Internet Freedom 2019: The 'Fortress' Plan

The special plan 'Fortress' is the fundamental organisational and legal document concerning the security and defence of Ministry of Interior (MoI) buildings. The plan must set out three scenarios for defending and repelling attacks on each MoI building.

Annex 1 to Order of the MoI of Russia No 174dsp of 26 February 2002 'Instruction on the organisation of the activities of on-duty units within the system of MoI.

The central topic of this report — drawn up by the *International Human Rights Group Agora* and the public organisation *RosKomSvoboda* — is the interference in the freedom of the Internet in Russia during 2019. This high-level overview is based on the results from the monitoring which we have been conducting on a regular basis since 2008.

The report consists of two main sections: the first one describes the authors' assessment of the Web freedom situation, while the second section presents the results from our monitoring and illustrates them with the most rampant examples. The Annex summarises the monitoring results in tabular form, including date, source, region and nature of interference in each known episode. Readers can also see a colour-coded map which provides a bird's glance on the relative level of Internet freedom across the entities of the Russian Federation.

Methodology

The monitoring results which form the basis of this report include all instances of *interference* in the freedom to receive and disseminate information on the Internet which have become known to the authors from open sources (official reports of government institutions, expert assessments, publications in mass media, blog posts, and statements of users and owners of Web resources).

Our starting point is the belief that unobstructed access to censorship-free Internet is a fundamental human *right*, and it is incumbent on the State to ensure that everyone can freely disseminate and obtain information and ideas throughout the Web. We acknowledge that freedom of expression is not absolute and, in accordance with the Russian Constitution and with the European Convention on Human Rights, it can be limited as long as each such limitation satisfies 'the triple test': it must be provided for in legislation which is reasonably clear, adequately accessible and sufficiently foreseeable, it must pursue a legitimate aim and must be necessary in a democratic society.

We consider it necessary to stress that the monitoring exercise does not include an assessment of the *lawfulness* of the interference detected. Thus, our monitoring results have captured a wide variety of situations, including shutdowns of social media accounts which feature terrorist content, censoring of politically and socially oriented media, criminal prosecution of users for their activity in the Web, detention of streamers and online journalists during public rallies as well as *any* other acts of the authorities which ultimately impede the reception or dissemination of online information.

What we consider outright *violations* of Internet freedom, which are non-excusable and the ultimate responsibility for which is always imputable to the State, are acts of intimidation and violence targeted against users, bloggers, journalists and owners of web resources.

The authors believe that the classification system developed in previous years is highly informative and have consequently used the same scheme in the present report while adding two new categories: 'Government-led internet shutdowns' and 'Pressure on IT businesses and software developers'. The summary table includes also instances of threats and violence related to the web-based activity of the victims, criminal prosecutions, various forms of administrative pressure (warnings from a public prosecutor, demands to delete or edit comments) as well as cases of

administrative liability, judicial or institutional prohibition of information or restriction of access to the Internet on the initiative of the authorities, and cyberattacks. Occurrences not falling in either of these categories come under the 'Miscellaneous' heading. A necessary caveat is that the 'Criminal prosecution' heading includes not only indictments and sentences, but also cases where there are serious reasons to assume that the person concerned will incur criminal liability, such as house searches, arrests, interrogations or similar procedural activities carried out in the context of an initiated criminal procedure. Sentences to effective imprisonment are highlighted as an individual reporting item.

That said, it is obvious that imposition of criminal liability in the form of imprisonment or hefty fine is much more serious that the removal by the social media administrator of a group consisting of just a few users. Nonetheless, due to the impossibility to assign unequivocal value to each particular restriction, we decided to not apply value factors and did our monitoring on basis of the principle 'one incident — one rating point'.

It should be borne in mind that a single individual or a single website may become subject to two or more restrictive measures. For example, an Internet user may be held criminally liable for a blog post, his or her post can be proscribed as a prohibited one and the website can end up in the register maintained by Roskomnadzor. In this scenario, we report three separate instances of restriction of Internet freedom insofar as each of these measures has its distinct consequences which, more often than not, concern various persons or entities.

Having regard to the global nature of the Internet, it is difficult to single out the Federation entity responsible for a particular restriction. Where a particular event can be unequivocally tied to a particular region (headquarters of the editorial board of a regional media outlet, place of residence of the website owner or of the user on whom liability is imposed), we have entered the relevant entity of the Federation in the monitoring database. Accordingly, the total number of Internet freedom restrictions shown on the map is significantly lower than the total number appearing in the bottom-line of the summary table.

In doing so we have endeavoured to take into account the place at which the decision that led to restriction of Internet freedom was taken. Where a court in one entity of the Federation rules that a web page must be prohibited, all Internet Service Providers (ISPs) across Russia become obligated to block that web page. What matters to us however is that the

prohibitive decision was made in the particular region. On the other hand, legislative initiatives, which will have an impact across the entire country, or demands to block a web resource raised by federal agencies, have been included in the summary table without a reference to a particular region.

Our monitoring also captures reported restrictions of freedom on the Internet in Crimea, including Sevastopol, inasmuch as the territory of the peninsula is de facto controlled by the Russian authorities which makes them responsible for upholding human rights and freedoms in that territory.

In drafting the present report, besides the results of our own monitoring, the authors consulted the database of SOVA Center for Information and Analysis which contains details of sentences for crimes involving extremist activities. Other resources used include the web portal of the Russian judicial system (ГАС «Правосудие»), official reports of the Roskomnadzor as well as websites of the Ministry of Justice, of the Office of the Prosecutor General of Russia and of the prosecution services of Federation entities.

Overview

According to statistics compiled by the research company Mediascope, in the spring of 2019 the monthly average headcount of Runet audience reached 93 million. The growth of the audience was mainly driven by mobile Internet users and users in senior age groups. This accounts for 76 % of the national population aged 12 years or more.

One year later, in January 2020, the research company GfK reported that the number of active Web users already stood at 94.4 million, meaning that the Web audience had once more grown by as many as three million users.

The .ru domain continued to shrink in 2019, this time by more than 60,000 domain names and reached 4,951,205 names (the decline continued in 2020).

Russia weakened its position in the Speedtest Global Index, an indicator which is published by Ookla on a monthly basis and measures the speed of Web access, retreating to 46th (previously 43th) in the Fixed Broadband category and to 96th (previously 77th) in the Mobile Broadband category. In both cases however the bitrates increased — by 45.01 to 60.71 Mbps and respectively by 19.04 to 20.58 Mbps.

