Media4Democracy.EU

Briefing Note
Review of Recent Laws Affecting Digital Rights in Russia

Seminar: Digital Legislative Developments in Russia Freedom of Expression Online
18 December 2019, Moscow

Toby Mendel and Galina Arapova

Table of Contents

Executive Summary

Respect for freedom of expression in the Russian Federation lags significantly behind international standards and this problem has become significantly more serious since Vladimir Putin returned to the post of President in 2012. Among a number of other developments, the adoption since 2016 of five major legal reform packages governing digital communications, including three in 2019 alone, have had an important negative impact on freedom of expression online. This Briefing Note explains the main provisions of these legal reforms, focusing both on their technical provisions and on how they could be used to limit free speech online in Russia.

The first two legal reforms, called the "Yarovaya" Laws after their author, were adopted in July 2016 and require those covered by the Laws, namely "telecommunication operators" and "organisers of information dissemination", to retain both metadata relating to communications and also the actual content of communications, for long periods of time. A list of the specific services which are covered includes a wide range of Russian telecommunications and Internet access service providers, social media and websites hosting discussion forums, although for now most international services have been exempted. These companies must provide access to the retained data to the Federal Security Services (FSB) and other law enforcement bodies, along with decryption keys. Although normally a court order is required for such access, this is not required for serious crimes, including terrorism offences, which is the main target of the Yarovaya laws. As such, these Laws substantially increase the powers of surveillance over online activities that were put in place in Russia in the 1990s through the System for Operational Investigative Measures (SORM), thereby significantly undermining protection for privacy and freedom of expression.

The "Disrespect for Authority" Law applies to online content which expresses "in an indecent form … blatant disrespect for human dignity and public morals" in relation to the State, official State symbols, the Constitution or public bodies. These rules are based on vague notions – such as "indecent form" and "blatant disrespect for human dignity and public morals" – and protect a range of actors – public bodies and inanimate objects, such as the State, the Constitution and State symbols – which cannot properly be said to have reputations in the first place. They also provide the authorities with an easy, extra-judicial means to block access to content. Once the Prosecutor decides content is illegal, he or she informs the Federal media regulator, Roscomnadzor, which in turn informs the service provider. The latter then informs the owner, who has 24 hours to take the content down, failing which the service provider must block it. The evidence suggests that, so far, well over one-half of all of the cases under this Law relate to statements about the president, giving a clear indication of its true purpose.

The "Fake News" Law provides for measures against content which meets two conditions. The first, is the distribution of "inaccurate socially important information … under the guise of a credible report". The second is the creation of a threat of: a) harm to life, health or property; b) mass disturbance of public order or public security; or c) interfering with various systems, such as transport, social infrastructure, credit institutions, industry or communications. None of the key terms are defined and the Law fails to provide for defences or *de minimus* standards for its application (for example to protect against application in the case of a simple error). Leading courts around the world have held that the notion of "fake news" is too vague to be used as a condition for regulating content. Under this Law, content can be blocked in the same way as under the "Disrespect for Authority" Law, although here the owner is only notified in the case

of a registered mass media outlet while for other websites immediate blocking by the service provider is envisaged. Since the Law just came into effect at the end of March 2019, it is too early to assess its impact, but the potential for abuse is significant.

Finally, the "Sovereign Internet" Law ultimately allows for a control centre operating within Roscomnadzor to undertake centralised management of the Russian Internet, in the case of a threat to its stability and security, including by cutting parts or all of it off from the global Internet. However, many commentators have suggested that the preparatory measures which will be put in place to enable centralised management are the real objective of the legislation. Internet access providers must install "technical means" to counter threats which will be provided free of charge by Roskomnadzor. The technical means being used in the pilot implementation of the Law allow for DPI (deep packet inspection) and for the blocking of illegal content, which may be adapted specifically for any particular provider. Together, the Law would appear to enable the authorities to block access to parts or all of the global Internet, to shut down the Internet entirely within Russia, to block certain traffic (i.e. to conduct fine-grained censorship) and to conduct close surveillance of the communication activities of selected actors, all without the need for any external authorisation (such as from a court).

It is too early to determine what the real impact of the measures contained in these five major legal reform packages governing digital communications will be. What is clear, however, is that they give the authorities vast powers, subject only to limited court oversight, to prevent a similarly vast range of largely undefined content from being disseminated online, as well as to monitor and conduct surveillance over online communications within Russia. Only time will tell what the actual implications are.

Media4Democracy.EU

1. Introduction

It is widely agreed that respect for freedom of expression in the Russian Federation, which has lagged significantly behind international standards since the adoption of the acting Constitution of the Russian Federation, has declined precipitously since Vladimir Putin returned to the post of President in 2012. Some of the key milestones here were: the re-criminalisation of defamation in 2012; the introduction of very restrictive rules on personal data protection; and the introduction of rules allowing for extrajudicial blocking of websites, leading, among other things, to the closure of a number of independent online media outlets. The selective implementation of laws, the absence of respect for the rule of law and the lack of an independent judicial system have made challenging violations of freedom of expression in the courts an elusive remedy.

