Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**573**
Land:	Rusland
Kilde:	RSF – Reporters Sans Frontières
Titel:	“Taking Control?” Report by RSF on internet censorship in Russia
Udgivet:	28. november 2019
Optaget på baggrundsmaterialet:	22. januar 2020

TAKING CONTROL?

INTERNET CENSORSHIP AND SURVEILLANCE IN

RUSSIA

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

A digital version of this report with links and references can be found online:
www.reporter-ohne-grenzen.de/russiareport

A REPORT BY REPORTERS WITHOUT BORDERS/ NOVEMBER 2019

© pixabay

TABLE OF CONTENTS

PREFACE

Today the internet is thought to be a strategically crucial sector in Russian politics although for a long time those in power in the Kremlin did not recognise its importance. Ten years ago, the virtual space in Russia was still a place where lively debates about problems in society and politics unfolded. In the future, it is planned to be censored and surveilled, if possible, centrally, according to Russia's new "sovereign internet law".

The present report traces the development from the first bans on content in 2012 to the present day. It shows how critical editorial teams are put under pressure and how the authorities attempt to silence individual journalists and bloggers. It provides information about new online media that report on societal ills against all odds, and it raises the question about the relevance of international platforms for the freedom of expression in Russia.

This report is based on about 30 interviews with journalists and activists, lawyers and human rights defenders conducted by Reporters Without Borders (RSF) Germany press officer Ulrike Gruska and RSF Germany board member Gemma Pörzgen in Moscow and Berlin. We would like to thank our dialogue partners for their openness and their patience in explaining the political and technical background of internet censorship in Russia to us. It was only with their help that we have been able to comprehensively portray the situation in Russia, which is ranked 149th of 180 countries in RSF's 2019 World Press Freedom Index.

←
Nothing remains hidden from the Kremlin: the human rights organisation *Roskomsvoboda* used this image to illustrate the news of a law banning anonymous communications via messaging services.

1 OVERVIEW

Regulation of the Russian internet began in 2012, initially mostly in reaction to domestic events. Up until then, the government had taken little notice of political debates in the virtual space–after all, its power had been supported reliably by the state-controlled television channels for decades. They were the main sources of information for the majority of the population. But the discontented members of the public who in the winter of 2011/12 gathered for the biggest demonstrations since the end of the Soviet Union no longer took television seriously.

↓
Internet censorship in Russia began during the 2011-2012 protests.
© RSF Germany

ONLINE MEDIA INSTEAD OF TV NEWS

Television is losing influence in Russia as more and more people get their information on the internet. This is documented by a study published by the Levada Centre, an independent polling agency in August 2019: ten years ago, 94 percent of Russians obtained their information about domestic and international politics mostly from television, but that number has dropped to only 72 percent. People under 35 in particular tend to learn about current events through social networks and online media. According to the study, television has lost much of its credibility: over half the population think that TV reporting in particular on business and economics does not correspond to reality. The share of those who regularly watch the state *Pervyy Kanal* (English: *Channel One*) has decreased from 72 percent (March 2018) to 47 percent (March 2019) within a year, while one third of the population regularly follow video blogs (even as many as two thirds among 18 to 25-year-olds). Trust in online media and social networks is growing; 56 percent of the population (85 percent of 18- to 25-year-olds) use social media daily or multiple times per week. The number of those using messaging services for text messages or phone calls has doubled in the past three years, according to the study: from 31 percent of the population (2016) to 62 percent. The trend towards greater use of online services and media is also reflected in the development of the Russian advertising market: 2018 was the first year in which businesses invested more money in advertising on the internet (approx. Rb 203 billion, €2.8 billion) than on television (approx. Rb 187 billion, €2.57 billion). The internet is also the fastest growing advertising sector (22 percent growth compared to 2017), while growth in TV advertising is slowing.

Across the country, tens of thousands protested against election fraud and against Vladimir Putin, who had become president for the third time. They organised their protests online, using Facebook and its Russian equivalent VKontakte to arrange rallies. They documented irregularities during the parliamentary election on December 4th 2011 and published live videos from polling stations on the website of the Russian human rights organisation *Golos*. They used social media to raise money for protests and exchanged information about individuals who had been arrested. The demonstrations were the top news topic in critical online media for months.

The state leadership was completely unprepared for the enormous impact of this decentralised protest movement organised online–and it reacted promptly: just one month after Putin had begun his third term, the Russian parliament discussed a law, in its first reading, introducing a blacklist of websites that were to be blocked. It was used to ban various content in the following years: articles presenting homosexuality as normal, blog posts that allegedly offend religious sentiments or call for extremism and posts using swearwords. The state's media regulator *Roskomnadzor* was granted the right to block websites without a court order.

↑
A live broadcast of Putin's annual press conference
© dpa

At the same time, the editorial departments of media critical of the Kremlin were targeted and put under pressure. Besides popular news websites, this had a particular impact on the liberal business media, whose investigative research about politically explosive topics had found a broad online readership. The authorities also cracked down on individual users who did not take the officially desired view: from 2015 to 2018, several hundred people per year were subjected to criminal prosecution because of their online activities and dozens were sentenced to prison. The victims of prosecution are not only media professionals or politically active bloggers. People who simply forward images or texts or click on "like" in the wrong place may end up in prison.

The foreign policy developments surrounding Euromaidan in Kiev, the war in eastern Ukraine and the annexation of Crimea in 2014 were an important turning point. It exacerbated the confrontation with the EU and the United States and, from the perspective of the Russian government, it also increasingly made the internet a battleground. Time and again, the media reported about a "troll factory" in St. Petersburg that allegedly coordinated targeted disinformation campaigns in Ukraine and beyond. Pro-Kremlin comments flooded discussion forums and news pages in various countries. In return, NATO declared cyber-attacks to be an integral part of military conflicts. The United States toughened its cyber strategy in the autumn of 2018, calling Russia one of its main strategic adversaries. Russia's "sovereign internet law" was introduced to parliament in late 2018 as a direct reaction to the new American cyber strategy, yet its origins can be traced back to the beginning of the Ukraine crisis.

Since 2018, the Russian authorities have increasingly been focusing their attention on international platforms such as Google, Facebook and Twitter. They are required by law to remove content banned in Russia and to store Russian citizens' personal data exclusively on servers in Russia. For a long time, the authorities merely issued verbal threats if these laws were not obeyed. In the meantime, fines are imposed and laws made more stringent to allow fines running into millions. Whereas Google is partly cooperating with the authorities, Twitter and Facebook have refused to do so to date.

In 2019, many of the developments described in this report reached an all-time high. Russia's "sovereign internet law", adopted in May, takes internet censorship in Russia to a new level: the government is attempting to gain control over the infrastructure of the web. It is seeking to block content even more effectively, surveil communication completely and, if necessary, be able to cut the Russian internet off from the worldwide web. In the spring, thousands of people protested against this law and for the freedom of the internet. In the summer, tens of thousands took to the streets for a greater voice in politics. Hundreds of demonstrators were arrested and quite a few were sentenced to prison. At the same time, independent online media and civil society organisations' information portals that resist the Kremlin's dictates experienced an unimagined wave of support.

THE DIGITAL ECONOMY IS BOOMING

Using apps to pay for parking, make a doctor's appointment or settle the bill in a restaurant is commonplace for people in major Russian cities. Free Wi-Fi is available in most public places, certainly in hotels and restaurants and even dozens of metres below ground on the Moscow Metro. Network infrastructure is well developed, broadband internet is the norm in big cities. At least for mobile internet, prices are among the lowest worldwide since a large number of Russian mobile network operators are competing for customers seeking fast and cheap mobile internet service for their smartphones or tablets. More than three quarters of the population in Russia are online regularly, the Russian Association for Electronic Communications (RAEC) estimates the number of active internet users to be roughly 93 million. In 2018, the digital economy accounted for roughly 4 percent of Russia's gross domestic product (Rb 3.9 trillion, approx. €54 billion)–an increase of 11 percent compared with the previous year, and the upward trend is continuing. The digital sector, particularly online retailing, is growing many times faster than other sectors of the economy; Russian companies have great hopes for exports in particular. "The digital economy is one of the most successful sectors of the Russian economy", Dmitry Kononenko of the German-Russian Chamber of Foreign Trade told RSF Germany. "E-commerce grew by 60 percent last year and Russian software is on its way to becoming the sixth largest export product." The state's efforts to increasingly control and restrict its citizens' internet traffic, he added, were endangering precisely that segment of the economy in which Russian companies were competitive internationally.

2 LAWS RESTRICTING PRESS FREEDOM AND FREEDOM OF EXPRESSION

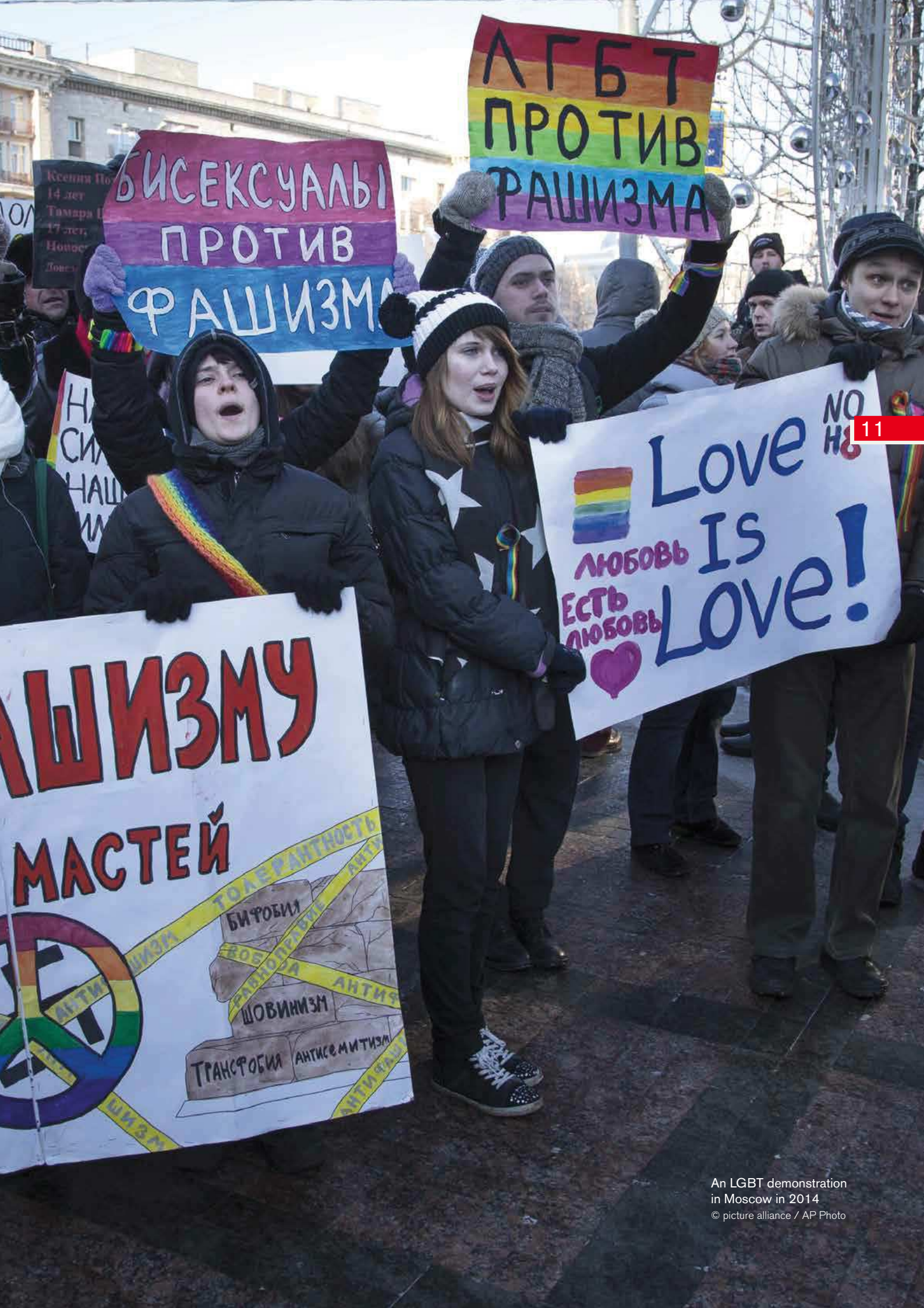
CHRONOLOGY FROM 2012 TO 2019

Introduced in 1991, shortly after the collapse of the Soviet Union, Russia's Law on Mass Media was widely regarded as one of the most progressive in Europe at the time. It bans all forms of censorship and guarantees the freedom to establish private mass media. But since the widespread protests of 2011/2012, the Russian parliament has passed a number of laws that restrict journalists' work and internet users' freedom of expression. These laws prohibit certain types of content, step up data traffic surveillance measures and state control over internet infrastructure, and limit the influence of foreign media companies. Many of them were rushed through the Russian parliament and are legally flawed, or they apply to circumstances that are already dealt with elsewhere. In many cases, the regulations are vaguely worded and open to interpretation and, as a result, they can be used to suppress unwanted reporting or discussion on social media and to impose penalties arbitrarily.