Withal, the cost of access to the Interner in Russia is among the lowest in the world as the country ranks second only after Ukraine (USD 0.08/month per 1 Mbps), and the coverage of 4G networks is above 60%.

The Russian authorities are making serious efforts to develop IT technology, provide more e-government services and make the Internet more accessible to citizens. Although the budget of the Digital Economy programme has been reduced, Web connectivity continues to expand in social establishments such as schools, paramedic/midwifery stations, and fire-fighting units. The official Public Services Portal launched the first prototypes of the so-called superservices which are expected to increase the scope of e-government services. These include Justice Online, Employment Online, Business Licences Online, Digital Enrollment in Universities, etc.

On the other side, in 2019 international human rights organisations again saw further tightening of Internet censorship and aggravated situation of journalists.

Thus, in the World Press Freedom Index published by Reporters Without Borders (RSF), besides dropping down from 148th to 149th position among 180 countries, Russia deteriorated its rating by 0.34 points. According to the RSF, the situation in Russia is worse than that in Venezuela, Cambodia and Palestine, but better than in countries such as Belarus, Turkey and Azerbaijan.

According to the annual report 'Freedom on the Net 2019: The Crisis of Social Media' drawn-up by Freedom House, with its 31 points out of 100 Russia remains, for the fifth consecutive year already, in the group of 21 countries listed as worst abusers of Internet freedom, together with China, Saudi Arabia, Cuba and Sudan. Freedom House experts make a particular reference to blocked social media, ISPs and websites, to the activity of pro-government commentators and to arrests of users in Russia.

Our conclusion is that the overarching course of action aimed at the establishment of total control by the State on Web information, users and media remains unabated. New laws concerning 'isolation of the Runet', 'fake news' and 'disrespect to the authorities' have come into force. Time and again, senior officials threaten to block VPN services, Twitter and Facebook and even to 'conclusively deal with the Telegram issue'.

The isolationist intents of the Russian authorities were clearly revealed in several new trends which gathered momentum in 2019. First and foremost,

the past year saw further proliferation of politically motivated shutdowns[*] at regional and local level as well as stronger pressures on IT businesses and software developers, as particularly seen in several criminal procedures waged against Internet entrepreneurs. Another notable event was the first censoring of a video game in the history of the Runet.

One isolationist technique is coercing the owners global Web platforms into collaboration with the authorities. In our previous report we suggested that the Web policy of the State may be at a fundamental turning point as the authorities would seek to establish control on large actors who have access to data about their users and are able to effectively rein the dissemination of information.

Withal, the authorities do not intend to abandon the existing policy of persecuting those who actually disseminate information. Overall, it may be asserted that while repressions in the Runet have become less ubiquitous, now they are more severe and better targeted. The threat looms on the most outspoken critics and opponents of the authorities, prominent persons, civil-society activists and, as it transpired, on successful IT entrepreneurs.

Furthermore, prosecutions may not necessarily be linked directly to activities in the Internet, instead they can be used just as a formal pretext for intimidation and collection of intelligence. Examples include searches conducted at the homes of family members of Alexander Gorbunov, host of the Telegram channel StalinGulag and holder of same-name accounts in Twitter and Instagram.

On the other side, the Internet community also demonstrates solidarity and commitment, and not only in strictly professional matters but also in issues of broad public concern. For example, a petition supporting the defendants in so-called 'the Moscow Case' (criminal prosecution of participants in a peaceful rally held in the summer of 2019 in Moscow) published on the largest hosting service for IT projects Github has, at the time of writing, gathered more than 2000 signatures.

The amendments to the Russian Criminal Code (RCC) made in the end of 2018 virtually put an end to the application of Article 282 RCC which in recent years has been a major tool for political repression. The introduction

[*] Government-led internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location. Typically, it is applied for the purpose of obtaining control over the flow of information// https://www.accessnow.org/keepiton/

of administrative precedence in extremism-related cases and the addition of new provisions in the Code of Administrative Offences (CoAO) restructured the State policy in this area and led to a more clear demarcation of the areas of influence of the various law enforcement authorities.

In 2019 the European Court of Human Rights (ECHR) delivered its first assessment concerning the blocking of websites in Russia and questioned the lawfulness of the practices established in the country. In its judgment in Kablis v Russian Federation the ECHR held that there had been a violation of the right to freedom of expression and of the right to peaceful assembly in the form of blocking the account and the personal blog of Grigoriy Kablis, a fellow at the Institute of Geology of the Komi Science Center of the Russian Academy of Sciences, following his posting of a notification of a picketing action (vigil) dedicated to criminal proceedings against high-ranking officials of Komi Republic. In particular, the ECHR held that the provisions of Russian domestic law which set out the procedure for extrajudicial blocking of websites do not provide sufficient guarantees against abusive practices.

Results of the Monitoring

*In 2019 we identified **438,981** instances of interference with freedom of the Internet in Russia, the overwhelming majority of which (434,275), similar to previous reporting periods, relate to restriction of access to websites and web services, or to prohibition of information on various grounds.*

In 2018 we counted 662,842 incidents, including 426,000 disruptions of web resources which, according to expert estimates, were caused by attempts of the Russian authorities to restrict Telegram Messenger by blocking the IP addresses of the major cloud service providers.

The level of violence remains persistently high. In 36 of the 57 identified instances of assaults or threats, the victims were representatives of mass media and the assailants were law-enforcement officers or security staff.

For example, journalists covering mass protest rallies in Moscow and Saint-Petersburg in the summer of 2019 experienced mass violence from law-enforcement officers. The Trade Union of Journalists and Media Workers reported at least 24 arrests of journalists at the Moscow rally on 27 July, including 9 arrests involving violence.