A major feature of the attack on freedom of expression, especially over the last few years, has involved digital communications given their increasingly dominant role in modern communications. Since 2016, at least five major legal reform packages have been adopted, three in 2019 alone, which have had an important negative impact on freedom of expression online. This Briefing Note provides an analysis of those five legal reform packages, assessing what they do, their legitimacy as restrictions on freedom of expression and how they are likely to impact on that right in practice in Russia.

This analysis takes as its starting point international guarantees for freedom of expression. International law recognises that freedom of expression is a fundamental human right but not one that is absolute. At the same time, it places strict conditions on any restrictions on this right. Specifically, restrictions must meet a strict three-part test which requires them: to be provided by a law which is clear and precise; to have as their aim the protection of one of the legitimate interests recognised under international law (namely the rights or reputations of others, national security, public order, or public health or morals); and to be "necessary" to protect that interest which, among other things, incorporates a proportionality test.

2. "Yarovaya" Laws

The "Yarovaya" Laws (or "Yarovaya" package) comprise two companion laws[1] passed on the same day in July 2016 and introducing a number of amendments to nineteen Federal laws.[2]

[1] Federal Law "On Amendments to the Federal Law 'On Countering Terrorism' and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and public safety" of 6 July 2016, No. 374-FZ, and Federal Law "On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety" of 6 July 2016, No. 375-FZ.

[2] These laws are: Federal Law "On Countering Terrorism"; Federal Law "On Federal Security Service"; Federal Law "On Operation-Search Activity"; Federal Law "On Foreign Intelligence"; Federal Law "On Arms"; the Criminal Code; the Criminal Procedure Code; the Air Code; Federal Law "On Freedom of Conscience and Religious Associations"; Federal Law "On Postal Communication"; Federal Law "On Countering the Legalisation (Laundering) of Criminal Income and the Financing of Terrorism"; the Code of Administrative Offences; Federal Law "On Transportation and Expeditionary Activity"; Federal Law "On Communications"; the Housing Code; Federal Law "On Information, Information Technologies and Data Protection"; Federal Law "On Transport

They were justified on the grounds of "countering extremism" but are broadly framed, allowing for arbitrary application and severely undermining the rights to freedom of expression, privacy and freedom of religion and belief. In addition to their human rights problems, these laws have been heavily criticised for imposing huge, indeed unmanageable, costs on the companies they cover in terms of massive data storage requirements, data processing systems and other infrastructure requirements.

The Yarovaya Laws provide for long periods of storage of both metadata (three years) and the actual content of communications (six months). However, due to the technical impossibility of this, the Russian government approved a data storage procedure in April 2018[3] which provides that the storage period shall be determined by the actual technical capabilities of those subject to the law and is in any case reduced to one month for actual content and three months for metadata.[4] Based on these standards, the laws entered into force on 1 July 2018, which was then postponed until 1 October 2018, because the companies covered could not meet the data storage requirements. In addition, there is still no formally certified equipment to use for purposes of these Laws and some telecommunications have refused to install equipment until it is certified, despite which at least one has already been charged with breach of the Law.

The Scope of Coverage of the Laws

The Yarovaya Laws apply to "telecommunication operators" and "organisers of information dissemination", both of which are subject to the data retention rules. The idea of an "organiser of information dissemination" is a new concept which covers companies carrying out activities to ensure the functioning of information systems and/or programmes which are intended and/or used to receive, transmit, deliver and/or process electronic communications. According to the Ministry of Communications, this includes any website which enables the exchange of communications or messages between users. However, in practice only companies that are listed in the official register maintained by Roskomnadzor, the mass media regulator, are subject to the rules.[5] At the moment, this list contains 192 companies,[6] including social networks (especially Russian social networks, such as vk.ru, odnoklassniki.ru), websites hosting discussion forums (thematic websites and many media outlets which allow for user generated content, such as E1.ru, panram.ru),[7] online meeting services (such as tinder.com), mobile applications and other online services which provide tools for communication between users, such as vimeo.com and wechat.com. However, a large number of websites which are accessible in Russia and which technically qualify as organisers of information dissemination,

Security"; Federal Law "On the Territorial Jurisdiction of the District (Naval) Military Courts"; and Federal Law "On the Safety of Fuel and Energy Complex".

[3] Decree of the Government of the Russian Federation of 12 April 2018, No. 445 "On Approval of the Rules for Storage of Text Messages of Users of Communication Services, Voice Information, Images, Sounds, Video and Other Messages of Users of Communication Services by Telecommunications Operators". Available on the official legal online website at: http://publication.pravo.gov.ru/Document/View/0001201804190032?index=2&rangeSize=1.

[4] As described in an article in the online media outlet Meduza. Available at: https://meduza.io/news/2018/04/19/pravitelstvo-utverdilo-sroki-hraneniya-dannyh-po-zakonu-yarovoy-internet-trafik-polzovateley-budut-hranit-30-dney-a-ne-polgoda.

[5] More information about this is available at: https://rkn.gov.ru/opendata/7705846236-InformationDistributor/.

[6] According to the register of organisers of information dissemination published on the website of the NGO RosKomSvoboda. Available at: https://reestr.rublacklist.net/distributors/.