Blacklist of websites subject to blocking

Federal Law No. 139-FZ of July 28th 2012,[1] which entered into force on November 1st 2012, introduced a blacklist of websites and URLs subject to blocking. The list, which is also known as the Unified Register of Prohibited Sites or single register, is managed by *Roskomnadzor*, the Russian state's media regulator, and is not accessible to the public. Once a website appears in the register, *Roskomnadzor* instructs the site's hosting provider or the owner of the social network or website to remove the relevant material. If the material is not removed, all internet providers in the country are required to block access to the site. According to the Russian human rights organisation *Roskomsvoboda,* at the beginning of November 2019 the register contained more than 290,000 entries.

[1] Unless otherwise stated, the dates in this chapter refer to the day the legislation in question was signed into law by President Vladimir Putin–the final stage in the legislative process before publication of the law.



An LGBT demonstration in Moscow in 2014

ROSKOMNADZOR: THE STATE'S MEDIA REGULATOR

Roskomnadzor, the Federal Service for Supervision of Communications, Information Technology and Mass Media, is the Russian supervisory authority responsible for mass media, telecommunications and data protection. It was established in 2008 and has been headed by Alexander Zharov since May 2012–which was when Vladimir Putin's third term as Russian president began. Under Zharov, *Roskomnadzor* has evolved from a small authority with a few dozen employees into an influential state body with more than 2,700 employees and local branches across the country. *Roskomnadzor* is responsible for radio licensing and the registration of mass media. In April 2019, the authority refused to issue registration certificates to several media outlets that are critical of the government. It oversees compliance with the media laws and is empowered to issue warnings to editorial offices that are allegedly failing to comply. Media outlets that receive two warnings within twelve months face immediate closure. In addition, *Roskomnadzor* manages various official registers, including the list of websites subject to blocking and the register of "organisers of dissemination of information". One of the first web pages to be banned by the authority was a public safety video made by a train company in Melbourne, Australia, warning people to be careful on train platforms. *Roskomnadzor* viewed the prize-winning video and viral hit in which animated characters die in various ways as propaganda for suicide. In 2019, the case of *Park Gagarina*, a news website based in the city of Samara in southwestern Russia, drew derision when it was fined for not updating its page on a weekend when it claimed there was no news to report. The website responded by launching a section in which it reports on absurd decisions by the media regulator.

Defamation recriminalised

In July 2012, two months after Putin was sworn in as president again, Russia's lower house of parliament, the State Duma, passed Federal Law No. 141-FZ, which reincorporated a controversial section on defamation into the country's Criminal Code. Defamation had been decriminalised and the corresponding section transferred to administrative law only a few months earlier in December 2011. Every year hundreds of people are charged with defamation in Russia, most of them journalists and bloggers based outside Moscow. The plaintiffs in many cases are public officials.

Definition of treason and espionage expanded

In November 2012, the State Duma passed Federal Law No. 190-FZ, which tightened the regulations on treason and espionage and expanded the definition of these crimes. Since this amendment, all activities directed against the security of the Russian state fall under the definition of treason. This was previously limited to activities directed against the "external security" of the Russian state. Under the new provision, individuals can be charged with espionage even if they were not working for a foreign intelligence agency. The penalties for violations were increased to fines of up to Rb 500,000 (approx. €7,200) or eight years' imprisonment.

Ban on swearwords

In April 2013, Federal Law No. 34-FZ, which bans the use of swearwords in the media, was added to the 1991 Law on Mass Media. The ban applies to journalists, their interview partners and readers' comments. The law stipulates penalties of up to Rb 200,000 (approx. €2,900) for broadcasters and publishers. There is no official list of prohibited language. The Russian state media monitoring agency *Roskomnadzor* decides which words violate the law on a case-by-case basis.

Ban on insulting religious feelings

Federal Law Nr. 136-FZ, an amendment to Article 148 of the Russian Criminal Code adopted in June 2013, criminalises actions that insult religious beliefs. Offenders face fines of up to Rb 200,000 (approx. €2,900) or one year in prison. The regulation does not clearly define what constitutes an action that "expresses clear disrespect for society" and aims to "insult the religious feelings of believers". It was initiated after the feminist punk rock band Pussy Riot performed its "punk prayer" in the Cathedral of Christ the Saviour in Moscow in February 2012.

Ban on "homosexual propaganda"

Federal Law No. 135-FZ of June 2013 bans the spreading of propaganda for "non-traditional sexual relations" in the presence of minors. It therefore also applies to journalistic reporting on LGBT issues, and even prohibits statements that portray "non-traditional sexual relations" as normal. Broadcasters and publishers found to be in breach of the law face fines of up to Rb 1 million (approx. €14,300). Access to the articles in question can also be blocked and media outlets closed down for up to 90 days.

Websites can be blocked without a court order

Passed in December 2013, Federal Law No. 398-FZ (also known as the Lugovoy law) empowers the authorities to block–within 24 hours and without a court order–online content that calls for "mass riots, extremist activities, or participation in unsanctioned mass public events that disturb public order". If the Prosecutor General's Office instructs media regulator *Roskomnadzor* to block such content, internet providers must react within 24 hours and block access to the relevant sites. Before this law, only very few types of content could be blocked without a court order, for example, child pornography or content that breached copyright.

→
Andrey Lugovoy, a former Russian intelligence officer, now a member of the State Duma

Harsher penalties for separatist appeals

Although "appeals for separatism" are already forbidden as a form of extremism under Article 280 of the Russian Criminal Code, the State Duma amended the law to include a new section in December 2013. Article 280.1 makes "public calls to action aimed at violating the territorial integrity of the Russian Federation" a punishable offence, and it was amended shortly afterwards to apply not only to mass media but explicitly to the internet as a whole. In the following years, more than a dozen people were charged under this article–in most cases for questioning the claim that Crimea belongs to Russia.

Law on bloggers and "organisers of dissemination of information"

Federal Law No. 97-FZ of May 2014 introduces the term "organisers of dissemination of information" on the internet. The term is broadly defined to apply to any person or entity that enables users to communicate with each other–including providers of social networking services and messaging apps. The law requires media monitoring agency *Roskomnadzor* to set up a national database in which all "organisers of dissemination of information" must be registered.

↓
The personal data of Russian citizens may now only be stored on servers in Russia.

All services registered in the database are obliged to store certain user data and make these available to the law enforcement agencies, as well as assist them in monitoring users' communications. The regulation applies to the Russian social networking sites VKontakte and Odnoklassniki and e-mail service Mail.ru, among others. The first foreign service to be added to the register was the Swiss messaging app Threema in March 2017, followed by messaging app Telegram in June 2017 and dating website Tinder in May 2019. More than 180 "organisers of dissemination of information" are currently registered with *Roskomnadzor* (as of November 1st, 2019).

The law also required Russian bloggers with more than 3,000 unique visitors per day to register as news media with *Roskomnadzor*. As such, they were subject to the same legal obligations as mass media, but without the constitutional protection and privileges enjoyed by the latter. More than three years later, in July 2017, this regulation was repealed by Federal Law No. 276-FZ (see below).

Data storage in Russia

The vague wording of Federal Law No. 242-FZ of July 2014 (which entered into force on September 1st 2015) stipulates that the personal data of Russian citizens may no longer be stored on servers located outside Russia but only on servers inside the country. The law applies to providers of e-mail services, social networks, search engines and other online services, including foreign services such as Google, Facebook and Twitter. Access to the US business and employment networking service LinkedIn was blocked in Russia in November 2016 after the network refused to comply with this requirement.

Restrictions on the activities of foreign publishers

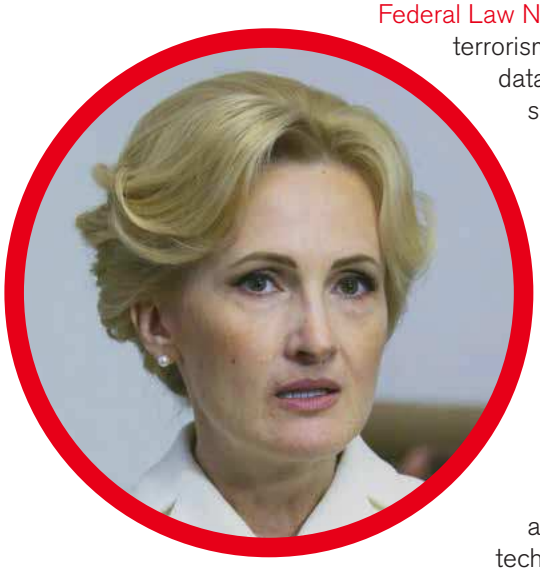
Federal Law Nr. 305-FZ of October 2014 (which went into effect on January 1st 2016), restricts foreign ownership in Russian media organisations to 20 percent. Supporters of the measure said it was designed to protect national security interests. Before this provision was introduced, there were no limits on foreign stakes in Russian print and online media, and foreigners could own a stake of up 50 percent in radio and television broadcasters. Many foreign companies consider a 20 percent stake to be financially unviable. The legislation prompted the *Axel Springer group* to give up its activities in Russia at the end of 2015, after more than ten years in the country, and the licence for business magazine *Forbes Russia*, known for its critical reporting, was transferred to Russian ownership. The Finnish media group Sanoma and Swiss publisher Edipresse were also compelled to sell their stakes in Russian media.

Further amendments to the Law on Mass Media (Federal Law No. 464-FZ of December 2015) require the media companies to inform media monitoring agency *Roskomnadzor* about any funding they receive from "international sources"–a term that is broadly defined in the law.

News aggregators accountable for content

Under Federal Law No. 208-FZ, which was passed in June 2016 and entered into force in January 2017, the owners of news aggregator sites with over one million users per day are accountable for the content of all information disseminated via the sites– except when such content is a verbatim reproduction of content published by registered mass media outlets. The law applies to all news aggregators (including search engines and social networks) that disseminate content in Russian or other languages of the Russian Federation. Ownership of these news aggregators is restricted to Russian companies or nationals.

Large-scale data retention



↑ Irina Yarovaya initiated the tightening of the anti-terrorism laws.

Federal Law No. 374-FZ (passed in July 2016 in a package of counter-terrorism legislation known as the Yarovaya laws) stipulates extensive data retention measures: providers of telecommunications services and internet services are required to store communications metadata, for example information about who made calls or exchanged messages with whom and the times of such communications, for three years. In addition, the specific content of users' communications, including phone calls, messages, images and videos, is to be stored for six months. These data must be made available to authorities on request and without a court order. To ensure the implementation of this mass surveillance, operators are required to invest millions in equipment and the construction of new data storage facilities. Although the law entered into force in July 2018, a year later many telecommunications companies and internet service providers had yet to install the necessary technology.

Security service wants access to encrypted messages

The same law requires companies that provide e-mail and messaging services to assist the Russian security agency, the Federal Security Service (FSB), with the surveillance of encrypted messages and, if necessary, provide it with decryption keys. Failure to comply can lead to heavy fines and even to the blocking of services. It remains unclear how this regulation is to be implemented in the case of services that provide end-to-end encryption, such as the messaging app *Telegram*: messages sent using end-to-end encryption can be accessed only by the sender and the recipient. The service provider does not have access to the encryption key.

