informatsionno-telekommunikatsionnoi seti 'Internet,' soderzhashchie informatsiiu, rasprostranenie kotoroi v Rossiiskoi Federatsii zapreshcheno." Adopted by the Russian government's Order N 1101 of 26.10.2012 and amended by Order N 320 of 21.03.2017.

Rules for the Federal Agencies (2017) "Pravila prinyatiia upolnomochennymi pravitel'stvom Rossiiskoi Federatsii federal'nymi organami ispolnitel'noi vlsasti reshenii v otnoshenii otdel'nykh vidov informatsii i matetialov, rasprostraniaemykh posredstvom informatsionno-telekommunikatsionnoi seti 'Internet,' rasprostranenie kotorykh v Rossiiskoi Federatsii zapreshcheno." Adopted by Russian government's Order N 1101 of 26.10.2012 and amended by Order N 320 of 21.03.2017.

Temporary Regulations (2012) "Vremennyi reglament ispolneniia gosudarstvennoi funktsii sozdaniia, formirovaniia i vedeniia edinoi avtomatizirovannoi sistemy Edinyi reestr domennykh imen, ukazatelei stranits saitov v informatsionno-telekommunikatsionnoi seti

‘Internet’ i setevykh adresov, pozvoliaiushchikh identifitsirovat’ saity v informatsionno-telekommunikatsionnoi seti ‘Internet,’ soderzhashchikh informatsiiu, pasprostranenie kotoroi v Rossiiskoi Federatsii zapreshcheno.” Adopted by Roskomnadzor on 01.11.2012.

Case law cited

Grani.Ru v. Roskomnadzor. Tagansky District Court of Moscow City, Case No. 2-1343/2014, Judgment adopted 6 May 2015.

Group IB v. Rostelecom. Court of Arbitration of Moscow City, Case No. A40-13859-14, Judgment adopted 10 July 2014.

Kharitonov v. Russia. Application no. 10795/14, still pending before ECtHR.

Mariya Alekhina and Others v. Russia. Application no. 38004/12, decided by ECtHR on 17 July 2018.

V. Kharitinov. Constitutional Court of Russian Federation, Ruling No. 1759-0/2014, adopted 17 July 2014.

[1] The official name of the register is: *Edinyi reestr domennykh imen, ukazatelei stranits saitov v informatsionno-telekommunikatsionnoi seti “Internet” i setevykh adresov, pozvoliaiushchikh identifitsirovat’ saity v informatsionno-telekommunikatsionnoi seti “Internet,” soderzhashchikh informatsiiu, pasprostranenie kotoroi v Rossiiskoi Federatsii zapreshcheno*. In the text, the register is referred to as Blacklist, *Chernyi Spisok* in Russian.

[2] According to the Shanghai Convention, which Russia ratified in 2010, extremism ‘is an act aimed at seizing or keeping power through the use of violence or at violent change of the constitutional order of the State, as well as a violent encroachment on public security…’. Russian laws do not contain a general definition of extremism. Instead, Section 1(1) of Federal Law No. 114-FZ (2012) provides for a list of 13 extremist activities which appears to broaden the scope of the concept. For instance, the law prohibits ‘making a public, knowingly false accusation against individuals holding a state office of the Russian Federation’. This approach has been criticised by the European Commission for Democracy through Law (the Venice Commission). For more information on legal definitions of extremism and concerns expressed by the Venice Commission, see the case *Mariya Alekhina and Others v. Russia*, paras 90–102.

[3] The way extremism is interpreted appears to share characteristics with the concept internationally referred to as hate speech. Hate speech is ‘the advocacy […] of the denigration, hatred or vilification of a person or group of persons […] on the ground of “race”, colour, descent, national or ethnic origin, age, disability, language, religion or belief, sex, gender, gender identity, sexual orientation and other personal characteristics or status’ (ECRI General Policy Recommendation 2015). This definition is close to an extremist activity defined by Section 1(1) of Federal Law No. 114-FZ (2012) as ‘propaganda about the exceptional nature, superiority or deficiency of persons on the basis of their social, racial, ethnic, religious or linguistic affiliation or attitude to religion’.

[4] See also indicative figures in annual reports by Roskomnadzor.

[5] 'Recreated' content means that the content as a whole or part of it has been copied and published on another website. 'Mirrored' content means that the copy of an entire blacklisted website has been created under a new domain name.