Type of restrictions	2016	2017	2018	2019
Homicide	0	1	0	0
Violence (threat to safety)	50	66	59	↓ 57
Regulatory proposals	97	114	82	↓ 62
Criminal prosecution/ effective imprisonment	298/32	411/48	384/45	↓ 200/38
Administrative pressure	53,004	22,523	4402	↓ 3,917
Impediment of access to web resources	35,019	88,832	488,609	↓ 161,490
Information banned by State actors*	24,000	2196	161,171	↑ 272,785
Cyberattacks	122	15	20	↑ 32
Lawsuits	170	39	58	↑ 79
Government-led Internet Shutdowns	Not reported			8
Pressure on IT businesses and software developers				12
Miscellaneous	3343	1509	8057	↓ 339
	116,103	115,706	662,842	438,981

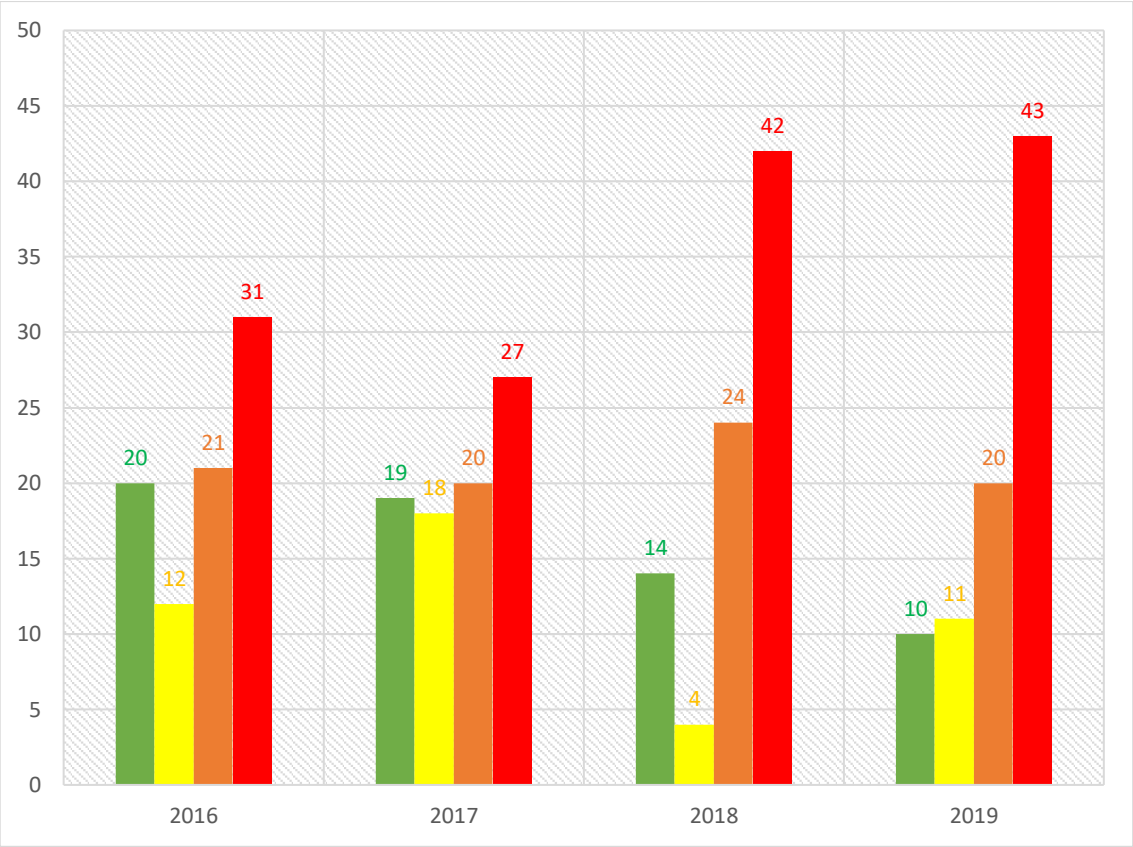
There has been a slight increase of the number of Federation entities where users experienced serious pressure: 43 regions fell in the 'red zone' in 2019 (against 41 in 2018).

Serious impairment of the situation was observed in the regions of Archangelsk, Volgograd, Kaliningrad, Kurgan, Leningrad, Murmansk, Novosibirsk, Rostov, Samara, Saratov and Tambov as well as Bashkortostan, Ingushetia, Karelia, Mordovia, Northern Ossetia and Udmurtia. In these

*Since official Roskomnadzor statistics for the fourth quarter of 2019 were not available at the time of writing, the columns of the summary table include the number of entries in the registers of prohibited information and of the administrative penalties imposed on communication operators in the first nine months of 2019.

regions, the overall number of incidents rose by more than 4 times compared to 2018 and included use of violence against journalists/bloggers or imprisonment sentences for Internet activity.

A relative improvement of the situation was observed in Komi, Khakasia, Chuvasia, Krasnodar and Krasnoyarsk territories, in the regions of Kaluga, Kirov, Pskov, Ryazan, Sakhalin, Smolensk, and in the autonomous circuits of Khanty-Mansiysk and Yamalo-Nenetsk. The number of registered incidents in these regions decreased and instances of violence or imprisonment were not reported.



During the reporting period, use of violence or threats related to the exercising of right to freedom of expression in the Internet were identified in 20 regions (Belgorod, Irkutsk, Kostroma, Leningrad, Magadan, Moscow, Murmansk, Novosibirsk, Omsk, Penza, Saratov, Sverdlovsk, Tver, Moscow and Saint-Petersburg, and Ingushetia, Krasnodar, Stavropol and Khabarovsk), and in the territory of the Crimean Peninsula.

Imprisonment sentences for Internet activity in 2019 were delivered by courts in 18 Federation entities (Amur, Belgorod, Vladimir, Vologda, Kemerovo, Kursk, Magadan, Novosibirsk, Orenburg, Rostov, Samara,

Sverdlovsk, Tomsk and Chelyabinsk oblast, Moscow, Ingushetia, Perm and Khabarovsk), as well as in Crimea.

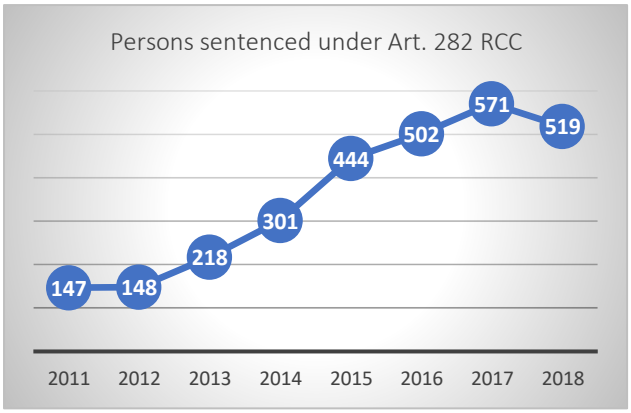
The number of regions in the 'green' zone declined for the fifth consecutive year, almost by one-third in 2019 compared to 2018 (from 14 to 10). Thus, the only regions which remained relatively free in the previous period were Chukotka Autonomous District, Jewish Autonomous District, Sakhalin and Ryazan oblast, Kamchatka territory and the Republics of Khakasia, Tyva, Komi, Karachay-Cherkessia and Kalmykia.