VPNs and anonymizers banned from showing blocked content

Federal Law No. 276-FZ of 29 July 2017 (which came into force on November 1st 2017) prohibits all references to content or websites that have been banned by the media regulator *Roskomnadzor.* This also applies to search engine result lists. VPN providers and internet anonymizer services are banned from providing access to banned content or websites, meaning that these services may not be used to circumvent internet censorship. The law also empowers *Roskomnadzor* to block all other sites that provide instructions on how to bypass internet censorship. Providers are required to block, within 24 hours, the internet access of services that continue to display forbidden content or provide links to this type of content despite being warned not to.

No more anonymous communication via messaging apps

Federal Law No. 241-FZ of July 29th 2017 prohibits anonymous communication via messaging applications. All services that are defined by law as "organisers of information dissemination" (see above, Federal Law No. 97-FZ of May 2014) are required to verify the identity of their users by their mobile phone numbers and are banned from providing their services to persons who have not provided clear proof of identity. After several delays, this regulation entered into force in May 2019. Companies that provide messaging services must block access to their services for anyone who does not provide clear proof of identity. Messaging applications that fail to implement the new regulations can be completely blocked in Russia. In addition, they are required to block user accounts that are used to spread "illegal content".

↑
The FSB wants access to the content of encrypted communications sent via messaging services.
© pixabay

Media as “foreign agents”

Under Federal Law No. 327-FZ of November 25th 2017, media outlets that are registered abroad or receive foreign funding must register with Russia’s Ministry of Justice as “foreign agents”. The law was passed after US authorities forced Russian international broadcaster *Russia Today (RT)* to register as a “foreign agent” in the United States under the Foreign Agents Registration Act. Media outlets subject to the law must mark all their publications or broadcasts with the disclosure that they are a “foreign agent”, and they are also required to disclose their finances in detail. The first media outlets to fall within the scope of the regulation were the US international broadcaster *Voice of America* and *Radio Free Europe/Radio Liberty (RFE/RL)* and several *RFE/RFL* regional services, including those in Crimea (annexed by Russia in 2014), Siberia and the North Caucasus region.

Immediate deletion of defamatory information

Federal Law No. 102-FZ of April 23rd 2018 deals with information that may discredit the honour and dignity of a person or the business reputation of a person or company. In court proceedings, judicial officers are empowered to have websites containing this information blocked if the defendant fails to delete it within the specified period of time. Before this law came into effect, they could merely levy a fine in such cases.

Harsh penalties for search engine operators

Federal Law No. 155-FZ of June 27th 2018 is an amendment to Federal Law No. 276-FZ from 2017 (see above) and stipulates harsh penalties for search engine operators that link to prohibited content or display this content in their search results. Companies face fines of between Rb 500,000 and Rb 700,000 (approx. €6,800 to €9,600). The same penalties apply for search engine operators that have failed to connect to the state “Register of prohibited websites” (see Federal Law No. 139-FZ of July 2012). The law also prescribes penalties for providers that fail to pass on information to the media regulator *Roskomnadzor* about an individual or company that offers VPNs and anonymizer services through its servers within the specified period of time.

↓
Soldiers are no longer allowed to take selfies while on duty.

Prison sentences for not deleting prohibited content

Two laws enacted on October 2nd 2018 tighten the penalties for providers that fail to remove online content that has been prohibited by court order. In extreme cases, offenders face up to two years' imprisonment. Federal Law No. 347-FZ stipulates fines of up to Rb 20,000 (approx. €270) for private individuals who fail to delete prohibited content within the specified time limit. For repeat offenders, up to ten days of detention may be imposed. Federal Law No. 348-FZ introduces the criminal offence of "malicious disregard" of a court decision.[2] For this offence, private individuals face fines of up to Rb 50,000 (approx. €700) or a year's imprisonment; state employees or employees of companies and organisations can be punished with fines of up to Rb 200,000 (approx. €2,700) or two years' imprisonment.

Soldiers banned from using smartphones

Federal Law No. 19-FZ of March 6th 2019 bans soldiers from using smartphones while on duty and also from posting photographs or information on social media that show them or their comrades on duty or that show weapons or allow conclusions to be drawn about their deployment location. The law was a response to public discussion of military operations which the Russian government would have preferred to keep secret (at the time). For example, in 2015, photographs from Syria showing preparations for a Russian military intervention circulated on social networks–several weeks before the Russian parliament voted on the operation. In 2014, Russian soldiers posted images from eastern Ukraine at the same time as the Russian government was denying any involvement in the fighting there. Russian media reported that dozens of soldiers were sentenced to between five and fifteen days' detention in the first four months after the law came into force.

Ban on "fake news" and "disrespect" towards the state

A package of four laws passed on March 18th 2019 targets the dissemination of content considered to be "fake news" and "disrespectful" statements about the state and its organs. Federal Law No. 31-FZ prohibits the dissemination of "socially relevant information" that has the appearance of a factual report but is deemed by the Prosecutor General's Office to be false, and therefore constitute a "threat to people, property or public safety and order". The media monitoring agency *Roskomnadzor* is empowered to delete such information with immediate effect. Federal Law No. 27-FZ stipulates fines of up to Rb 400,000 (approx. €5,500) for individuals and up to Rb 1.5 million (approx. €20,500) for companies that disseminate this information.

Federal Law No. 30-FZ prohibits the dissemination of information that shows "blatant disrespect for society, the government, official symbols of government, the constitution or government bodies". For violations of this regulation, Federal Law No. 28-FZ stipulates fines of up to Rb 100,000 (approx. €1,400). Offenders who repeatedly "disrespect" state power or disseminate "disrespectful" statements can be fined up to Rb 300,000 (approx. €4,100) or sentenced to up to 15 days in prison. By the end of August 2019, fines for "disrespect" had been levied in at least 36 cases, most of them concerning remarks about President Vladimir Putin on social network VKontakte.

---

[2] Russian: "'злостное нарушение' решения суда". This law amends Article 315 of the Russian Criminal Code.

Russia's "sovereign internet law"

➲ The **Domain Name System** (DNS) is the internet equivalent of an address book. It translates domain names that humans find easy to remember (for example, www.rsf.org) into numerical Internet Protocol (IP) addresses that can be processed by computers. It is stored on thousands of servers across the globe. In an uncensored system, any website can be called up by the DNS's many servers. A national Russian DNS that internet providers were obliged to use would allow the Russian authorities to block specific user requests and exclude the possibility of attempts to circumvent this. At present, the use of alternative DNS servers that the Kremlin cannot control because they are operated from outside the country is still possible from within Russia.

Federal Law No. 90-FZ of May 2019 stipulates that in future a larger proportion of Russian internet traffic will be routed through servers located inside Russia. The stated purpose is to create a more independent Russian internet and ensure that it is able to continue functioning in the event of disruptions or cyberattacks from outside the country. Some of the law's provisions came into effect at the beginning of November 2019, while others will enter into force on 1 January 2021.

The law provides for the following measures. First, Russian telecommunications companies and internet service providers are to route internet traffic exclusively through domestic **internet exchange points (IXPs)** that are registered with the media monitoring agency *Roskomnadzor*. Second, all internet service providers are to install **new technology**[3] that enables *Roskomnadzor* to centrally block websites and reroute internet traffic. This would mean that it would no longer have to rely on the assistance of providers that have not always followed the government's instructions in the past. Third, a **national Domain Name System** is to be set up, which providers will be required to use from January 1st 2021. Fourth, a new control centre is to be established that would be subordinate to *Roskomnadzor* and able to centrally monitor and censor the flow of information in Russian cyberspace if necessary.[4]

3 The law does not specify what technology is to be installed. It seems likely that, among others, the Russian state has Deep Packet Inspection in mind–a technology that makes it possible to examine unencrypted content in electronic communications as they are being sent (see Chapter 6).

4 For details about the content and background of this law, see: Burkhardt, Fabian: *Russlands „Souveränes Internet". Digitale Abschottung nach außen und verstärkte Kontrolle im Inneren* (SWP-Aktuell 2019, December 2019).

RUSHED AND VAGUELY WORDED

Many of the laws that have come into force since 2012 were rushed through the Russian parliament, in some cases with just a few weeks between the first reading in the State Duma and their signing into law by the president. An extreme case was the law on the deletion of defamatory information, which went through all three parliamentary readings within a few days and was approved with equal speed by the Federation Council, the upper house of the Federal Assembly (the Russian parliament). When defamation was recriminalised in July 2012, the whole procedure was completed within just three weeks–in the middle of the summer break.

"In many cases, it is only years later that the consequences of these laws become apparent," Artem Kozlyuk of human rights organisation *Roskomsvoboda* said in an interview with RSF. He added that those who draw up the laws often lack the necessary digital expertise. Damir Gainutdinov, a lawyer for human rights organisation *Agora*, explained that many of the regulations are vaguely worded and open to interpretation, and consequently they can be used to stifle unwanted reporting and discussion on social networks. "Their arbitrary application creates a climate of uncertainty and fear," he said. "We are manoeuvring in a grey area filled with unclear legislation," said Anastasia Lotareva, editor-in-chief of online magazine *Takie dela*, describing the situation.

↑
The Kremlin controls most of the television channels, but it has not been able to do the same on the internet yet.


ЗАЧЕМ
ПРЕДВЫБОРНО
ДАЛИ СТРАНУ ВТО ?
ВСТАВАЙ, ПРОКЛЯТЬЕМ ЗАКЛЕЙМЁННЫЙ!
ПУТИН ВРУН

3 CHANGES OF OWNERSHIP AND DISMISSALS: EDITORIAL DEPARTMENTS UNDER PRESSURE

The websites *Gazeta.ru* and *Lenta.ru*, both founded in 1999 by Russian internet pioneer Anton Nosik, and the TV channel *TV Dozhd* were among the first widely read independent online media. Their audience grew enormously during the mass protests of 2011/2012–and they were then the first to experience the state's crackdown on freedom of expression on the internet. Shortly afterwards, traditional online and offline business media whose investigative reporting and politically explosive stories attracted attention were targeted, too. Recalcitrant editors-in-chief were either fired or chose to leave. Foreign investors were pushed out of the country, and publishing houses were taken over by entrepreneurs with close ties to the Kremlin. The state's media regulator *Roskomnadzor* put pressure on critical editorial teams by issuing warnings and blocking entire websites.

←
Tens of thousands of people took to Moscow's streets in December 2011 to protest against election fraud and Vladimir Putin.
© dpa

The mass protests in 2011/12 were a turning point for the internet portals *Gazeta.ru* and *Lenta.ru*. They were enormously popular during the demonstrations because of their well-founded critical reports on the events, but their reporting changed considerably in the following years. As early as November 2011, *Gazeta.ru* lost its deputy editor-in-chief Roman Badanin,[1] who resigned following a conflict with management: he had refused to put advertising banners of the Kremlin party, United Russia, on the website two weeks before the parliamentary election. Instead, he sought support for a project of the human rights organisation *Golos* that called on people to document irregularities at polling sites. After the controversial election on December 4th 2011, banker Alexander Mamut, who has close ties to the Kremlin, bought *Gazeta.ru*. Editor-in-chief Mikhail Kotov left in March 2013. A few months later, almost the entire politics desk was replaced, and *Gazeta.ru* became a news portal whose reporting was mostly meaningless.

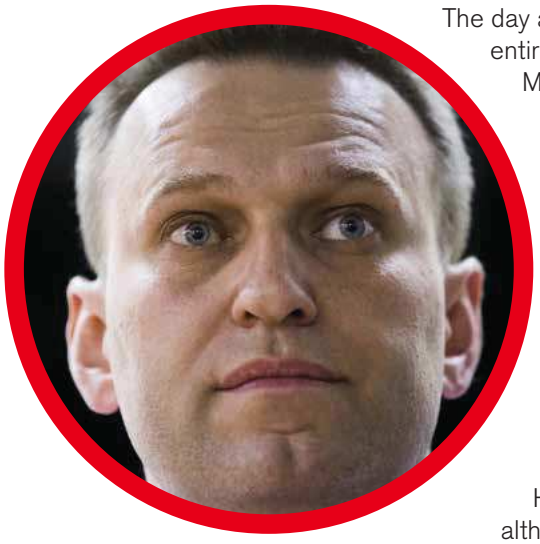
↓
Businessman Alexander Mamut
© picture alliance / Stanislav Krasilnikov / TASS / dpa

[1] Badanin later worked as editor-in-chief of *Forbes Russia*, the news agency *RBC* and *TV Dozhd* and founded the not-for-profit investigative portal *Proekt* in 2018 (see Chapter 4).