[6] The official name of the system is: *Avtomatizirovannaia informatsionnaia sistema priema i obrabotki soobshchenii o protivopravnom kontente*. It works in the following manner. When courts or three federal agencies have sent all necessary information, Roskomnadzor includes the relevant website on the Blacklist within 24 hours (Rules on the Blacklist 2017, para 9). Yet, when the Prosecutor General's Office sends a notification, Roskomnadzor includes a notified website on the Blacklist immediately, although after checking whether notified content is still present on a page indicated in the notification (Order on the Unified Information System 2015, para 37). The process is different if an internet user sends a notification. In those cases, Roskomnadzor can add a notified website on the Blacklist only after examination. Who conducts this examination depends on the type of content placed on a notified website. If this type falls under competence of one of the federal agencies, Roskomnadzor forwards a notification to the relevant agency within 24 hours via the Special Information System of Immediate Interaction (Temporary Regulations 2012, paras 14, 17). The relevant agency is obliged to respond within 24 hours (Rules on the Blacklist 2017, paras 7, 8). When a positive assessment from the relevant agency has come, Roskomnadzor adopts a decision on including in the Blacklist within 24 hours (Temporary Regulations 2012, paras 23, 25).

[7] This function was executed by the Federal Drug Control Service until November 15, 2016.

[8] See also the organisation's website at http://www.ligainternet.ru/.

[9] See also the organisation's website at http://www.rfs-rf.ru/grfc/.

[10] I have studied cases lodged with Tagansky District Court of Moscow. This court corresponds to the place of Roskomnadzor's domicile and consequently decides on claims regarding unlawful blocking. The case-study was conducted on July 25, 2018 by making searches in two databases: the databases on the website of the Court of Moscow City and the database on the website www.consultant.ru. The study revealed ten cases: (1) regarding accidental blocking of digital-books.ru, decided on July 19, 2013; (2) blocking of grani.ru by the court ruling of May 6, 2015; (3) blocking of vulcanoclub.com for illegal gambling by the court ruling of October 12, 2015; (4) blocking of magister.msk.ru for extremist materials by the court ruling of March 20, 2015; (5) blocking of golosislama.com for extremist materials (the date of the court ruling is concealed by the document); (6) four cases regarding blocking information connected with Navalny's activities (see note 11); and (7) the court ruling in the case lodged by Panova (the name of the website and dates of proceeding are concealed in the document).

[11] These cases include, first, the case lodged by Navalny and decided on February 18, 2015 (the name of the blocked website is concealed in the document); second, the case lodged by Mediafocus regarding blocking of mirrored content on pages placed on facebook.com and ej.ru (the date of the court ruling is concealed in the document); third, the case decided on February 20, 2018 regarding blocking of navalny.com; fourth, the case decided on February 26, 2018 regarding blocking of two pages of znak.com for information on Navalny's activities.

[12] Tagansky Raionnyi Sud goroda Moskvy, Delo No. 2-1343/2014, May 6, 2015.

[13] According to Twitter (2015), the company withheld content promoting suicide and materials published by Right Sector, an organisation involved in the war against pro-Russian forces in Ukraine. Yet, the company did not follow notifications regarding, for instance, the Charlie

Hebdo Twitter account, Tweets supporting Pussy Riot, Tweets linking to YouTube videos disapproving of the Russian government.

[14] *'Kureniie kannabisa'.*

[15] On April 16, 2018, a court ordered to block Telegram, a popular messenger, due to incompliance with anti-terrorist legislation known as 'Iaarovaia's Law'. To evade blocking, the company started changing IP addresses connected to the servers of companies such as Google and Amazon. As not only Telegram, but other websites used the same IP addresses, accidental blocking caused an avalanche of collateral damage. Yet, because the Telegram blocking was implemented on a legal basis other than the blacklisting mechanism analysed in this chapter, the Telegram example is not discussed in detail.

[16] *Kharitonov v. Russia,* Application no. 10795/14, still pending in June of 2018 before the European Court of Human Rights.

[17] On July 19, 2013, Kharitonov lost in Taganskiy District Court of Moscow. On September 12, 2013, Moscow City Court dismissed his appeal. The courts stated that Roskomnadzor did not breach the blacklist legislation and therefore was not liable for over-blocking.