[7] Panorama online-media was fined RUB 100 000 for not registering itself as an "organiser of information dissemination". See: https://mmdc.ru/news-div/judge_history/ori-ne-ori-smi-kotoroe-ne-voshlo-v-reestr-roskomnadzora-oshtrafovali-na-100-tys-rubley/.

including many foreign ones – such as online stores, blogs, message services, social networks, and online media and forums – have not been placed on the list.

These rules are considered by experts to be the next level of surveillance of online activity as compared to the existed rules. The System for Operational Investigative Measures (SORM) has existed in Russia since the 1990s. It allows the State to wiretap telephone and other means of communication, and requires Internet service providers to install equipment directing all Internet traffic to a monitoring point within the Federal Security Service (FSB), enabling it to monitor all Internet activity, including private communications.[8] The operation of the SORM was regulated by bylaws elaborating on the execution of federal laws. This was criticised, including in the *Roman Zakharov v. Russia* decision of the European Court of Human Rights. Ignoring the clear position of the European Court in that case, the Russian authorities, instead of repealing SORM, adopted the "Yarovaya" Laws which strengthened the SORM and the ability of security services to control peoples' private exchange of information.

The Scope of Data Collection and Other Requirements

The Yarovaya Laws require telecommunications operators and organisers of information dissemination to store the actual content of communications – including text messages, voice messages, images, sounds, video and other electronic messages – for six months and the metadata for these communications for three years. As noted above, the data storage periods were reduced but the aim is to increase them gradually to the full term over a period of five years. In terms of which communications are covered, the rules stipulate that data about users who can be identified as being in the territory of the Russian Federation (by IP address, telephone number, geographical metadata or as indicated by the Ministry of Internal Affairs) or as being Russian citizens (based on an identity document) must be retained. Non-compliance with these obligations may lead to an administrative fine which, for legal entities, ranges from RUB 800,000 to 1,000,000.

Restrictions on Privacy and Freedom of Expression

The Yarovaya Laws impose significant restrictions on the privacy and communications' rights of users. All retained communications data must be provided, upon request, to the Federal Security Services (FSB) and any other law enforcement body which is legally entitled to conduct operational search activities (i.e. pre-investigation activities), which includes the police, Federal Penitentiary Service, Federal Customs Service and foreign intelligence service.[9]

Normally, these services need to get prior permission from a court for wiretapping and receiving correspondence. However, in urgent cases which could result in the commission of a serious or especially serious crime, including a terrorist act, they can access this data without prior court authorisation, although they must then notify a court about these actions within 24 hours. There is, as a result, a high probability that the Yarovaya Laws, which focus on terrorism, will in practice lead to greater access to communications data without judicial authorisation.

[8] See Center for Strategic and International Studies, Reference Note on Russian Communications Surveillance, 18 April 2014. Available at: http://csis.org/publication/reference-note-russian-communications-surveillance.
[9] See Article 64(1.1) of the Federal Law "On Communications" of 7 July 2003, No. 126-FZ.

Furthermore, these laws require operators to identify their subscribers by their mobile phone numbers, which are registered to users with their passport details.[10] This information, in turn, is used by the special services in order to determine the exact identity of individuals engaged in certain conversations and correspondence. This seriously undermines the right to anonymity of Internet users since any connection to a public wifi network in Russia will now allow for the identification of the user. With dissent online and offline increasingly punished in Russia, anonymity is vital for the free flow of information and exchange of ideas which are deemed to be controversial by the State. Anonymity is also vital for the protection of journalistic sources.

Importantly, services included on the list must provide to the security services decryption keys for any encrypted content they retain.[11] The authorities, after receiving the decryption keys, will be able to read and use the coded correspondence at their sole discretion, including when they are conducting their work in secret. Failure to comply with this rule may lead to sanctions, including blocking access to these services in Russia, which Roskomnadzor unsuccessfully tried to use against Telegram, a messaging and social networking application, in 2018 (because they have so far failed to block this service in Russia).[12] The system thus denies users the protection for private correspondence which is available using reliable foreign encryption and digital security tools, and will threaten not only ordinary Internet users but also civil society activists and journalists, as well as and their confidential sources of information.

These changes give State actors almost unlimited access to personal data, including both the actual content and metadata of correspondence, for users of both mobile phones and the Internet. Private Internet Access (PIA) – one of the largest private VPN providers in the world – has already refused to work in Russia due to the adoption of the Yarovaya laws.[13]

European Standards

The regime established by the Yarovaya Laws does not respect European standards regarding the human rights to privacy and freedom of expression. In 2006, the European Union adopted the Data Retention Directive,[14] which required Member States to put in place legislative measures to ensure the retention of user communication metadata for between six and 24 months. This is similar to the Yarovaya Laws but significantly less intrusive inasmuch as it did not extend to the actual content of communications. The Directive was challenged before the European Court of Justice which, in a decision of April 2014, held that it breached the European Union Charter of Fundamental Rights, in particular because the blanket data collection it envisaged violated the right to privacy.[15] Since that time, the European Union has not attempted to re-impose a blanket data collection regime.