↑
Meduza founder Galina Timchenko
© picture alliance / AP Photo

Shortly afterwards, the politics desk of the online newspaper *Lenta.ru* was also replaced. *Lenta.ru* was one of the most often quoted media on the Russian internet following the protests of 2011 and 2012. It was known for its extensive coverage of anti-Putin activists such as the punk band Pussy Riot or opposition politician Alexei Navalny. On March 10th 2014, *Lenta.ru* published an interview with a leader of the Right Sector in Ukraine–the right-wing extremists that Russian state media called the leaders of the "fascist coup" on Kiev's Maidan. *Roskomnadzor*, the Russian state's media regulator, then issued a warning to *Lenta.ru* for "distributing extremist material" and the owner of the website, businessman Alexander Mamut, ordered editor-in-chief Galina Timchenko to leave her position "within a matter of seconds". But the respected journalist, who had headed *Lenta.ru* for ten years, had her colleagues on her side: in an open letter to their readers, the editorial team complained almost unanimously about "censorship" and about the new editor-in-chief who, they claimed, had come "directly from the offices of the Kremlin". Timchenko was followed by 39 staff members who left *Lenta.ru*, among them the entire politics desk.[2]

ENTIRE SITES BLOCKED FOR THE FIRST TIME



↑
Opposition politician Alexei Navalny
© picture alliance / AP Photo

The day after Galina Timchenko was fired, the authorities blocked entire sites for the first time, as opposed to individual articles: on March 13th 2014, *Roskomnadzor* ordered the blocking of the oppositional news sites *grani.ru* and *ej.ru*[3]. The website of opposition politician Garry Kasparov (*kasparov.ru*), who lives abroad, and Kremlin critic Alexei Navalny's blog on the popular platform Livejournal.com were also blocked. The Lugovoy law of December 2013 served as the legal basis. It empowers the authorities to block–without a court order–websites that call for "mass riots" or "extremist activities". The day it was blocked, a piece on *EJ* had criticised Russian state television's euphoria about the annexation of Crimea. *Grani.ru* had received a warning from *Roskomnadzor* because of a report on an art project entitled Pussy Riot Icon, among other things. However, some providers did not follow the orders as desired: although they did block access to the sites, they also provided links to information about how to circumvent web censorship.

---

[2] Around six months later, in October 2014, Timchenko and roughly 20 former *Lenta* journalists launched their new project, the online portal *Meduza*, in Riga, Latvia (see Chapter 4).
[3] *EJ*, the *Ezhednevny Zhurnal* (Daily Journal), and *grani.ru* were the best-known platforms for prominent liberal commentators.

↑
Supporters of the far-right party Right Sector demonstrating in the Ukrainian capital, Kiev. An interview with one of its leaders cost *lenta.ru's* editor-in-chief Galina Timchenko her job.
© picture alliance / Pacific Press Agency

On March 12th 2015, the World Day Against Cyber Censorship, RSF unblocked *grani.ru* and other banned websites from other countries: they were mirrored (that is, copied) and placed in the clouds of major server providers such as Amazon, Google and Microsoft. The only way to block them there would be to block the entire cloud–which would entail significant economic damage. The editorial department of *grani.ru* then mirrored the contents of its site again multiple times–yet *Roskomnadzor* blocked several hundred of these mirrored sites as well. Editor-in-chief Yulia Berezovskaia, who by that time was living in exile in France, announced that *grani.ru* had moved to the domain graniru.org for this reason.

© Robin Grassi / RSF

Since then, there have been many cases in Russia of online media being blocked in their entirety. In May 2016, *Roskomnadzor* had the news site *Krym Realii*, which was operated by *Radio Free Europe/Radio Liberty*, blocked after it had published an interview with a representative of the Crimean Tatars. The Prosecutor's Office claimed that the website incited hate and extremism. The news site *Russiangate*, which had published investigative articles about organised crime and corruption in the state leadership, was shut down completely in 2018. On January 23rd 2018, it published a report about real estate owned in secret by Alexander Bortnikov, the head of the Federal Security Service (FSB), Russia's domestic intelligence service. *Roskomnadzor* subsequently blocked the site within a few hours without any advance warning, allegedly because of extremist content. The next day editor-in-chief Alexandrina Yelagina was fired, the investors withdrew their financial support for the project, and the editorial department discontinued its work.

On July 14th 2019, the news site *Fortanga* in the North Caucasus Republic of Ingushetia was also blocked on the instructions of *Roskomnadzor.* As is so often the case, the reason given was that the site was disseminating "extremist material". *Fortanga* had been established in October 2018 following protests by the local population against changes to the administrative border with the neighbouring Republic of Chechnya. The site publishes critical reports about the work of the Ingush authorities and documents persecution of activists. A number of former members of *Fortanga's* editorial team were arrested shortly before the site was blocked. One of them stated that he had been tortured in prison. Akhmed Buzurtanov, the founder of *Fortanga*, said that the impact on its readership of the site being blocked had been minimal since most people followed its reporting on social media and messaging services such as YouTube, VKontakte, Instagram and Telegram. A few days later, the site was accessible again in Russia, he added.

↓
Protests in Ingushetia against the new border with neighbouring Chechnya

BUSINESS MEDIA UNDER PRESSURE

↑
Regina von Flemming was CEO of publishing group Axel Springer's Russian division.
© dpa

Traditional media have also come under increasing pressure because of the new laws. This has mostly affected Russian online and offline business newspapers and magazines whose investigative reporting and politically explosive stories attracted attention. In October 2015, the Russian edition of *Forbes Magazine*, which is highly regarded for its professional investigative reporting, saw a change of ownership. The background was a law limiting foreign interests in Russian media to at most 20 percent. It entered into force in January 2016. For this reason, the *Axel Springer Group*, which had originally held the Russian licence for *Forbes*, left Russia entirely after more than ten years. The new owner of *Forbes Russia*, businessman Alexander Fedotov, announced that the publication would avoid "the political realm" in future. In the following years, multiple editors-in-chief left the magazine because of his major interference in the editorial work. The smouldering conflict between the owner and the editorial department escalated in the summer of 2018, and Fedotov sold the magazine to the North Caucasian businessman Magomed Musaev, who promised to observe the independence of the editorial work and brought a number of journalists back to *Forbes Russia*.[4] The editorial team celebrated the magazine changing hands again as a victory in the struggle against political influence–yet it is an open question whether Musaev will succeed in protecting the editorial department's independence.

The law limiting the activities of foreign publishers affected not only *Forbes Russia,* but also the business publication *Vedomosti.* It was established in 1999 as a joint project of the British newspaper *Financial Times,* the US newspaper *The Wall Street Journal* and the Finnish media corporation *Sanoma.* Because of the new law, the three foreign investors sold Vedomosti to Israeli-Russian media entrepreneur Demyan Kudryavtsev in 2015. In May 2017, he replaced renowned editor-in-chief Tatyana Lysova with Ilya Bulavinov, who had previously been head of internet broadcasting for the state-run TV station *Pervyy Kanal* (Channel One). In July 2017, the Russian authorities unexpectedly stripped Kudryavtsev of his Russian citizenship. In the spring of 2019, it became known that *Vedomosti* was again seeking a buyer.

The media holding company *RBC (RosBiznesConsulting)* lost its senior leadership in mid-2016 because of its critical reporting; a year later, it was sold to a publisher with close ties to the Kremlin. *RBC*'s holdings include a daily newspaper, a news agency, an online magazine and a TV station; at the time, it was the largest independent media company in Russia. *RBC's* media had made a name for themselves with their investigative research into corruption surrounding prestigious construction projects and Russia's military actions in Syria and eastern Ukraine. In the course of the international publication of the Panama Papers, they revealed offshore dealings of confidants of Putin's in April 2016. Russian media reported that the Kremlin was particularly dissatisfied that the daily newspaper *RBC* had illustrated an article on the Panama Papers with a photo of President Putin.

[4] A newly established Board of Directors, which took up its work in December 2018, is to plan the strategic development of *Forbes Russia*. Its members include Elizaveta Osetinskaya, editor-in-chief of *Forbes Russia* from 2011 to 2013 and founder of the news platform *The Bell*, and Elmar Murtazayev, editor-in-chief of *Forbes Russia* from 2014 to 2016.

↑
After 22 years as editor-in-chief of *Novaya Gazeta*, Dmitry Muratov gave up the post in November 2017. Since then he has been the chairman of the Kremlin-critical newspaper's board of directors.
© dpa - Report

The same month, the tax investigation authorities searched the business offices of oligarch and opposition politician Mikhail Prokhorov, whose corporation owned *RBC.* In mid-May 2016, Maxim Solyus, editor-in-chief of the daily newspaper *RBC,* was fired. Elizaveta Osetinskaya, director of the media holding company, and Roman Badanin, editor-in-chief of the news agency, then resigned, too. They were followed by 20 more staff members, most of them senior editors. Elisaveta Golikova and Igor Trosnikov of the state news agency *TASS* took over chief editorships. In the first editorial meeting, a recording of which was leaked to the press, they declared that journalism should observe certain rules and that a certain line was not to be crossed. In May 2017, owner Prokhorov yielded to pressure and sold his majority interest in *RBC* to publisher Grigory Berezkin, who has close ties to the Kremlin and owns *Metro*, a newspaper that is free of charge, and the tabloid *Komsomolskaya Pravda*, among others.

The reputation of the liberal business paper *Kommersant*, the most important quality newspaper in Russia in the 1990s, also suffered considerably when it became part of a media company owned by an oligarch with ties to the Kremlin. In May 2019, the paper lost its entire domestic editorial team: journalists quit in protest at the firing of their colleagues Maxim Ivanov and Ivan Safronov, who had refused to reveal their informants for a controversial article, claiming protection of sources. More than 200 staff members of the publishing house then complained in an open letter that one of the country's best media was being destroyed because its owner was interfering in editorial work. In 2006, billionaire Alisher Usmanov had bought the publishing house, whereupon the then editor-in-chief left the paper. A number of editors-in-chief followed in rapid succession. Most recently, prominent *Kommersant* editor-in-chief Sergei Yakovlev resigned after over 20 years with the publisher. In March 2019, the newspaper also let its St Petersburg correspondent Maria Karpenko go. The official reason was that she had "violated editorial policy" with her channel on Telegram. Karpenko had often criticised the policies of the Governor of St Petersburg, Alexander Beglov, in her writing.

↓
Inside the editorial offices of *Novaya Gazeta* in Moscow
© dpa - Report

WARNINGS ISSUED TO TRADITIONAL CRITICS OF THE KREMLIN

↑
A newsstand at Moscow Domodedovo Airport
© RSF Germany

The best-known media in Russia that are critical of the Kremlin, the newspaper *Novaya Gazeta* and the radio station *Echo Moskvy*, are subject to particularly close monitoring by *Roskomnadzor*. *Novaya Gazeta* received two warnings from *Roskomnadzor* in 2014 and 2015 within a 12-month period, which meant that it could have been closed down at any time–a situation the editorial team felt to be highly threatening. One of the warnings referred to an expletive in the advance publication of a literary work; yet the word itself had not even been printed but instead replaced with an ellipsis. In April 2018, the radio station *Echo Moskvy* became one of the first media that had to pay a fine simply because of content that *Roskomnadzor* considered objectionable. The agency issued a Rb 20,000 (approx. €260) fine for "obscene speech" in a YouTube video; popular TV moderator and opposition activist Ksenia Sobchak had provided a link to the video in her blog, which is hosted on the *Echo Moskvy* website. The legal basis was a 2013 law banning the use of swearwords in the media. In this case, it was obviously no longer applied only to journalistic content; the editorial department was also made responsible for hyperlinks.

NOW ONLY ONLINE: THE CHANNEL *TV DOZHD*

"Give TV another chance!" This was the slogan of the private TV channel *TV Dozhd* when it first started broadcasting in April 2010. Founded by journalist Natalya Sindeyeva and her husband, entrepreneur Alexander Vinokurov, *TV Dozhd* (TV Rain) confronted the excessive power of submissive pro-Putin news on state television and offered a forum for critical media professionals and opposition politicians. Its first editor-in-chief, in this post up until 2015, was the renowned Russian journalist Mikhail Zygar. His goal was to make *TV Dozhd* an independent TV station, not a medium of the opposition.