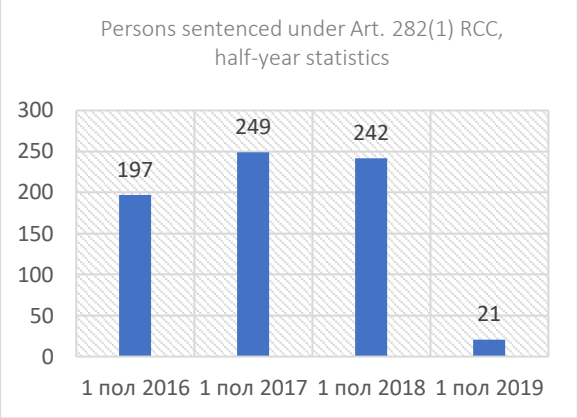
Nine subjects of the Federation (Irkutsk, Moscow, Omsk and Saratov region, Saint-Petersburg and Moscow City, Altay, Krasnodar and Primorskiy territory) have been firmly anchored in the 'red' zone since 2015. In Moscow City, Irkutsk and Moscow region instances of violence targeting web activists and online media journalists have been identified in each and every year, while in Saint-Petersburg there have been such instances in four consecutive years.

Persecution of Users

The past year saw a major decrease of criminal prosecution related to Internet activity — the number of cases dropped down to 200 incidents from 384 in 2018. However, there was a marginal decrease in the number of sentences to effective imprisonment (from 45 to 38), which in our opinion indicates that repressions are now more differentiated and law enforcement practices are being accommodated to the changing situation. On the other side, the new articles added to the Code of Administrative Offences (CoAO), in particular those related to disrespect to the authorities, publication of fake news and incitement of hatred, are already used effectively and the combined number of proceedings under these articles is comparable to the peak of anti-extremist criminal cases.

A key factor for this development was the partial decriminalization of Art. 282 of the Russian Criminal Code. As a result, this provision essentially is not used anymore and the number of cases has dropped by nearly 10 times: according to statistical data published by the Judicial Department of the Russian Supreme Court, in 2018 there were 519 sentences under Art. 282 (including 505 under paragraph 1), while in the first half of 2019 the sentences under that article were as little as 27 (21 under paragraph 1).





One of the seldom applications of Art. 282 in 2019 was in the case of *Vladislav Sinitsa*, an active participant in the summer protest rallies held in Moscow. Besides the protests as such, in social media at that time there was much discussion over some new tactics used by combatants of the National Guard and police forces: they were hiding their faces behind tinted helmets and were not wearing identification badges. In response to the obvious intent of law enforcement services to anonymity those of their members who apply violence to demonstrators, journalists and passers-by, civic activists initiated several de-anonymizing projects (the most popular one is an anti-corruption project known as Scanner) in order to collect evidence and report these crimes to law enforcement services and courts. The activists analysed photographs of law enforcement personnel taken during the rallies and matched them to open accounts in social media.

Four days after Sinitsa criticized a Twitter post made by a pro-government commentator, he was arrested and charged with incitement of hatred and with making violent threats to the social media group of 'law enforcement officers'. One month later Sinitsa was sentenced to five years of imprisonment. State mass media offered apple coverage of the case stressing that opposition activists call for assaulting the children of law enforcers. Furthermore, the federal TV channel NTV aired a video entitled

‘Opposition blogger encourages killing the children of National Guard personnel’.

As a general rule, courts impose additional penalties on activists charged with crimes by banning them from the Internet. Another defendant in the Moscow Case, *Egor Zhukov*, a student at the Higher School of Economics, received a suspended sentence of 3-year imprisonment for calls to extremism – in his YouTube video blog Zhukov offered reflections on non-violent methods to fight dictatorships. In addition, he was barred from administrating websites for two years. It is remarkable that Sinitsa, who was sentenced on charges for making violent threats on Twitter, was not banned from the Internet.

Similar prohibitions can also be used as preventive measures, for example in the case of *Roman Udot*, Board Member of GOLOS Movement for the Protection of Voters' Rights. While releasing him from home arrest, the court barred Roman from using Internet and mobile connection.

At the same time, the new Art. 20.3.1 CoAO (incitement of hatred and humiliation of dignity) was put to use as soon as it came into force in the beginning of 2019 — 158 persons were charged under that article only in the first half of the year (138 were fined, 9 were sentenced to administrative arrest and 11 were sentenced to compulsory labor).

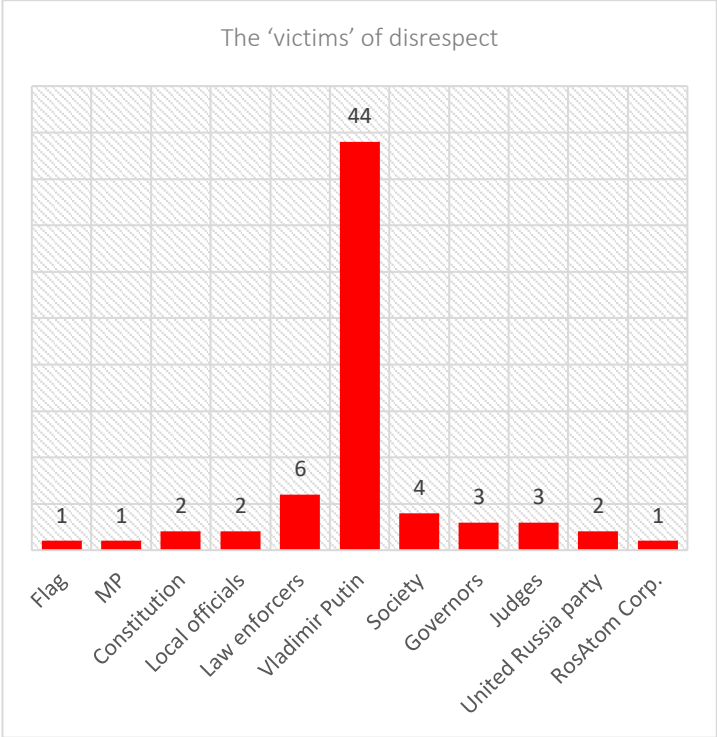
In November 2019, blogger *Alexei Kungurov* was sentenced to 15 days of administrative arrest in Tyumen for his post in Living Journal entitled ‘Is it acceptable to say that Russian people are shit?’ where he offered rough satirical reflections on the national mentality of Russians.