[10] Article 64(1.1) of the Federal Law "On Communications" and Article 13.20 of the Code of Administrative Offences.
[11] An article in Russian in the local media about this is available at: https://rg.ru/2017/07/06/oleg-ivanov-v-reestre-uzhe-85-organizatorov-rasprostraneniia-informacii.html.
[12] For a local media article about this, see: https://www.m24.ru/articles/obshchestvo/17042018/152698. An OSCE statement about this is available at: https://www.osce.org/representative-on-freedom-of-media/377767 and an Article 19 statement on this case is available at: https://www.article19.org/resources/russia-blocking-telegram-serious-violation-freedom-expression-privacy/.
[13] See an article on this in the Russian press at: https://tass.ru/ekonomika/3449523.
[14] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[15] The decision is available at: http://curia.europa.eu/juris/documents.jsf?num=C-293/12/.

Expanding Criminal Code Rules and Penalties

The Yarovaya Laws also significantly increased the sanctions for terrorist and extremist activities in all their forms as set out in the Criminal Code.[16] Importantly, the sanctions have increased for Article 282 of the Criminal Code "Incitement to Hatred or Hostility, as well as the Humiliation of Human Dignity" – under which Internet users are regularly charged – from no minimum to a minimum of two years' imprisonment and from a maximum of two years' to a maximum of five years' imprisonment. The minimum age for liability under terrorism related crimes has also been reduced to 14 years from 16 years.

3. "Disrespect for Authority" Law

The "Disrespect for Authority" Law, adopted in March 2019, introduces amendments to the Federal Law "On Information, Information Technologies and Data Protection", including a new Article 15.1.1 providing for the blocking of websites which express "in an indecent form information which shows blatant disrespect for human dignity and public morals, the State, official State symbols of the Russian Federation, the Constitution of the Russian Federation or public bodies exercising governmental authority in the Russian Federation". This applies to all online publications regardless of the author or whether they are published on the website of a mass media outlet, a social media company or any other website. Breach of these rules can lead to the blocking of offending websites and fines of up to RUB 100,000 initially but increasing to up to RUB 300,000 and even administrative detention for up to 15 days for a second offence.

Every State provides some sort of legal protection for individual reputations against targeted and unjustified attacks. Russia already has a legal rule for this, in Article 5.61 of the Code of Administrative Offences, breach of which leads to a small fine. However, the restrictions in the Disrespect for Authority Law are, without doubt, the harshest and broadest of all of the Russian restrictions relating to criticism. They are based on vague notions, such as "blatant disrespect for human dignity and public morals", protect a range of institutions exercising State power and attributes in general, as well as a range of inanimate objects, such as the State, the Constitution and State symbols, which cannot properly be said to have reputations in the first place, and provide the authorities with an easy, extra-judicial means to block access to content. They therefore represent an instrument of censorship which is aimed at silencing online debate about political issues and other matters of public concern in Russia.

Scope of Protection

As noted above, the Disrespect for Authority Law deals with criticism directed at inanimate objects that cannot actually be offended, such as the State as a whole, the Constitution, official State symbols (such as the coat of arms or the flag) and bodies exercising State power (public bodies *per se)*. This significantly expands the scope of protection against criticism in Russian law whereas international law suggests that objects like these should not receive protection for reputation. In addition, the notions of "indecent form", "blatant disrespect" and "human dignity and public morals" are not defined and are, as a result, unduly vague. This means that implementation of the rules could be arbitrary leading to further violations of the right to freedom of expression.

There is, in particular, no defined concept of "indecent form" in Russian legislation. Linguists have traditionally defined this to cover obscene language and invective, i.e. swearing. This has

[16] In particular, amendments were introduced to Articles 205, 205.2, 205.5, 208, 282, 282.1, 282.2 and 282.3.

been established through interpretation of Article 297 of the Criminal Code concerning "contempt of court" and Article 319 concerning "insulting representatives of the authorities" (or public officials). These articles do not state explicitly that insults must be expressed in an indecent form but authoritative unofficial interpretations and the case law suggest that this is part of the offence. In the past, this term was limited to swearing and obscenity but it has now been expanded to include informal and vulgar phrases, slang and even ordinary vocabulary. As a result, any criticism of public authorities, State symbols or the State could be deemed to be "indecent".

In practice, for example, the words "insane" and "crocodile", uttered in relation to a judge, have resulted in prosecutions under Article 297 of the Criminal Code for "contempt of court"[17] and for "insult of a public official".[18] It goes without saying that this is not swearing, showing that the scope of "indecent form" has widened considerably.

Insult of the President

There is no specific provision in Russian legislation providing special protection for the head of state against criticism. However, although the president is not explicitly listed in the Disrespect for Authority Law, it has been used to protect him or her against strong criticism. Indeed, a report by the Agora human rights group found that 26 of the 45 cases (58%) lodged under this law from its adoption to the end of September 2019 involved statements about the President. Fully 70% of all cases related to comments posted on the VKontakte (InContact) or VK social network.