TV Dozhd quickly became popular due to its live coverage of the mass protests against Vladimir Putin in 2011/12. The station reported on the court case against the feminist punk band Pussy Riot as well as about opposition politician Alexei Navalny's allegations of corruption against high-ranking government officials–topics not mentioned in the state-controlled media. *TV Dozhd*'s broadcasts of the protests on the Maidan in Kiev in 2013 reached an audience of 18m; state television defamed the protests as provocations by paid fascists.

In early 2014, a controversial survey about the siege of Leningrad during World War II served as a pretence for taking massive action against *TV Dozhd*. "Should Leningrad have surrendered to save hundreds of thousands of people's lives?" the editorial team asked the public 70 years after the siege was lifted. The survey was online for a few minutes only, and the editorial team apologised repeatedly after the first wave of outrage in social networks. Nonetheless, the country's leading cable and satellite operators cancelled their contracts with the TV station. Since then, viewers have only been able to watch *TV Dozhd* online; a large section of the audience as well as financially strong advertisers were lost. In the autumn of 2014, the editorial department had to give up its office in central Moscow because the landlord did not extend the lease. It then reported from apartments for a time before finding new offices on the site of the former Flacon design factory in Moscow.

TV Dozhd switched to a paid model and has been financing itself mostly from subscription fees since then. According to editor-in-chief Alexandra Perepelova, they accounted for approx. 65 percent of the budget in mid-2019; the number of subscriptions has stagnated at approx. 60,000. Although roughly six million people visit the station's website per month, it is struggling to survive financially.

On July 26th 2019, the day before the Moscow police brutally cracked down on demonstrating protesters and briefly arrested more than 1,300 people, *TV Dozhd* removed the paywall indefinitely and asked viewers for donations to sustain its editorial operations. That day, 45,000 people followed the live coverage on *TV Dozhd* from central Moscow on YouTube.

A news conference at television channel *Dozhd* in February 2014: founder Natalya Sindeyeva fears for the future of her channel.

4 COURAGEOUS AND COMMITTED: THE DIVERSITY OF RUSSIAN ONLINE MEDIA

In reaction to growing state control over the internet and pressure on traditional news media, a host of new websites and alternative media projects have sprung up on the Russian-language internet in recent years. They fill the void that censorship and self-censorship are leaving in the media and cover topics that are suppressed in state-controlled reporting. Individuals, too, are attracting large audiences on social media and, in some cases, their channels have more subscribers and followers than established media platforms. And in various regions of Russia, small online media are covering issues that stir up emotions locally with their courage and commitment.

The Insider, *The Bell* and *Proekt* are three examples of these new websites– founded by first-rate journalists who left (leading) positions at established media outlets and with their investigative reporting and exclusive information from the upper circles of politics are now making a name for themselves in new publications. Their texts and topics are frequently taken up by media with large audiences both inside and outside Russia, thus evading the attempts of those in power to exert full control over news coverage. Many of the new online media outlets are registered outside the Russian Federation in order to escape Russian legislation and harassment by the authorities. *Meduza*, the most popular Russian-language news website, is not only registered outside Russia but also has its editorial offices in the Latvian capital, Riga.

In addition, there are websites such as *OVD-Info*, *Mediazona* or *Takie Dela* launched not by journalists but by human rights activists who want to inform the (web) community about their cause and enlist support for their activities. Their reports, analyses and in-depth coverage of issues such as social problems and cases of arbitrary justice have made these websites an indispensable source of information about the situation in the country.

Meduza

Meduza is the most widely read independent Russian-language online medium. According to *Meduza*, its news page reaches more than 11 million people per month, almost three quarters of them in Russia. Galina Timchenko, who was fired from her position as editor-in-chief of *lenta.ru* (see Chapter 3), founded *Meduza* in October 2014 in Latvia, thus putting the editorial staff beyond the reach of Russian media regulators. Initially, *Meduza* was mainly a news aggregator that compiled reports and other news items from Russian-language sources–especially about topics not mentioned in the state media. Over time, *Meduza* increasingly published articles of its own; an English version went online in early 2015. Today *Meduza* seeks to address a young readership in particular with Instagram stories, news games and podcasts. The roughly 30 members of the editorial staff are based in Riga, with correspondents working in Russia. *Meduza*'s work is financed through advertising banners, native advertising and investors whose identities are not known. In January 2016, Galina Timchenko handed over the position of editor-in-chief to Ivan Kolpakov, who had co-founded *Meduza* and served as her deputy up until then. She has since been active in the background as Director General. In June 2019, *Meduza* received worldwide attention when its correspondent Ivan Golunov was arrested in Moscow and was to be charged on fabricated drug allegations (see Chapter 5).

↑
Investigative journalist Ivan Golunov surrounded by colleagues after his release in June 2019

↑
Roman Dobrokhotov, founder of *The Insider*
© private image

The Insider

Founded by opposition activist and journalist Roman Dobrokhotov in 2013, the website *The Insider* specialises in investigative research. "At the time, people said we wouldn't survive for long", the 36-year-old told RSF. He claims that about 2 million people visit his website every month. *The Insider* has long been well known outside Russia, too. This is thanks mostly to research conducted jointly with the research network *Bellingcat*: Dobrokhotov and his team were involved in exposing the identities of the Russian intelligence officials who poisoned former agent Sergei Skripal in the UK and the fact that Russian agents allegedly planned a coup in Montenegro in 2016. Its research on the downing of the Boeing MH-17 over eastern Ukraine in July 2014 also caused a sensation. In its column "Anti-fake", *The Insider* seeks to systematically expose fake news. In 2016, Dobrokhotov proved that parts of Russian state television reports about "the case of Lisa"–a 13-year-old Berlin girl who went missing and had allegedly been abducted and raped by refugees–were shot using paid protagonists. Dobrokhotov registered his website in Latvia to protect it from prosecution in Russia. "Another important security measure is that we do not have an office in Russia; everyone works on the move on their laptops", he says. This protects his team–roughly a dozen freelance researchers and journalists–at least from searches or attacks like the one on the office of the magazine *Snob* in June 2019. *The Insider* team received the Council of Europe's Democracy Innovation Award in 2017 and the Free Media Award from the ZEIT-Stiftung and the Norwegian Stiftelsen Fritt Ord in 2019.

The Bell

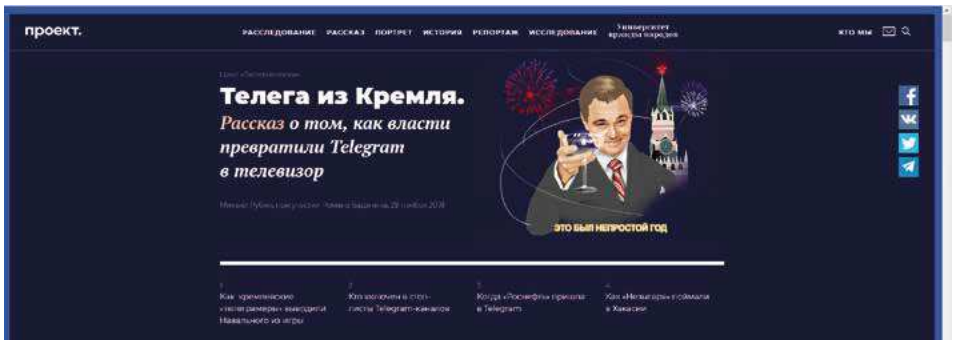
The most important news from Russia and the world, for businesspeople and anyone interested in money, written in a concise and comprehensible style, and readable in five minutes–that was what Elizaveta Osetinskaya had in mind when she launched *The Bell* in the summer of 2017. What began as a newsletter with a few hundred recipients quickly became a news platform with an excellent reputation, attracting attention time and again with exclusive information and investigative research about the business community. Instead of presenting events in classical news style, *The Bell* often organises and explains it along guiding questions: What are the benefits? What do we know so far? What do I stand to gain? Founder Osetinskaya, who had previously been editor-in-chief at *Vedomosti, Forbes Russia* and the media holding company *RBC*, got the project up and running while spending three years conducting research in the United States. She works with a small team of experienced journalists. The editor-in-chief of *The Bell* is Irina Malkova, who previously headed the editorial team of the liberal news site *Republic*. Today *The Bell* distributes four Russian-language versions of its newsletter–including one specialised in technology–as well as a weekly one in English with the most important news. The website features news covering over 20 categories, from Crimea and cryptocurrencies to Trump and sanctions. The *BellClub*, with roughly 500 members who meet regularly for behind-the-scenes discussions with prominent Russian businesspeople and politicians, is also part of the project. The editorial work is

financed by the club's membership fees, advertising and a number of private donors. Developing an economically viable business model is a challenge, Osetinskaya told RSF: "The Russian business community is afraid of supporting independent media."

↑
Elizaveta Osetinskaya, founder of *The Bell*
© picture alliance / AA

Proekt

The portal *Proekt*, which has been online since July 2018, making it one of the most recently established Russian online media, is to become the "most important investigative medium in Russia", says its founder Roman Badanin. Following the example of the American portal *ProPublica*, it is engaged in not-for-profit journalism and financed by private and public donations. The team of roughly ten would initially work with an annual budget of half a million US$ (approx. €430,000), Badanin said before launching *Proekt*. As one of Russia's most experienced political journalists, after leaving *Gazeta.ru* in 2011, (see Chapter 3), Badanin was editor-in-chief at *Forbes Russia*, the news agency *RBC* and *TV Dozhd* (TV Rain). He developed the concept for his new medium while spending a year at Stanford University–and he registered his website in the United States to preclude prosecution in Russia and to be able to fundraise abroad. A few months after its launch, *Proekt* published detailed research on how the presidential administration was trying to influence public opinion using anonymous channels on the messaging service Telegram. Putin's advisers attempted to take legal action against the text, but the case was dismissed in the court of first instance in June 2019. In the meantime, Badanin's team continued to research in the circles closest to the president: in April 2019, *Proekt* used leaked documents from the office of Yevgeny Prigozhin, also known as "Putin's chef", to show how Russia was meddling in the politics of African countries in order to destabilise the region. An investigative report prepared jointly with the *Organized Crime and Corruption Reporting Project* (*OCCRP*) about the clandestine properties of "loyal oppositionist" Vladimir Zhirinovsky was published in June 2019.



←
This report by *Proekt* shows how the Kremlin seeks to influence public opinion via the messaging app Telegram.
© Screenshot projekt.media

OVD-Info

OVD-Info is the news platform of the eponymous human rights group that provides information in particular about arrests, police brutality and politically motivated court cases. Its name is derived from the abbreviation for the local police stations (Otdel vnutrennikh del, Department of Internal Affairs) where people are taken after being arrested, for example, after demonstrations. Moscow journalist Grigory Okhotin and programmer Daniil Beylinson put the website online in December 2011 following the first protests against fraud in the parliamentary election and were met with an overwhelming response when they published the numbers of people arrested and their names. Today, eight years later, *OVD-Info* is a human rights group with a team of almost 30 as well as several hundred volunteers. It sends lawyers to police stations and provides advice to persecuted persons free of charge; its hotline is available 24 hours a day, seven days a week. *OVD-Info* documents the events during major demonstrations such as those in the summer of 2019 in live feeds and subsequently publishes the numbers of arrests, assaults and indictments. Consequently, the portal has become the key source for media in Russia and abroad for reporting on political protests. The group is financed by the Russian human rights organisation Memorial, the European Commission and through successful crowdfunding and other sources: individual donations totalled around Rb 5.6 million (approx. €76,000) in 2018, and they are rising rapidly: people in Russia had donated more than Rb 27.5 million (approx. €388,000) for *OVD-Info*'s work in the first nine months of September. On June 12th 2019, the day of the demonstration against the arbitrary nature of the judicial system following the release of journalist Ivan Golunov, *OVD-Info* received more donations on a single day than previously in an entire month.

↓ Hundreds of people were arrested during protests in Moscow in August 2019.