Meanwhile, the Mendeleev Regional Court in Tatarstan imposed a fine of 10,000 Rubles on *Radislav Fedorov* for publishing a video in VKontakte (VK) titled ‘Who are you, Dimon?’. The video depicted opposition leaders Alexei Navalny and Leonid Volkov escorting former Prime Minister Dimitry Medvedev to an electrocution chair while Vladimir Putin, his press-secretary Dmitry Peskov and Rosneft CEO Igor Sechin watched the procession with some rap-like narrative in the background.

Considering that administrative cases are faster and simpler compared to criminal proceedings and having regard to uncertainties about the limitation periods for the enforcement of liability, we can expect to see more cases under that CoAO article going forward.

One of the hottest topic in 2019 was disrespect to the authorities. While the formal description of the offence in Art. 20.3.1 of the CoAO is ‘disrespect to

the State, its organs, the society and the Constitution', the phrase 'disrespect to the authorities' is used even in official documents, e.g. in official reports of Roskomnadzor, which clearly indicates the actual content and intent of the law. Indeed, the 'disrespect' provision, the adoption of which was lobbied for by Vladimir Putin himself, has been used mostly to persecute critics of the President (in 44 of the 78 cases known at the time of writing). However, disrespect is not limited only to the President.



In October 2019 the court of **Nizhny Novgorod** levied a fine of 70,000 Rubles on *Irina Slavina*, a journalist of KozaPress, for comments about the installation of an inscription commemorating Joseph Stalin in the town of Shakhunya. Slavina replaced to root of the town's name with a rude word and was found guilty of disrespect to society.

In November the Leninskiy District Court of **Yekaterinburg** levied a fine of 30,000 Rubles on political analyst *Fedor Krasheninnikov* for his comments in Telegram about yet another arrest of politician Leonid Volkov.

Unlike disrespect to the authorities, the provisions on liability for deliberate dissemination of false information of public relevance (Art. 13.15, paragraphs 9–11 of the CoAO) are not applied very often. 13 cases under these provisions are known at the time of writing, however many of them have been dismissed by courts or police without considering the merits. Nevertheless, the emerging case-law indicates that the new provisions can be used to prevent the dissemination of important information.

Sergey Belogorokhov, an activist of the Chelyabinsk-based environmental movement Stop-GOK was ordered to pay a fine of 40,000 Rubles for reporting in VKontakte a sinkhole in the town of **Roza** which could have been caused by blasting activities at Korkinskiy open-pit coal mine. The court

found that the information was deliberately falsified relying on a statement from the contractor OOO 'Promrekultivatsiya' (a joint venture between Russian Copper Company and Chelyabinsk Coal Company). The statement said that there was not any blasting activity on that particular day.

Regulation of the Internet and Control on the Infrastructure

*In 2019 we counted **62** various proposals for regulating the Internet, some of which have already become law and include not only additional grounds for the prohibition of information, but also sanctions for users, new obligations of IT companies and measures aimed at the centralization of all Web traffic. Since 2012, the year in which the State became really serious about regulating the Web, there have been **614** regulatory proposals of that kind.*

As noted above, regulatory packages on 'fake news'* and 'disrespect to the authorities' came into force in March 2019. In addition to administrative liability for disseminating such information, the law provides that the web resources involved can be blocked by a decision of the Prosecutor General or his deputies.

Criteria for the assessment of the credibility of the information and of its public relevance may or may not exist, but in any case, they are not published officially, which open the gates widely to arbitrariness and abuse. Moreover, the mechanism of blocking web resources is such that the decisions can be challenged only after the information concerned has been removed. In September 2019 the head of Roskomnadzor announced that until then his institution had received from the Office of the Prosecutor General orders to remove information from 47 websites, while Roskomnadzor had themselves identified 128 'mirrors' with identical information. Furthermore, in November Roskomnadzor published a list of resources which had received multiple orders to remove purportedly false information. These included private websites as well as popular groups and media accounts in social platforms.

Important amendments to the procedural laws, proposed by the Supreme Court of the Russian Federation, came into force on 1 October 2019. Among other things, the amendments concern the proceedings in cases related to

*Defined in the Information Act as incredible information of public relevance, which is disseminated in the form of seemingly credible messages and can potentially threaten the life and/or health of citizens; cause damage to properties; cause massive disruption of public order and/or public security; cause disruption or shutdown of critical communal, transport or social infrastructures, credit institutions or sites in the energy, manufacturing or communication sectors (Art. 15.3, paragraph 1).

prohibition of information (including the proscription of information materials as extremist ones) as well as the rules of appealing judgments of Moscow City Court in matters related to the protection of copyright and/or neighbouring rights in the Internet (including judgments for 'perpetual' blocking).

These amendments legitimized what has already become a prevalent approach[*]. The issue addressed by the Supreme Court is that regional courts usually dealt with these cases in the absence of the parties concerned, i.e. the owners of the sites about to be prohibited and the authors of the materials about to be proscribed as extremist ones. Thus, the courts' judgments typically became known a few months after they had been delivered. In the meantime, the resources had already been blocked, but Russian courts practically did not allow website owners to challenge the judgments after such a long period.

However, critical procedural problems have remained unresolved, including the discretion enjoyed by prosecutors to choose the venue at which the case is to be examined and the assignment to the court of the vague responsibility 'to determine the range of persons, rights and legitimate interests that may be affected by the court's judgment', meaning that the actually concerned parties may continue to be kept at bay from these proceedings.

In early December 2019 Vladimir Putin signed a law which makes it possible to proscribe as 'foreign agents' not only NGOs and foreign mass media, but also citizens who disseminate messages intended for an unlimited range of individuals and receive monetary or other benefits from a foreign source. A 'foreign agent' status means, in particular, that the 'agents' are required to label all their publications (such as individual tweets or posts in social media), submit additional reports to the authorities about their activities and spending, and make public disclosures of these circumstances. The same law also provides for restricting the access to the websites of mass media proscribed as 'alien agents' if they become subject to administrative liability.

Also in early December 2019, the Code of Administrative Offences was substantially updated in terms of imposing much higher fines for breaching the rules governing the dissemination of content. The December amendments heighten the fines for repeated offences committed by owners of audio-visual services (the so-called 'online cinema theatres'): up to

[*] Cf. Ruling of Supreme Court of the Russian Federation No 78-KG 17-101 of 20 April 2018 in the application of Tonkoshkurov N.A. [official website of the Russian Supreme Court]: www.vsrf.ru/stor_pdf.php?id=1646816

1 million Rubles for relaying TV channels or programmes which are not registered as mass media (Art. 13.35) and repeated breach of the rules for disseminating information among children (Art. 13.36); up to 5 million Rubles for repeated dissemination of calls to terrorism or extremism (Art. 13.37).