In particular, the president could be regarded as a "representative of the authorities" so that, if he is harshly criticised, a criminal case could have been brought under Article 319 of the Criminal Code for "Insulting a representative of the authorities", even before the Disrespect for Authority Law was adopted. But this is a lengthy process involving an investigation and adversarial court proceedings which allow the defendant to defend him- or herself in court, and which only results in a relatively small fine of up to RUB 40,000. In addition, the president must be officially recognised as an aggrieved party and may be questioned during the investigation and in court. As a result, no such case has been brought in Russia under Article 319. Under the Disrespect for Authority Law, however, remedial action is much easier and quicker, with no investigation and with the possibility of blocking access to content within a day by means of extrajudicial blocking (see below). This is already starting to happen, for example with cases under the Law being brought against ordinary Internet users who have published social media posts which are critical of President Putin.[19]

Duplication of Restrictions

Another concern with these provisions is that they duplicate rules already provided for in other laws. This is problematical because it creates parallel, often less freedom of expression

[17] A report on the case is available at: https://zona.media/article/2016/04/02/codex-297.
[18] Reports on the case are available at: https://memohrc.org/ru/special-projects/delo-reznika; and https://mmdc.ru/news-div/judge_history/oglashenie_prigovora_po_delu_zhurnalista_reznika_v_rostovenadonu_naznacheno_na_22_yanvarya/?sphrase_id=2389.
[19] A report on this is available at: https://www.znak.com/2019-05-15/zhitelya_vologodskoy_oblasti_sudyat_za_status_o_tom_chto_putin_ne_skazochnyy_a_realnyy. See also: https://meduza.io/news/2019/05/14/zhitel-yaroslavlya-poluchil-30-tysyach-rubley-shtrafa-za-fotografiyu-graffiti-putin.

protective, regimes for the same type of content. Where this is the case, the new provisions merely introduce new penalties, namely the possibility of blocking access to the information, as well as significantly higher administrative fines and, ultimately, the possibility of administrative detention. Two of the key duplications are as follows:

1) Article 329 of the Criminal Code, "Abuse of the State Coat of Arms of the Russian Federation or the State Flag of the Russian Federation", protects State symbols, thereby overlapping with the Disrespect for Authority Law.[20] It seems clear that the aim here is not actually to protect these symbols, which do not need protection, but to limit political debate.
2) Protection of the judiciary from insulting remarks made in public, including online, is provided for in Article 297 of the Criminal Code "Disrespect to court".

For these offences, as noted above in relation to the president, the main change with the Disrespect for Authority Law is that access to content can rapidly be blocked, at the discretion of the General Prosecutor, without needing judicial approval, which is required in the original offences under the Criminal Code or the Code of Administrative Offences. As a result, the new law represents a very powerful tool for the administration to limit public debate about matters of public concern.

Blocking and Other Measures

The Disrespect for Authority Law empowers the General Prosecutor and his deputies to take individual decisions as to whether or not information falls within the scope of its provisions. Once information is deemed to be illegal, the Prosecutor General notifies Roscomnadzor, the Federal mass media regulator, of its decision. Roscomnadzor, which is not independent of government, then "immediately" notifies the relevant Internet access or hosting provider which, in turn, notifies the website or social media account owner of its obligation to delete the content. If this is not done voluntarily within 24 hours, Roscomnadzor may require the Internet access provider to block access to the website "immediately".

The original decision by the General Prosecutor can be challenged in court but this takes a very long time and cases involving challenges to Internet blocking in Russia unfortunately show that judicial practice usually favours the State, so that the blocking is not lifted. Part of the problem here is that the courts consider these cases on a purely formal (legally technical) basis without demonstrating an understanding of the specific features of the Internet and how these sorts of measures affect free speech.

4. "Fake News" Law

The "Fake News" Law was adopted in a rush in early 2019 with the first reading taking place on 24 January 2019 and the law entering into force on 29 March 2019. This was despite the fact that most of those who commented on the draft law – including the main body responsible for executing it, the mass media regulator, Roskomnadzor – gave negative feedback.[21] It defines a new offence of disseminating inaccurate information that causes certain consequences and then establishes procedures to limit the dissemination of the information via the takedown or blocking of it, as well as fines for those responsible.

[20] The first law uses the word "abuse" whereas the Disrespect for Authority Law refers to "blatant disrespect" but this essence of both offences is similar.

[21] See a report on this in Russian at: https://www.vedomosti.ru/politics/news/2019/01/14/791325-genprokuratura-oskorbleniyah.

Substantive Elements

The scope of information covered by this Law, when it has been disseminated via information and telecommunications networks, including the Internet, is as follows:

> [I]naccurate socially important information distributed under the guise of credible reports, which creates a threat of harm to life and (or) the health of citizens, property, the threat of mass disturbance of public order and (or) public security or the threat of interfering with the functioning or cessation of the operation of life-support objects, transport or social infrastructure, credit institutions, energy facilities, industry or communications … .[22]

This contains two key elements. The first is the distribution of "inaccurate socially important information … under the guise of a credible report". The second is creating a threat of: a) harm to life, health or property; b) mass disturbance of public order or public security; or c) interfering with life-support objects, transport, social infrastructure, credit institutions, energy facilities, industry or communications.