Mediazona

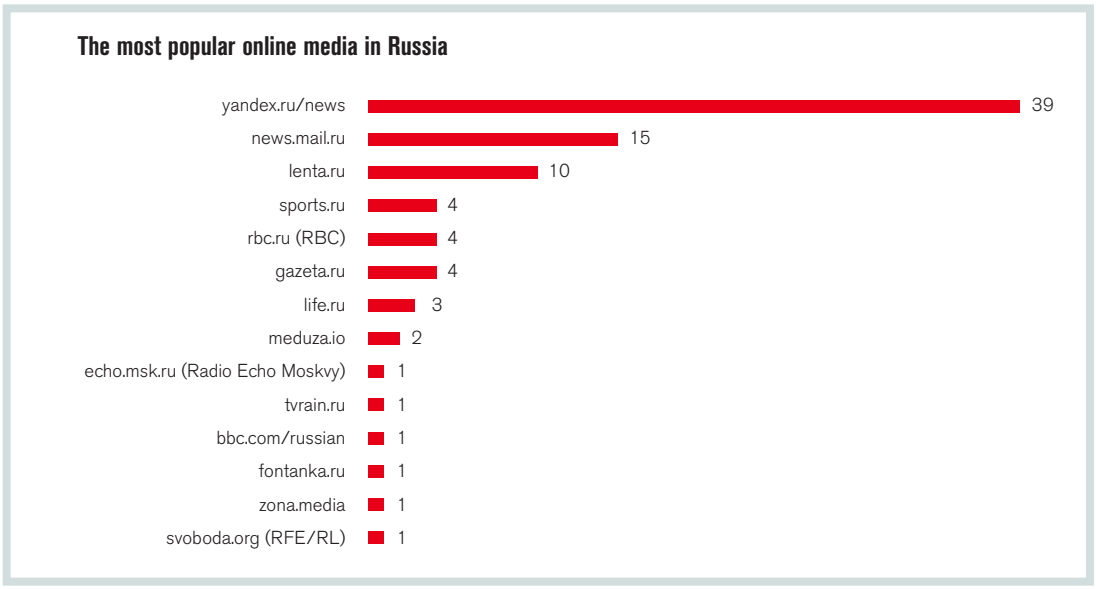
The website *Mediazona* reports on the penal and judiciary systems, specifically about the conditions in the prisons, arbitrary arrests, police brutality and court cases against activists. It was founded by Nadezhda Tolokonnikova and Maria Alyokhina in 2015. Because of a protest in Moscow's Cathedral of Christ the Saviour, the two members of the punk band Pussy Riot had spent almost two years in prison where they say they experienced abuse and inhuman conditions. The editor-in-chief of *Mediazona* is Sergei Smirnov; he worked for *Gazeta.ru* until 2013 and later as deputy editor-in-chief for the online magazine *Russkaya Planeta*. *Mediazona* is exclusively in Russian; individual texts are published in English as well in cooperation with international media such as the British daily *The Guardian*, the magazine *Vice* or the platform *OpenDemocracy*. *Mediazona* journalist Yegor Skovoroda was part of a group of media professionals and human rights activists who were brutally assaulted on their way to meet with victims of torture in Chechnya. Initially, *Mediazona* survived mostly thanks to fees for Tolokonnikova's and Alyokhina's talks and photoshoots. In 2017, they founded a fashion label to finance the platform. *Mediazona* has successfully crowdfunded since December 2017: in mid-2019, the website had more than 3,000 regular supporters from whom they received monthly revenues of roughly Rb 1.2 million (approx. €16,000).

↑
Pussy Riot activist and *Mediazona* founder Nadezhda Tolokonnikova
© picture alliance / AP Photo

Takie Dela

Takie Dela (So It Goes) is the online magazine published by the charity *Nuzhna Pomosh* (Need Help), a foundation that seeks to support civil-society engagement in Russia and collects donations for not-for-profit projects. Founded in May 2015, the portal reports on the everyday life of people with disabilities or chronic illnesses, about hospices for children or assistance for abused women. Appeals for donations describing what purposes money is needed for and how it is used are published at the end of many reports. More than Rb 200 million (approx. €2.7m) were donated to the foundation *Nuzhna Pomosh* in 2018, almost half of this for running the magazine *Takie Dela*. "We don't write about politics", says editor-in-chief Anastasia Lotareva, "in other words, we don't write about Putin". Of course, many topics, such as the poor conditions in orphanages or the lack of hospices for children, were political. "But", she says, "social topics are not considered political in Russia". That is why her correspondents enjoy a certain amount of freedom. In 2017, the editorial team was awarded a prize from the Russian government for "a new format" to promote charity and volunteering in Russia.

↑
Anastasia Lotareva, editor-in-chief of *Takie Dela*
© private image



What percentage of the population regularly visits these websites? Result of a representative survey in March 2019 by the Levada Centre, an independent polling agency.

↑ Yury Dud, Russia's best-known YouTuber
© picture alliance / Sergei Bobylev / TASS / dpa

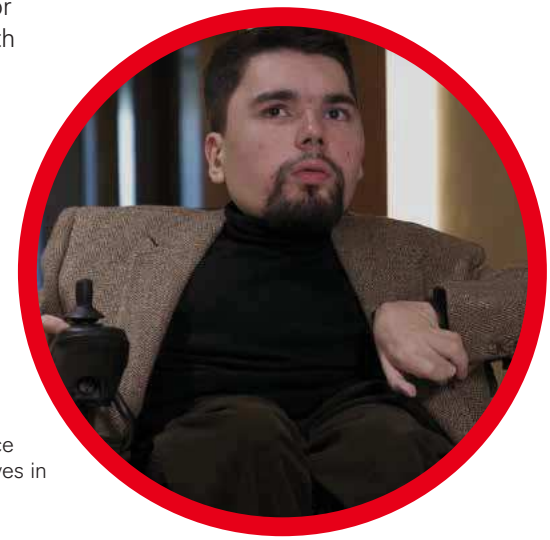
Individuals, too, are attracting significant audiences via their social media channels. The YouTube channel of well-known former sports journalist Yury Dud has almost six million subscribers. Dud, who was chief editor of the popular website ***sports.ru*** for seven years, launched his *vDud* channel in February 2017. The main focus is interviews in which Dud asks well-known personalities from politics and show business probing questions–providing a welcome contrast to the stiff reporting of the state-run channels. Initially, Dud's interview partners were mostly rappers and media celebrities, but after a while he began inviting people who are excluded from state television, for example Alexei Navalny (14 million visits) or Mikhail Khodorkovsky (10 million visits). Since April 2019, more than 17 million people have watched Dud's two-hour documentary on the Gulag penal and forced labour camps–a topic rarely covered in state-controlled media. His three-hour-long film about the Beslan school siege in which more than 330 people were killed attracted over seven million views in the first two days after its online release in early September, and by the end of October it had 17 million views.

The film reviews of YouTuber Evgeny Bazhenov (alias *BadComedian*) also attract several million viewers. In June 2019, he sparked a lively debate about internet censorship when he made it known that a film studio with close ties to the Ministry of Culture of the Russian Federation was suing him for copyright infringements. Bazhenov described this as an attempt to gag him, triggering a wave of support on social media and elsewhere as a result of which the company abandoned its lawsuit against him.

↑
Meduza journalist Ivan Golunov in an interview with Ksenia Sobchak after his release
© Screenshot YouTube
Ксения Собчак

Many well-known figures of Russia's political and public life now address their audiences directly via social networks, no longer needing to rely on traditional mass media for this. The opposition politician Alexei Navalny is very successfully disseminating the results of the research by his Anti-Corruption Foundation into how high-ranking politicians are amassing fortunes via YouTube (three million subscribers) and Twitter (2.1 million followers). His video about the real estate holdings of Prime Minister Dmitry Medvedev, released in March 2017, has been watched by about 32 million people to date. Ksenia Sobchak–a glamorous TV presenter who became an activist and then opposition candidate in the 2018 presidential election and is currently general producer at the holding company Gazprom-Media–attracts up to seven million views with interviews on her YouTube channel *Ostorozhno, Sobchak!* (Watch out, *Sobchak!*). The *Meduza* correspondent, Ivan Golunov, who was briefly held in custody in June 2019, gave Sobchak his first interview a few days after his release.

On the messaging app Telegram, anonymous channels such as *Nesygar* which post (what they say is) insider information from Kremlin circles have become influential news sources, sometimes even setting the agenda for the traditional media. On Twitter, channels like *@KermlinRussia* or *@StalinGulag* are attracting more than a million followers with their acerbic commentary and parodies of current events.



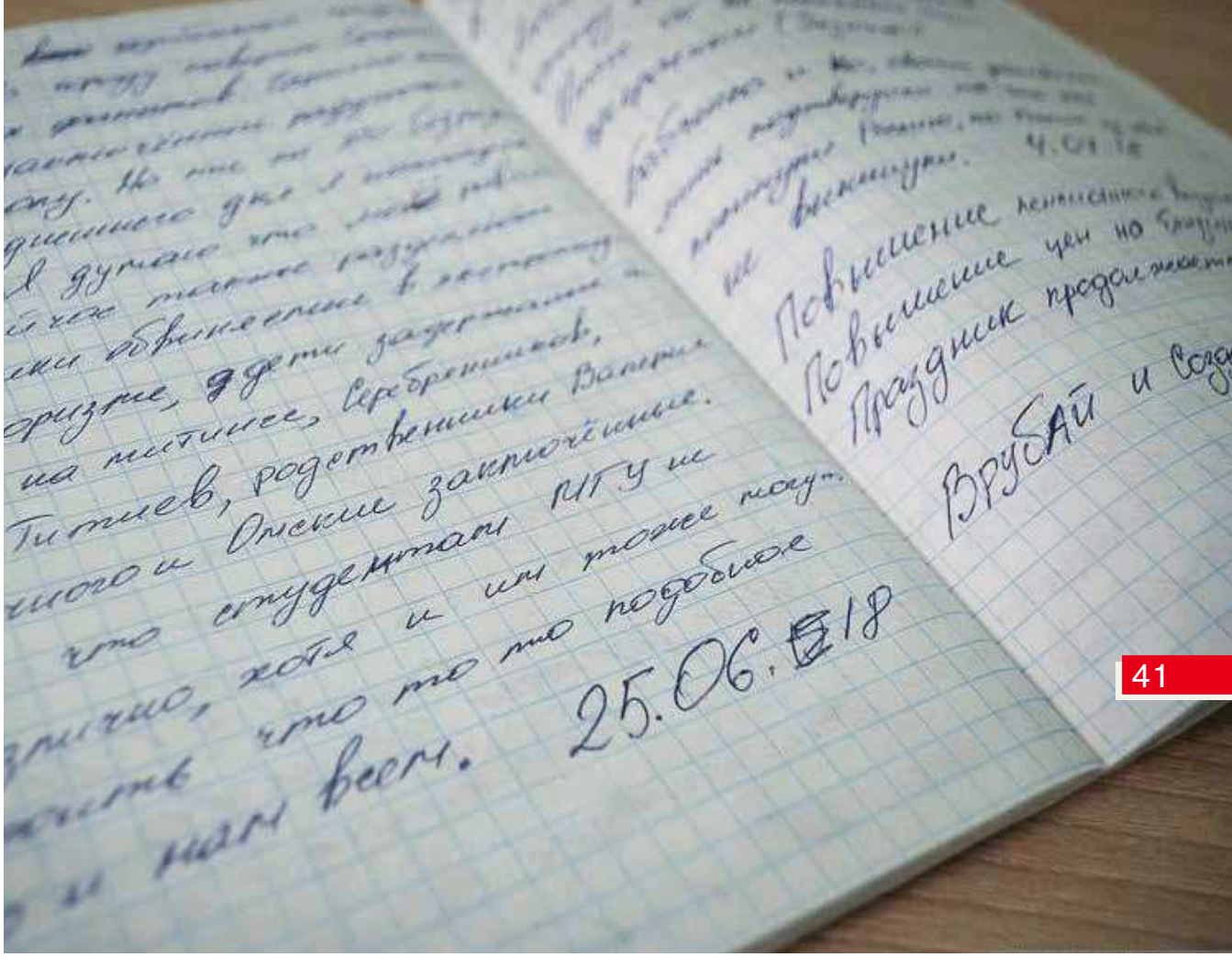
→ The author behind *StalinGulag* is Alexander Gorbunov (27) from Dagestan, a federal subject of the Russian Federation in the North Caucasus region. After years of maintaining his anonymity, the blogger revealed his Identity in early May 2019, saying he was doing so to prevent reprisals against his family. Shortly before this, armed police had searched the home of his parents in Dagestan. Gorbunov himself lives in Moscow.