Owners of search engines may find themselves fined with up to 5 million Rubles if they repeatedly display links to websites containing prohibited information or to pirate sites.

However, 'legislation of the year' became Federal Law 90-FZ of 1 May 2019, which users and experts called 'the Sovereign Internet Act' or 'the Runet Isolation Act'. While the explanatory memorandum to the draft act insisted that the aim of the new legislation is to 'ensure the sustainable functioning of Internet in Russia in case its functioning is threatened from abroad', many experts have stressed that its implementation will reduce the efficiency of the Web and will probably make the connectivity slower and more expensive, and can potentially be used for censoring or isolating the Runet.

More specifically, the Act provides for the installation at operators' nodes of technical devices for countering threats (DPI) at the expense of the national budget; requires the setting up at Roskomnadzor of a Centre for monitoring and management of public communication networks, which will ensure the availability of communication services in Russian in any 'extraordinary' situation and will coordinate the efforts of communication operators in such situations; and endorses a national system for cryptographic protection and a national domain name system.

The key problem with this Act is the uncertainty about the threats which it is supposed to pre-empt. The published Draft Decree of the Russian Government entitled 'Concerning the approval of rules and procedures for centralised management of public communication networks' indicates that, in addition to breaches of the integrity, confidentiality and availability of communication networks, a threat can also be the provision of access to prohibited information or resources.

This means that e.g. the functioning of the Telegram Messenger (which remains accessible by Russian users despite the prohibition imposed by Taganskiy Regional Court of Moscow) does, in the opinion of the authorities, threaten the safety of the Runet. In turn, this will enable Roskomnadzor block individual ports, protocols or sets of IP addresses in its own monitoring centre in such a way that telecom operators will never know about the so-imposed measures.

The draft decree received negative feedback from experts and is for the time being put on hold. Nevertheless, having regard to the provisions of the Information Safety Doctrine of the Russian Federation, approved by Vladimir Putin in 2016, it is highly probable that the system put in place now will in future be used not only for defending critical infrastructures from cyber attacks, but also for censoring and tracking users. For example, the information threats listed in the Doctrine include transboundary circulation of information, publication in international mass media of extensive materials which contain prejudiced assessments of the State policy of the Russian Federation as well as undermining the traditional Russian spiritual and moral values.

Government-led Internet Shutdowns

Nevertheless, the Russian authorities actively resort to mechanisms that are already in place. Article 64 of the Russian Communications Act provides that the provision of communication services to legal entities and individuals can be suspended by order of the authority which carries out operative-search activities or is responsible for the safety of the Russian Federation. However, this provision became systematically used for political purposes only in recent years.

In the Autumn of 2018 and in the Spring of 2019, during protests in Ingushetia against the transfer of some Ingushetia territories to Chechnya, 'the Big Three' operators repeatedly shut down the mobile Internet services. An Ingushetia citizen lodged in court an application against the Ministry of Interior (MoI) and the Federal Security Service (FSS). During the trial it emerged that these shutdowns were ordered by the FSS.

An FSS representative presented to the court a pack of standard letters to communication operators requiring them to shut down 3G/LTE segments across the entire Republic for the purpose of 'checking information about plots to perpetrate subversive and terrorist acts'.

In the Summer of 2019 a tactic of local shutdowns was tested for the first time in Moscow during mass protests against barring independent candidates from elections for the Moscow City Council. On that occasion the authorities and the operators explained that service disruptions were due to network overload, however independent experts presented evidence that the mobile Internet shutdown was centralized.

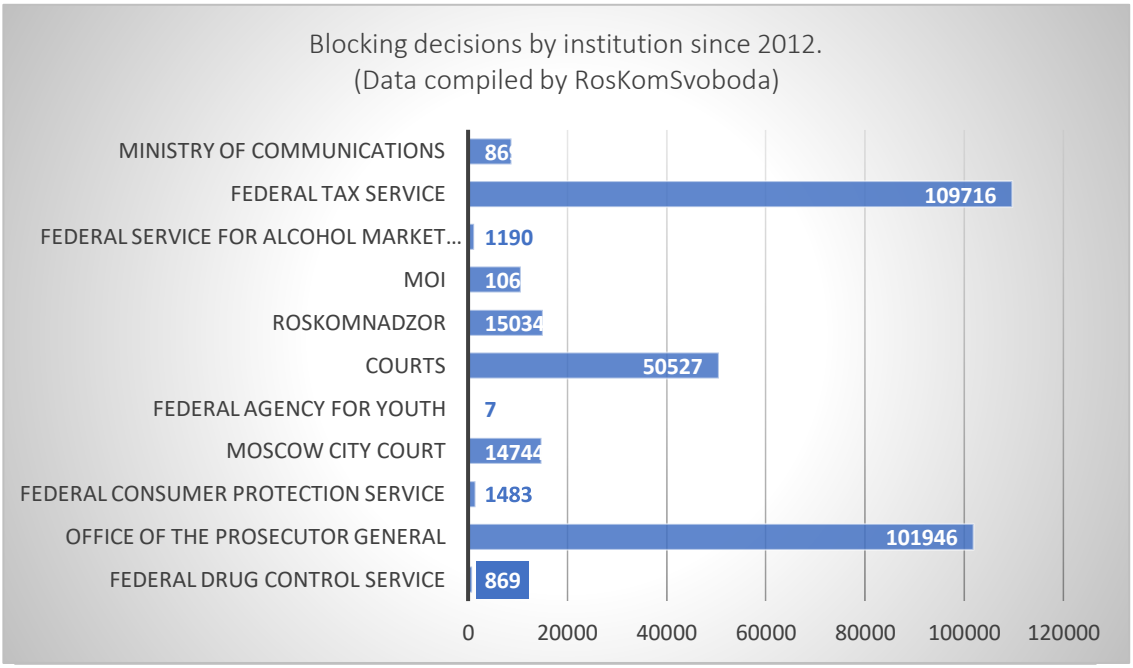
Mobile Internet shutdowns occurred during protests against the construction of a garbage landfill in **Shiyes (Archangeslk oblast)** and in rallies calling for invalidation of the election of a local mayor in **Ulan-Ede (Buryatia).**

Occasionally, disruptions of access occur as a result of localized interruptions of the signal: residents of the town of **Seredka (Pskov oblast)** complained about network connectivity problems caused by a jamming system deployed at a nearby high-security prison; journalists present at Lublinskiy District Court of Moscow reported that communications in the court house were shut down during the interrogation of a police informant in a headline-making criminal case.