None of the key terms – such as "inaccurate", "socially important", "guise of credible reports", "threat of harm", "mass disturbance", "threat of interfering", "functioning", "social infrastructure" or "communications" – are defined. All of these terms are capable of a wide range of interpretation. The key concept of "inaccuracy" or "falsity" has been held by many peak courts to lack the precision required of a restriction on freedom of expression. For example, the Supreme Court of Canada, considering a provision quite similar to the Russian "Fake News" Law, noted:

> Before we put a person beyond the pale of the Constitution, before we deny a person the protection which the most fundamental law of this land on its face accords to the person, we should, in my belief, be entirely certain that there can be no justification for offering protection. The criterion of falsity falls short of this certainty, given that false statements can sometimes have value and given the difficulty of conclusively determining total falsity.[23]

Other terms are even less clear, such as what constitutes socially important information or what represents a credible report. The lack of key definitions, along with the broad discretion allocated to the Prosecutor in deciding whether to engage the procedures to block or takedown information (see below), means that this Law fails to pass the "prescribed by law" part of the test for restrictions on freedom of expression.

By its own terms, the Law seeks to protect against a very broad range of possible consequences including, for example, an interference with transportation systems, credit institutions, energy facilities or even industry, writ large. This breaches the "legitimate aim" part of the test for restrictions on freedom of expression since, while some such interferences might harm the rights of others, one of the legitimate aims, this would not be the case for many of the consequences covered by the rule. For example, an inaccurate report about a bank failing might interfere with its work and require it to put out a statement demonstrating its financial health, but this would not harm anyone's rights.

Finally, the lack of any defences or *de minimus* standards for the application of this Law means that it also fails to pass the "necessity" part of the test for restrictions. Even an essentially irrelevant error – such as that a bank had been unable to pay a debt of RUB10 million when in

[22] Unofficial translation.
[23] *R. v. Zundel*, [1992] 2 S.C.R. 731, p. 758.

fact it was only RUB9 million or even RUB11 million – would engage responsibility. Similarly, even a negligible impact, such as the one described above whereby a bank had to issue a correction, would engage responsibility. These features mean that the Law is not proportionate, especially given the harsh measures envisaged to limit free speech, described below.

Based on similar considerations, leading courts in a number of jurisdictions have struck down general rules on false news linked to consequences along the lines of those in the Russian provision as being incompatible with the right to freedom of expression.[24]

Administrative Measures and Penalties

The procedures under this Law for limiting further dissemination of information are engaged whenever the Russian Prosecutor General, or his or her deputies, decide that information falls within the scope of the rule. It is unclear how the Prosecutor will determine whether either the information is inaccurate or there is risk of the listed consequences occurring. Theoretically, an investigation into this could be conducted. However, that would take time, which goes against the whole thrust of the scheme, which is designed to foster rapid responses. More importantly, in practice under the analogous procedure for blocking extremist content, investigations have never been conducted.

Once information has been tagged as being in breach of this Law, the only way to stop it being blocked or taken down is to challenge the initial decision of the Prosecutor via the procedure set out in the Code of Administrative Court Procedures, which is identical to the procedure for a civil claim. Such cases normally take many months if not years to decide, in sharp contrast to the immediate takedown or blocking which follows the Prosecutor's initial decision.

Once the Prosecutor deems information to be in breach of this Law, he or she instructs the media regulator, Roskomnadzor, to take measures to restrict access to the information. It is important to note that Roskomnadzor is not independent of government. Those measures differ depending on whether or not the entity responsible for disseminating the information is a registered mass media outlet. In the latter case, Roskomnadzor "immediately" notifies the editor who shall, again "immediately" after receiving the notification, takedown the information (i.e. remove it from the website). If the editor fails to do this, Roskomnadzor contacts the relevant Internet access provider which shall then, once again "immediately", block access to the information.

In other cases, Roskomnadzor skips the step of contacting the "editor" (i.e. website owner) and goes straight to the Internet access provider, instructing it to restrict access to the information "immediately". Roskomnadzor then also contacts the entity that hosts the website, also instructing it to take measures to ensure that access to the information is blocked. The hosting provider then has 24 hours to contact the owner and instruct him or her to takedown the information. However, presumably in most cases by the time the owner had a chance to takedown the information, blocking by the access provider would already have taken place.

[24] See, for example, *Chavunduka & Choto v. Minister of Home Affairs & Attorney General*, 22 May 2000, Judgment No. S.C. 36/2000, Civil Application No. 156/99 (Supreme Court of Zimbabwe; *Hector v. Attorney-General of Antigua and Barbuda*, [1990] 2 All ER 103 (Judicial Committee of the Privy Council); and *R. v. Zundel*, note 23 (Supreme Court of Canada).

No protections are provided for, such as to give time to the editor or website owner to assess the information to determine what exactly is inaccurate and only take that down or perhaps correct it, or to account for communications delays or other challenges (for example where the owner is travelling or ill). Furthermore, for technical reasons or just to make it simple, in other cases under analogous legal provisions entire websites have often been taken down even when only part of the information was deemed to be objectionable, which is obviously not proportionate.