↑ The popular TV presenter Maria London switched to YouTube after her show was cancelled.
© Screenshot **Картина Маслом** HTH24

In various regions of Russia, small online media are fearless and committed in their coverage of issues that are having a local impact–underfunded hospitals, corruption in local government, extravagant construction projects that destroy the environment. The online newspaper *Znak*,[1] which is based in Yekaterinburg and mainly covers current events in the Ural region, is now well known across Russia and ranked third on a list of the country's most frequently linked online media outlets in June 2019–ahead of *RBC* and the *BBC's* Russian service. In late 2018, reporters at the St Petersburg-based online paper *Fontanka* helped to identify suspects in the Skripal poisoning case as employees of Russia's military intelligence service GRU.

The grassroots media project *7x7* was launched in the Komi Republic in north-western Russia in 2010. Under the slogan "Horizontal Russia" it aims to strengthen the blogosphere in the regions and is creating an independent and free space for initiatives and cooperation among civil society groups. *7x7* received the Free Media Award 2019 for setting a "unique example of collaboration" among activists and regional bloggers, human rights activists and professional journalists. The website has repeatedly garnered attention nationwide, for example in August 2019 with the publication of the diary of a 23-year-old man who is in prison for allegedly being a member of a terrorist group and claims he has been tortured while in custody.

[1] *Znak* was founded at the end of 2012 by Aksana Panova, former chief editor of news site u*ra.ru* (now called ura.news), Panova left her old post amid allegations of fraud which she says were motivated by her critical reporting and which were later dropped. Within just a few years, *Znak* became far more successful than *ura.ru*.



↑
The news site *7x7* published a diary written by a 23-year-old man while in prison.
© semnasem.ru

In the Caucasus, the independent news site *Kavkazsky Uzel* (*Caucasian Knot*) has maintained a tight network of correspondents since 2001. Founded by the human rights organisation Memorial, the website appears in Russian and English and is considered to be the main source of information on developments in the region. For security reasons, the editorial staff do not have their own offices, and its reporters often put their lives in danger to do their work. The human rights activist Natalya Estemirova and journalist Akhmednabi Akhmednabiyev both wrote for *Kavkazsky Uzel*. Estemirova was murdered in Chechnya in 2009 and Akhmednabiyev was shot dead in Dagestan in 2013. The information website *Memo.ru*, which belongs to the human rights organisation Memorial and publishes *Kavkazsky Uzel*, has been on the "foreign agents" list since November 2014.

The list of independent regional media outlets goes on: in Siberia, news site *Tayga.info* reports on topics that are ignored in state media, the popular TV presenter Maria London provides biting commentary on current affairs from the city of Novosibirsk on YouTube, and the editorial staff of television channel TV2, which was based in Tomsk and was shut down in 2015, are now continuing their work online as a news agency. In Kaliningrad, Igor Rudnikov has resumed his work with his newspaper *Novye Kolesa*, undeterred after just spending 20 months in prison because of his reporting. From St Petersburg, the online newspaper *Bumaga* reports on life and culture in the metropolis while website *Lenizdat.ru* covers topics related to the media and press freedom.

DEDICATED LOCAL NEWS COVERAGE IN NIZHNY NOVGOROD

↑
Local journalist Irina Slavina
© RSF

Journalist Irina Slavina's telephone is constantly ringing. A man is just calling her from a neighbouring village because a barrier blocking access to the lake was recently set up. "People usually ring me when something bad's happened", says Slavina, 46, who lives with her husband and two children in Nizhny Novgorod, a city of more than a million on the Volga, 400km east of the capital. She doesn't have an editorial office, which also protects her from searches by the authorities. She works from home on her laptop and is often on the move around the city; after all, her heart is in local news coverage.

Slavina previously worked for various media, where she repeatedly encountered problems. In the spring of 2015, she decided to establish a media outlet of her own. The only name favoured in a survey of her Facebook friends was *KozaPress*. She liked the idea: "koza" means "goat", and "goats love freedom, they're curious and they climb all over." A young man from a local IT company built a website for free, and she succeeded in registering *KozaPress* as a media outlet.

The professionally designed website has been online since November 2016 and is widely read in the city. "Many public officials read *KozaPress too"*, says Slavina. Roughly 4,000 people visit her site every day, most coming via the Yandex search engine or social media. The project doesn't generate a lot of money, says Slavina, but her family supports her commitment to journalism.

Opinions about her differ among her fellow local journalists. "Irina Slavina is a courageous person, she refuses to accept censorship and she risks a lot", says a journalist with one of the local newspapers. But he thinks she often has trouble being objective and presents material in a biased way. He finds her style to be too emotional. "But it is good that the portal exists and takes up important topics that people can't read about elsewhere", says another journalist.

The reputation of the online portal *KozaPress* now extends all the way to Moscow. Many journalists in the capital who otherwise have little interest in the provinces have long heard about this editor-in-chief who gets sued time and again. It seems a bit like David and Goliath, but there are also astounding victories besides defeats. Initially, Slavina found herself exposed to defamation. Then, in January 2017, the tyres of her car were slashed repeatedly. The same year, a local legislator sued *KozaPress* in court because of an article about corruption, aiming for Rb 100,000 in damages. But the judges surprisingly ruled in favour of Slavina. "It was a wonderful verdict", Slavina remembers. "It said in black and white that a journalist even has the right to provoke."

It was not to be the only lawsuit against the online portal, however. Lawyers from the organisation *Agora* defended Slavina. “I would never have succeeded without their help”, the journalist said about the wave of lawsuits. She was hurrying to a press conference on March 5th 2019 when the police stopped her, intending to arrest her. She ended up in prison for one night before *Agora* lawyers secured her immediate release. This time, the accusation was not about Slavina’s reporting but about an unauthorised demonstration: on February 27th, the anniversary of the death of opposition politician Boris Nemzow, who had been murdered in 2015, she had demonstrated in the city’s pedestrian zone, holding his portrait in her hand. Nemzov was Governor of Nizhny Novgorod in the 1990s. “This was his hometown, he was from here”, says Slavina.

The state’s media regulator *Roskomnadzor* lost a spectacular court case against Slavina in June 2019. Numerous media across the country reported on the case. It was about a press release from the local criminal investigation authority that *KozaPress* had published. The symbol of an organisation banned in Russia could be seen on the photos included in the press release. For this reason, *Roskomnadzor* accused Slavina of violating the Law on Mass Media. “I was threatened with a fine of Rb 44,000”, says Slavina. However, her lawyers succeeded in proving that the photos did not originate from her but from the press release, which had been deleted from the internet in the meantime. “I’m spending more and more of my time in court rather than doing my work”, Slavina complains, adding that her husband still places his hopes in the rule of law in Russia; she herself has long lost faith in it.

↓
A pedestrian zone in Nizhny Novgorod

Every year, several hundred internet users are prosecuted in Russia for alleged violations of the Criminal Code.

5 ARBITRARY AND SEVERE PENALTIES: EVERY USER RISKS PROSECUTION

Between 2015 and 2018, several hundred people in Russia were prosecuted because of their online activities, and dozens sentenced to prison. Those prosecuted included not only politically active bloggers and journalists, but also people who simply shared texts and images via social networks. A mere "like" in the wrong place can put someone in jail–especially when it concerns Russia's policy in Ukraine or Syria or criticism of the Russian Orthodox Church. Although President Putin introduced a corrective to the controversial anti-extremism Article 282 in the Russian Criminal Code in summer 2018, the persecution of dissidents has not decreased significantly since then.

A few years after the mass protests in Moscow and other cities in 2011/2012, it became clear to the Russian leadership that the measures it had undertaken so far were not enough. There was one thing that blocking websites, bans (see Chapter 2) and personnel changes in the editorial offices of critical media (see Chapter 3) were not able to prevent: people on the internet discussing topics that were hushed up by state-controlled media. Authorities began prosecuting individual users and imposed sentences that were sometimes horrendous–not only against journalists and politically active bloggers, but also against people who simply shared information with their friends or recommended content. In Russia, even clicking "like" in the wrong place can result in several years' imprisonment.

It is difficult to predict where the authorities will strike next. To some extent, their decision about whom to proceed against is made arbitrarily. While one user is prosecuted as an extremist because of a harmless meme, another can write sharp-tongued commentaries on current politics without any consequences at all. "It's like playing roulette", says Alexander Verkhovsky, Director of the SOVA Center for Information and Analysis[1] in Moscow, "nobody knows where they draw the line." As a result, self-censorship–already widespread in the editorial offices of media close to the Kremlin–is increasing in the general population as well: "Many people today quite deliberately refrain from commenting, or do so only very cautiously, particularly where political topics are concerned", said Artem Kozlyuk from the organisation *Roskomsvoboda* in an interview with RSF.

[1] SOVA Center for Information and Analysis (sova is Russian for 'owl') in Moscow publishes research and studies on the government's misuse of counter-extremism legislation, on racism and xenophobia, and on the relations between the churches and secular society.

←
Agora lawyer Damir Gainutdinov
© private image

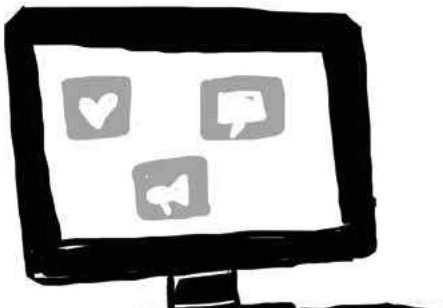
Since 2015, the authorities have been cracking down on individuals, a development that peaked in 2016 and 2017. This is apparent from the data collected by the human rights organisation *Agora*, which documents how freedom of speech is restricted on the internet each year. According to their data, 411 persons were prosecuted in 2017–twice as many as in 2015 and three times as many as in 2014. In 2016 and 2017, they also recorded particularly high "administrative pressure", meaning the number of warnings, financial penalties and demands from the state's media monitoring agency to change or delete content.

How internet users are persecuted and prosecuted in Russia Source: Agora

	2011	2012	2013	2014	2015	2016	2017	2018
Violence/threats	10	3	23	26	28	50	66	59
Criminal prosecution[1]	38	103	226	132	202	298	411	384
Prison sentences[2]	no data available				18	32	48	45
Administrative pressure[3]	173	208	514	1.448	5.073	53.004	22.523	4.402
Civil suits	11	26	37	60	49	170	39	58

1 - Searches, arrests, interrogations, indictments, criminal trials, prison or fines
2 - Defendants sentenced to prison or psychiatric detention (2016: three cases, 2017: five cases)
3 - Reprimand, demand to change or delete online content, fine

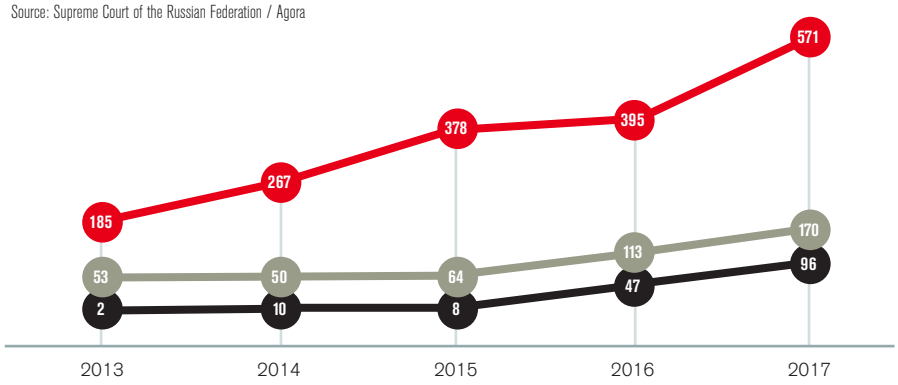
Note: *Agora* counts all cases in which authorities proceed against users–i.e. the numbers include cases in which the user's freedom of speech and freedom of information were violated, as well as those related to cases concerning behaviour such as radical right-wing statements, hate speech or instigation of violence.