Content Censorship: Website Shutdowns and Prohibition of Information

*In the matter of nine months in 2019, Roskomnadzor, acting either on its own initiative or on the basis of decisions of the MoI, the Federal Tax Service, the Office of the Prosecutor General, the Federal Consumer Protection Service, various courts and a range of other institutions, included in the register of prohibited information more than **270,000** websites and webpage indexes, which is almost 30 % more than the number in 2018. Telecom operators were ordered to restrict access to 100,000 resources more. Withal, 'collateral' shutdowns affected* more than **4.74 million** web resources.

In the aftermath, by the end of 2019 the overall number of web resources blocked on the basis of official decisions of the authorities for the entire



existence of 'blacklists' stood at around 315,000. The bulk of these decisions came from the Federal Tax Service — 109,716 (34.8 %), the Office of the Prosecutor General — 101,946 (32.4 %) and the courts — 50,526 (16 %).

Affected by these decisions can be Russian resources as well as foreign mass media. Thus, in January 2019 a blocking decision targeted the Norwegian magazine *Barents Observer*, which publishes some of its materials in Russian language. The Russian authorities were unhappy with an article about Dan Ericsson, a Sami who committed suicide over taboos and prejudices about his homosexuality.

In March 2019 it emerged that two of the largest communication operators in Russia, MTS and Rostelecom, had bypassed the official register of Roskomnadzor and had restricted traffic on the SMTP server of the secure mail service ProtonMail on the basis of letters from the Federal Security Service. A repeated attack on that mail service took place in early 2020.

In December 2019 Roskomnadzor lodged at Taganskiy District Court of Moscow applications for blocking in the territory of Russia two other secure mail services, Mailbox.org and Scryptmail.com, which, similar to Telegram, did not comply with the order of the FSS to provide access to the correspondence of their users.

The practice of using the blocking legislation in business conflicts saw further evolution in the previous year as censoring was requested by commercial entities. In the spring of 2019 Roskomnadzor, relying on a judgment of Kazan District Court, ordered the major legal portal *Pravo.ru* to remove the translation of an article published in the UK newspaper *The Times*, which was dedicated to litigation among businessmen Rustem Magdeev, Dmitriy Tsvetkov and Emil Gainullin. The board of editors managed to obtain a court ruling which established that the precautionary measures had been applied to dozens of web resources that were not concerned with the subject-matter of the dispute and were not involved in the judicial proceedings.

In April 2019 Roskomnadzor launched an even more massive blocking campaign demanding the removal of thousands of publications about the affair between Andrey Kostin, President of the State-owned VTB Bank, and Nailya Asker-zade of the All-Russian State Television and Radio Broadcasting Company (VGRTK). It emerged later that already in the autumn of 2018 the Arbitration Court of Saint-Petersburg issued a ruling on an application from the VTB by which the bank requested protection of its business reputation; there were not any defendants in the proceedings.

In April 2019 the Crimean Human Rights Group reported that access to 14 Ukrainian web portals was fully shut down in Crimea and 28 other resources were blocked in part, withal all these measures had been taken outside the framework of the Russian register of prohibited websites.

In August 2019 *Meduza* had to close down access for Russian readers to an article entitled 'Once you smoke some joint, you will never abandon it. Tie someone to a bed and he will stop injecting himself with heroine. Not really', in order to avoid full blocking of the entire resource. Objections to the publication came from the MoI as they were unhappy with the titles of the individual sections of the publication. Furthermore, the MoI prohibited a *Baza* article 'Life Broadcast from a Ketamine Trance' which explained the history of research into this substance, and a note in *The Village* entitled 'I Serve Time for Stuffing' which was about a young man sentenced under Article 228 of the Criminal Code for working as a 'stuffer'.

In December 2018 Roskomnadzor ordered the editors of the self-made magazine '*Old Fellow, You Are Transformer*' («Батенька, да вы трансформер») to remove the article 'Heroine is Property of the Model' which was about a young woman who has a normal life despite being an everyday user of heroine for ten years. In its ban decision the MoI asserted that the publication created a positive image of a 'drug addict'. In 2019 the editors challenged at the Supreme Court a joint order of several institutions setting out criteria for the evaluation of prohibited information. In a nutshell, the journalists asserted that the so-established criteria go beyond the restrictions set out in the Communications Act, essentially restrict the dissemination of any information about drug users; instil stigma and thereby forestall open public debates on the social situation of these users. In the beginning of 2020 the Supreme Court dismissed their application and upheld the challenged order.

In September 2019 YouTube, acting on the basis of a court decision, asked the *LifeHacker* website to remove the video 'How to Bypass Blocking of Sites and Trackers', and one day later it became known that a prosecutor in Saratov had objections to the website of the human rights organisation Team29 — the prosecutor held that an article entitled 'How to Bypass Blocking of Website' is unlawful after which the article was removed.

In October 2019 the news agency *Fergana* was blocked for the second time in Russia following publication of materials about committed suicides. At this time all Fergana resources are blocked in Russia.

In the end of November 2019 Roskomnadzor acted on an order from the Office of the Prosecutor General and blocked one webpage of Shutterstock, a major U.S. based stock market service, for publishing an insulting depiction of the Russian flag. Similar decisions were taken in respect of the popular image boards Dva.ch, Arhivach, Risovach, the LiveInternet portal as well as Twitter, YouTube, Facebook, Instagram and a range of other resources.

According to information from Roskomnadzor, by October 2019 the Office of the Prosecutor General had ordered the removal of materials published on hundreds of links. The authorities assert furthermore that in the overwhelming majority of cases the website administrators, including international ones, comply with these orders and remove the prohibited content.

In passing, the courts sometimes reject prosecutors' demands to remove information, including in matters which are highly sensitive to the authorities. For example, the City Court of Naberezhnye Chelny refused to grant a prosecutor's request to block a group of Alexei Navalny supporters in VKontankte.

Despite the increasing number of blocks, bypassing Internet censorship in Russia with techniques such as VPN, anonymizers, proxy plug-ins for web browsers, Tor and so on does not seem a major problem for citizens. For example, on an averaged basis, in 2019 the number of Tor users in Russia was 353,000 per day (which ranks Russia second after the US with their 363,000 users). The functioning of these technologies is not yet banned in Russia and using them is not an offence.