The takedown or blocking of access to the information does not absolve those responsible of administrative liability, and the Law provides for fines, which are increasingly steep for citizens, officials and legal entities, for disseminating the information in the first place.

According to our information, the Law is being applied only to websites for which the Prosecutor has made two or more orders regarding fake news and a test version of the registry for this contains 27 different websites, including some online media and social media accounts but no media which have registered with Roskomnadzor. We are not aware of the number of lawsuits brought under this Law but the media has reported on several cases.

5. "Sovereign Internet Law"

The "Sovereign Internet" Law, as its name suggests, provides the legal basis for various Russian authorities, in case of threats to its stability and security, to isolate the Russian Internet from the global Internet and to manage it centrally as a separate, autonomous (sovereign) service (centralised management). Adopted in May 2019, the rationale for this Law, according to the Explanatory Note, is to counter threats to the Russian Internet from the United States. If centralised management were actually imposed, this would essentially result in the government centrally running the Russian Internet, posing a massive threat to freedom of expression in direct breach of clear international standards. However, the systems mandated by the Law so as to enable centralised management already gives the authorities enormous control over the Internet, even if centralised management is never actually imposed. This has led some commentators to suggest that the real goal is more along the lines of arrogating to the authorities the sort of control that China exercises over its internal Internet.[25] The Law formally came into force only on 1 November 2019 and so far is being piloted only in the Urals Federal District.

The Sovereign Internet System Envisaged by the Law

Under this Law, the media regulator, Roskomnadzor, is required to monitor communication networks operating in Russia so as to identify "threats to the stability, security and integrity of the information and telecommunications network 'Internet'" which would warrant the imposition of centralised management. Management of the Russian Internet in such a case would be consolidated under the direction of a new management and monitoring centre (control centre), operating under Roskomnadzor. The Russian government will define what types of threats may justify centralised management and the procedure for determining those threats. In the event that centralised management is imposed, the control centre may directly manage the telecommunications network or issue binding instructions to telecommunications operators,

[25] See, for example, Ilya Khrennikov, "Russian 'Sovereign Internet' Bill Attacked Over Censorship Risks", Bloomberg, 12 February 2019. Available at: https://www.bloomberg.com/news/articles/2019-02-12/russian-sovereign-internet-bill-attacked-over-censorship-risks.

communications (Internet) networks, traffic exchange points and international connections (which are the entities covered by the system).

Of perhaps even greater interest are the preparatory measures that may or will be put in place to enable centralised management, should the need for it arise. Perhaps the most important of these is the obligation of Internet access providers to install "technical means" to counter threats. Significantly, Roskomnadzor will provide operators with those technical means ("free of charge") and also establish the technical conditions for installing, operating and updating them. The Law does not provide any details about or constraints on those technical means but presumably they could potentially be used for many purposes, including to enable Roskomnadzor to exercise significant direct control over the Internet. The technical means being used in the pilot allow for DPI (deep packet inspection) and for the blocking of illegal content, which may be adapted specifically for any particular system. Numerous other provisions in the Law protect technical means, and any impact they may have, against legal liability or the operation of other rules.

The entities covered by the centralised management system are subjected to a number of other technical obligations. Any agreement to transfer ownership or control of an international communications line is required to include information about the purpose of the line and the means of communication installed on it, and this information must be provided to Roskomnadzor. Roskomnadzor is tasked with establishing a registration system for owners or operators of traffic exchange points, who are also required to inform Roskomnadzor about the commencement of their activities, while Roskomnadzor has broad powers to set directly the rules for their functioning. These owners and operators are prohibited from providing connection services to communications networks which do not comply with various provisions of the Law.

Operators and networks are also subjected to numerous obligations. They are required to inform Roskomnadzor about any communication links through international communications lines and to comply with any technical requirements regarding this set by the Ministry of Communications. They must use registered traffic exchange points when interacting with other operators or networks, use hardware and software approved by the Ministry of Communications to identify addresses corresponding to domain names, restrict access to information as required by various laws (such as the "Fake News" Law) and provide a wide array of information upon request to Roskomnadzor.

Collectively, these provisions give the authorities enormous control over the operation of the Russian Internet, even without imposing centralised management.

Impact of these Measures

Many important technical details regarding the operation of the "Sovereign Internet" Law are left to be determined by subsequent regulation or simply by measures taken by official bodies, so it is difficult to determine exactly how the system will work. A very important example of this is the almost complete lack of indication or constraints in the Law on how the technical means will function. But it is clear that the measures envisaged will potentially give the authorities, and Roskomnadzor in particular, enormous control over the entities that run the Internet.

Some of the powers that experts have suggested this Law would give the government include:

- To block access to parts or all of the global Internet in Russia.
- To shut down the Internet entirely within Russia.
- To block certain traffic or types of traffic (described by some observers as the power "to conduct fine-grained censorship").
- To monitor Internet traffic very closely, including by conducting close surveillance of the communication activities of certain actors, without the need for any further authorisation (such as from a court).

Clearly if centralised management were actually imposed all of these risks would be much greater. Indeed, in that case, blocking access to parts of the global Internet or even cutting Russia off from it entirely would likely be a key objective. Essentially, in case of centralised management, the government would have direct control over most of the Internet in Russia.

These powers all represent serious breaches of international law regarding freedom of expression. For example, in their 2011 Joint Declaration, the special international mandates (rapporteurs) on freedom of expression at the UN, OSCE, OAS and African Commission stated:

> Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.[26]

It is particularly problematical that these powers could all be initiated and conducted in a completely non-transparent manner and by bodies which are either part of government or lack independence from government, and often without external actors even being aware that they were taking place. The rules also envisage very limited judicial oversight, given that they explicitly allocate broad discretion to various authorities.

Perhaps ironically, the one thing that these measures do not appear to ensure is security online. Russia does not have a carefully researched cyber security policy and the specific systems put in place by this Law do not seem to be logically connected to increasing cyber security. Certainly they do not reflect the sorts of measures put in place by other countries which have devoted serious attention and effort to online security.

6. Conclusion

Three of the five major legal reform packages governing digital communications that are analysed in this Briefing Note were adopted only in 2019 while implementation of the other two, adopted in 2016, was delayed due to technical challenges. As a result, it is far too early to determine what their real impact will be. However, we can identify a number of features that are of grave concern to freedom of expression and privacy online.

The "Disrespect for Authority" and "Fake News" Laws provide for measures to be taken against a wide range of largely undefined online content, much of which was not previously prohibited under Russian law. International standards largely rule out the prohibition of these types of content and this problem is significantly exacerbated by the fact that key terms in both

[26] Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, para. 3(a). Available at: https://www.law-democracy.org/live/legal-work/standard-setting/.

Laws are undefined. Significantly, well over one-half of all of the cases so far under the "Disrespect for Authority" Law have involved statements about the President.

In addition to expanding the scope of prohibited content, both of these Laws also give the Russian authorities highly discretionary powers to block or takedown content immediately upon a decision of the Prosecutor General, in some cases without even notifying the owner or person who is responsible for the content. While these measures may be challenged in court, the content will remain taken down or blocked unless and until a court determines that the measures were not legitimate, which would normally take many months or even years.

Pursuant to the "Yarovaya" Laws, data retention obligations – covering both metadata and the actual content of communications – have been massively extended, to the point where it remains unclear that it is even technically possible to retain such a large amount of data. The rules provide for access to this data, including with decryption keys, where necessary, by the Federal Security Services (FSB) and other law enforcement bodies, in some cases without obtaining a court order. As such, these Laws given the authorities substantially expanded powers to conduct surveillance of online activity over what was provided for previously by the System for Operational Investigative Measures (SORM). This represents a serious breach of the rights to both privacy and freedom of expression.

The true implications of the "Sovereign Internet" Law are perhaps the most difficult to assess. Although the Law ultimately gives the authorities the power to undertake centralised management of the Russian Internet, many observers believe that its real purpose lies elsewhere. In particular, the Law provides for various preparatory measures, so as to be ready for centralised management should it prove necessary, which include requiring Internet access providers to install "technical means", provided free of charge by Roskomnadzor, to counter threats. A pilot implementation for this Law involves technical means which allow for DPI (deep packet inspection) and for the blocking of illegal content. As a result, it empowers Roskomnadzor both to undertake close surveillance of the communication activities of selected actors and to conduct fine-grained censorship, in each case without the need for any further authorisation (such as from a court).

Respect for freedom of expression in the Russian Federation has declined significantly since Vladimir Putin returned to the post of President in 2012. The five major legal reform packages governing digital communications analysed in this Briefing Note represent an important escalation of that decline. Indeed, if used to their full potential, they would allow for extensive censorship of online communications and virtually unlimited surveillance of those communications.

Note on Authors

Toby Mendel is the Executive Director of the Centre for Law and Democracy (CLD), a Canadian-based human rights organisation which focuses on legal and policy work regarding foundational rights for democracy, defined to include freedom of expression, the right to information, freedom of association and assembly and the right to participate. Since Toby founded CLD in 2010, it has grown to be recognised as a leading global voice, especially on freedom of expression and the right to information. Prior to founding CLD, Toby worked for over 12 years as the Senior Director for Law and Article 19, an international organisation focusing on freedom of expression.

Galina Arapova is the Director of the Mass Media Defence Centre (MMDC), a human rights NGO based in Russia. Since MMDC was founded in 1996, it has become a prominent Russian freedom of expression and media protection NGO with a strong focus on legal assistance to media professionals. Galina is a practising media lawyer with a very well-established practice in defending media and journalists in domestic courts and before the European Court of Human Rights. She has vast experience as a media law expert and trainer, conducting training for journalists, lawyers, judges in Russia, CIS countries, Eastern Europe and Sweden. She is member of the Russian Press Council (a media self-regulation body, see: www.presscouncil.ru), vice-chair of the international board of international media freedom organisation Article 19 (based in London, UK), trustee of the European Center for Press and Media Freedom (based in Leipzig, Germany), and a member of the High-Level Panel of Legal Experts on Media Freedom.