Furthermore, in the Spring of 2019 Roskomnadzor for the first time applied the law in order to force VPN services and search engine operators filter their traffic by sending out to the top ten companies demands requiring them to connect to the traffic filtering system as per the Russian blacklist of websites. Most of the companies in the list responded that they will not comply with the demand except Kaspersky Lab, which according to Roskomnadzor complies with all statutory requirements.

The Russian legislation on the blocking of web resources makes it possible to restrict access not only to specific web pages, but to complete domains and sets of IP addresses. That said, communication operators are free to decide what blocking technique to use for the sets of domains and IP addresses (and even their subnets) which Roskomnadzor identifies and uploads several times every day. If providers choose to block IP addresses, access is then restricted not only the banned content but to many other

'innocent' web resources to which the authorities have not any objections whatever. By the end of 2019 the number of websites which suffered 'collateral' blocking by these providers exceeded 4.74 million.

In September 2019 the Russian company Zhivaya Fotografia (Live Photo) — one of the 'collateral' victims of Roskomnadzor's attempts to block the Telegram Messenger in the Spring of 2018 — lodged an application at the European Court of Human Rights.

Persecution of IT businesses and Software Developers

This is one the latest developments observed in the past year. The new trend demonstrates that the Russian authorities aim to strengthen information sovereignty and establish control not only on the dissemination of information by users in the Internet, but also on the infrastructure of the Web. In the opinion of the authors of this report, this may be the beginning of a fight against Russia's dependence on international services and technologies, meaning that the development and maintenance of software can be a dangerous business.

The NGINX Case

On 12 December 2019 there was a search at the Moscow office of NGINX, a web server developer, as part of a criminal investigation over copyright violations alleged by the company Rambler Internet Holding. The founders of NGINX Igor Sysoev and Maxim Konovalov were arrested and their fate remained unknown for hours.

In brief, Rambler claimed that Sysoev created the server software at the time when he worked for the company, meaning that the product is proprietary and cannot be used without the rightholder's consent.

With nearly one of every four websites running on NGINX, the product is one of the most popular web servers in the Internet. In March 2019 F5 Networks, Inc. — a global leader in the area of multicloud services — announced that it had acquired NGINX for USD 670 million. The criminal investigation and the office search triggered stormy responses in the Runet and across the professional IT community. Support for Sysoev was voiced by major web companies, activists and experts, which forced Rambler withdraw their claims and cancel the contract with the law firm which initiated the persecution of NGINX on behalf of the holding.

The Sovereign IP- Addresses Case

In the middle of last December it emerged that Aleksei Soldatov, Doctor of Physics and Mathematics, former Deputy Minister of Communications and co-founder of the Runet, had been charged with fraud together with two other entrepreneurs. The accusations against the three defendants were that they put in place a scheme for transferring abroad 470,000 IPv4 addresses which before that were administrated by the Russian R&D Institute for Public Networks Development (RosNIIRos).

Formally, after a decision had been taken to liquidate the Institute, the IPv4 addresses were transferred from RosNIIRos to the Czech organisation Reliable Communication in accordance with the rules of RIPE NCC to ensure the continued operation of the base of Russian subscribers, which includes many academic institutions.

Experts suggest that Soldatov has been subjected to criminal prosecution because he refused to surrender to the State the control on the .su domain, which, in the framework of the Runet sovereignty process, must become part of the national domain system.

Summary

Similar to the 'Fortress' plan deployed by police to keep lawyers and observers at bay from mass arrests at peaceful rallies, the Russian authorities have declared the entire Runet a fortress, hoping to keep arbitrariness and fraud hidden behind the fortress walls.

By and large, bureaucrats discard the notion that interference with the freedom of speech is an extraordinary measure of last resort and tend to perceive website shutdowns, prosecution of users and disruption of Russian and international mass media as tools of political struggle and methods to oppose the West in the information war.

'The issue around the Russian broadcaster of *BBC* is not only a regulatory, but also a political one, therefore we are investigating, will continue to investigate, and when the time is right we will announce whether we would have any specific allegations', said Alexander Zharov, head of Roskomnadzor, shortly after it became known that the UK regulator Ofcom had brought allegations against the State-owned TV channel *RT*.

Along these lines, the authorities are putting in place infrastructures and legal procedures for potential isolation of the Runet – in 2020 the communication authorities plan to conduct a series of drills 'to ensure resilient, safe and integrated functioning of the Internet and of the public communication networks in the territory of the Russian Federation'. The first phase of the drills will test the readiness for blocking encrypted traffic.

Shutdown efforts will probably include stepping-up pressure on Internet businesses, both Russian (to establish control) and international (in an attempt to force them into self-censorship and collaboration), however, even apolitical services and companies may also get caught in the new reality.

After much wavering in the past years, the authorities have finally defined the main vector of their policy in respect of the Russian segment of the Internet — *control*, *censorship* and *isolation*. Initial references to internal and external threats can be found in the Information Safety Doctrine adopted in 2016. The follow-up actions were aimed at delivering this task, the ultimate objective of which is the creation of a sovereign Internet of Chinese/North Korean style. The year 2019 saw the adoption of key legislation which enables the achievement of this objective.

The main intrigue now is whether the authorities will be able to walk the talk. For the time being, such initiatives either do not take off the ground (Yarovaya's Bill on traffic storage and decryption) or do not work (blocking the Telegram, prohibiting cryptocurrencies), or are all too easy to bypass (numerous shutdowns of websites). As always, Internet users are fairly quick to learn new techniques and adapt to the changing environment, and technology charges forward, which in turn stretches to infinity the frontline with law enforcers and makes it increasingly difficult to counter the free flow of information.

The Authors

Stanislav SELEZNEV — Lawyer, Legal Analyst of Agora International

Pavel CHIKOV — PhD (Law), Head of Agora International

Damir GAINUTDINOV — PhD (Law), Legal Analyst of Agora International

Artem KOZLYUK — Head of *RosKomSvoboda*

Sarkis DARBINYAN — Lawyer, Head of Legal Practices of RosKomSvoboda

Stanislav SHAKIROV — Technical director of RosKomSvoboda

AGORA
—Международная правозащитная группа—

Agora International Human Rights Group is an association of dozens of lawyers from several countries specializing in the legal protection of civil liberties in the post-Soviet space.

РОСКОМСВОБОДА

RosKomSvoboda is a public organisation devoted to the defending digital rights and to the promotion of ideas such as freedom of information, inadmissibility of State censorship and proscription of State interference in private life.