The following offences were allegedly committed by defendants online: Article 282 of the Criminal Code on "incitement of hatred or enmity" as well as "organising an extremist community"; Article 280 on "public appeals for the performance of an extremist activity"; Article 280.1, introduced in 2013 and made even stricter after the annexation of Crimea, on "public calls to action aimed at violating the territorial integrity of the Russian Federation"; and Article 205.2 on "public justification of terrorism". These articles are formulated so vaguely and generally that, in practice, they can be interpreted to cover almost any unwanted remark. According to *Agora*, of the 45 cases in 2018 in which people were convicted to prison for their online activities, there was only one case that did not concern one of the Criminal Code's anti-extremism articles.

Convictions for violations of the anti-extremism articles in the Russian Criminal Code

Source: Supreme Court of the Russian Federation / Agora



Art. 205.2 (blue): Justification of or calls for terrorist activity

Art. 280 (orange): Public calls for separatism or extremist activity

Art. 282 (grey): Incitement of hatred or enmity

Up until 2018, courts were not even required to summon the operators of the websites or the authors of the articles to be blocked. Some judges issued rulings after extremely short trials and neither reviewed the material on which they were ruling nor heard testimony from witnesses. Often the persons concerned learned only afterwards that their website or certain content on it had been blocked, reported *Agora* lawyer Damir Gainutdinov in an interview with RSF. It was not until April 2018 that the Russian Supreme Court ordered that trials about banned content could not take place without the presence of the authors or website owners concerned.

←
A "like" in the wrong place can land you in jail.

THE JOURNALIST: IVAN GOLUNOV

↑
Investigative journalist Ivan Golunov
© picture alliance / Vladimir Pesnya / Sputnik / dpa

On June 6th 2019, Ivan Golunov, an investigative reporter for the Latvian-based online portal *Meduza*, was arrested in Moscow. The police claimed to have found cocaine in his apartment and accused him of drug trafficking, for which he could face 20 years in prison. Thus far, this was not so uncommon in Russia. However, the 36-year-old experienced an unprecedented wave of solidarity: thousands of people demonstrated on his behalf, even media professionals aligned with the government sided with him–so that after a few days, Golunov was released.

One of the topics Golunov was researching was corruption in Moscow's funeral and construction sectors. Since his articles printed the names of people who accepted bribes, his colleagues suspected that Golunov's arrest emanated from officers from the intermediate ranks of the FSB who wanted to put a halt to his research. "They just didn't know who they were dealing with", *Meduza*'s editor-in-chief Galina Timchenko told RSF. Golunov had an impeccable reputation, "even with officials, who all knew that he always worked very professionally and never betrayed any of his sources".

After Golunov's arrest, RSF pointed out numerous irregularities in the case: it took twelve hours before one of his friends was informed and was able to contact a lawyer. The police circulated photographs which–contrary to their claims–were not from Golunov's apartment. The investigators initially refused to take samples from the journalist's hands, which could have proven his innocence. Held in police custody for 24 hours, Golunov was not allowed to eat or sleep, and, by his own account, was beaten by police officers. When he was brought before a judge on June 8th, he was completely enervated.

Behind the scenes, Alexei Venediktov, editor-in-chief of the radio station *Echo Moskvy*, and Dmitry Muratov, head of the supervisory board of the newspaper *Novaya Gazeta*, interceded on Golunov's behalf. They met with representatives of Moscow Mayor Sergey Sobyanin and Russia's Commissioner for Human Rights, Tatyana Moskalkova. More than 6,500 media professionals showed their solidarity with their colleague in an open letter. In the opinion of many journalists, the fact that even the Kremlin-friendly television station *NTV* and the editor-in-chief of the international news station *RT*, Margarita Simonyan, demanded an explanation showed that there were groups within the Kremlin that were critical of the arrest. Hundreds of people assembled before the court for Golunov's arraignment on June 8th to show their support, rejoicing when he was unexpectedly released and placed under house arrest.

Two days later, Russia's three leading business newspapers (*Kommersant*, *Vedomosti* and *RBC*) appeared with identical title pages, displaying: "We Are Ivan Golunov" in giant font. Dozens of domestic and international newspapers reprinted Golunov's reports, which *Meduza* released for free sharing online. On June 11th, Minister of Internal Affairs Vladimir Kolokoltsev announced that all charges against Golunov had been dropped, and several officials were suspended. Whether those responsible for Golunov's arrest will ever be held accountable is questionable, however: in mid-November, investigators classified all materials in the proceedings against the police officers, declaring them a state secret.

THE ACTIVIST: MIKHAIL SVETOV

Even from prison, YouTuber Mikhail Svetov kept tweeting to his internet community. On July 31st 2019, a court had sentenced the leader of the small Libertarian Party of Russia to 30 days in jail for violating laws by participating in a protest rally organised by the opposition. Audio footage of his courageous defence before the court went viral and kept circulating online for days.

The 34-year-old is part of a small scene of political YouTubers in Russia. He considers himself a net activist, and was one of the main organisers of the first major demonstration against internet censorship in March 2018. "We were protesting against the attack on Telegram and Pavel Durov", explains Svetov who uses his popular YouTube channel for political activities. "The internet is the only free space in Russia where people can build networks and organise themselves". says Svetov. He fears that the free internet could disappear in an increasingly totalitarian state.

"A new generation has grown up under Putin", he says. "We grew up with great freedoms; we no longer know state censorship like our parents". As an activist, Svetov feels connected to a global culture that builds networks online. He studied in the UK and lived in Japan as a successful IT entrepreneur until the mass protests began in Russia in 2011. Svetov decided to return home to fight for his country's future. The YouTuber has acquired a large following of young fans who invite him to events all over the country so that they can experience their hero with the long hair and big glasses live on stage. According to his own calculations, Svetov has given lectures in 47 Russian towns in the last eighteen months.

The majority of the scene, however, is made up of apolitical bloggers and YouTubers. Some of them earn a great deal of money on the web. Svetov attempts to explain to them that the new laws could also have an adverse effect on their earnings. But so far he has not been able to convince any of the influential YouTubers to express themselves publicly. In spring, the well-known YouTuber Yury Dud did in fact attend a rally but declined to come up on stage. "We do receive support from the scene, but hardly anyone wants to appear in public. There is a great deal of fear around", says Svetov. He is not deterred by the excessive power of the state: "I try to explain to people that they have to overcome their fear." But then again, he is also financially independent, having earned a fortune selling Bitcoins starting in 2011.

Svetov hopes that the online scene will become more politicised and join the opposition if Russian authorities continue to restrict freedom on the internet. He fears that they may succeed in isolating the Russian internet. "If it affects national security, it will work", he says. "After all, Putin does not want to disturb the banking sector or company websites, or make ordering a taxi online more difficult. What he wants to prevent is us continuing to organise our protests on the internet."

↓
Mikhail Svetov

↑
An episode of *The Simpsons in which* Homer plays on his smartphone in a church was removed from private TV channel *2x2's* programme as a precaution. It was interpreted as an allusion to the case of a blogger who was sentenced to two years in prison for playing "Pokémon GO" in a cathedral.

THE INDIVIDUAL CASE AS A CAUTIONARY TALE

Russian online portals often report about particularly harsh sentences and the fates they affect. Reports trigger heated debates on the web, which occasionally lead to a public outcry and visible protest. At the same time, however, news of this kind has a deterrent effect on other users. For instance, take the case of Andrei Bubeyev[2] from the provincial city of Tver, an electrician and the father of a three-year-old son. He was arrested in May 2015 for sharing a text entitled "Crimea Belongs to Ukraine" and a caricature on the social network VKontakte. For this crime, the court sentenced him to two years and three months in prison. Bubeyev's lawyer emphasised that her client was not a blogger, but merely a man interested in politics, who was connected with just twelve friends over VKontakte. After his release in August 2017, Bubeyev and his family left the country and moved to Ukraine.

In December 2016, blogger Aleksei Kungurov from the city of Tyumen in western Siberia was sentenced to two years and six months' imprisonment. The reason was a blog entry in October 2015 in which Kungurov questioned the Russian air strikes in Syria. The authorities became aware of this post only after Kungurov also criticised Russia's actions in Ukraine in March 2016. The court ruled that the Syria entry constituted "justification of terrorism" (Art. 205). By contrast, the Human Rights Center Memorial classified Kungurov as a political prisoner after his conviction– like Bubeyev before him. Kungurov was not released until June 2018.

In May 2017, video blogger Ruslan Sokolovsky of Yekaterinburg received a suspended sentence of two years and three months for a deliberate provocation. In August 2016, he had published a video on YouTube which shows him at the Russian Orthodox Cathedral playing "Pokémon GO"–a game which the state's leaders condemned as a sign of Western decadence. Sokolovsky ended up spending nine months shuttling between pre-trial detention and house arrest before being

[2] A series on the *Coda Story* channel "Jailed for a Like" presents three- to four-minute animated videos describing cases like those of Andrei Bubeyev, Aleksei Kungurov and Ruslan Sokolovsky.

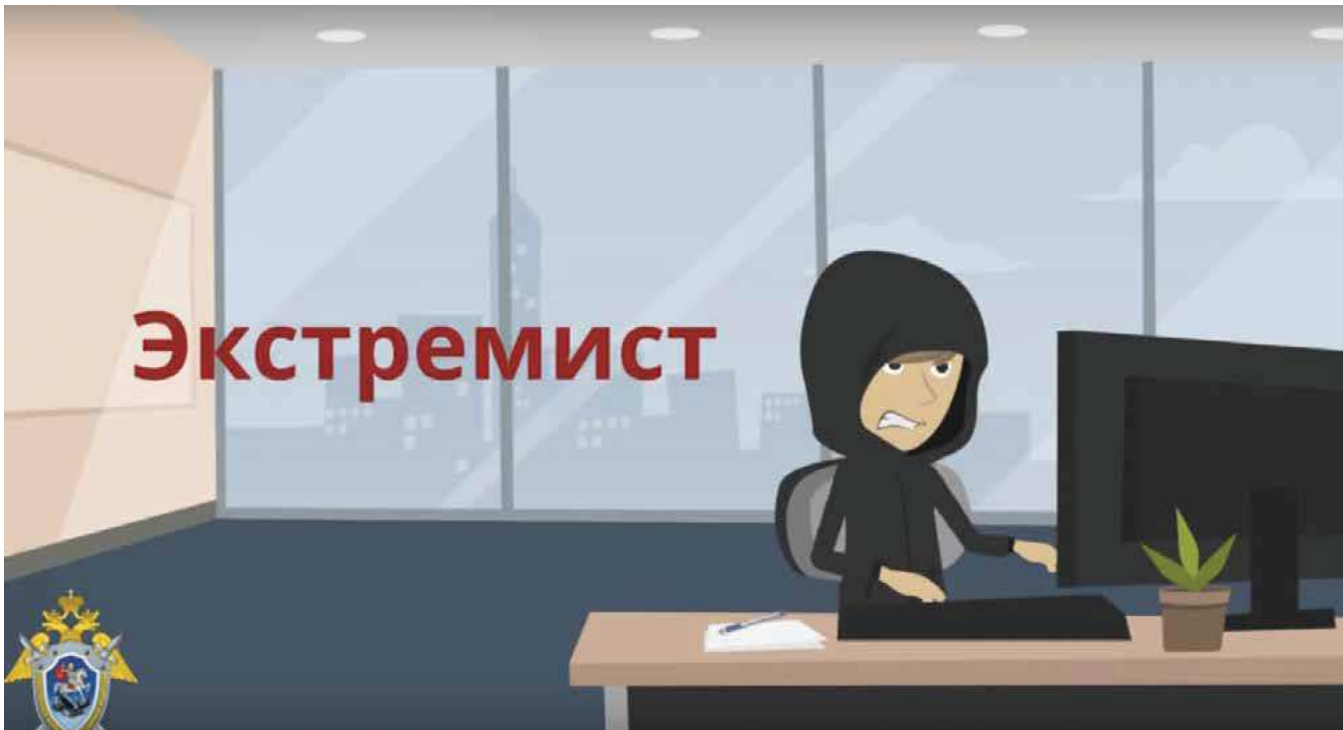
sentenced for “incitement of hatred or enmity” (Art. 282) and “offending the feelings of religious believers” (Art. 148). His name was put on the official list of suspects connected with extremism and terrorism, all of whom had their bank accounts frozen for security reasons.[3] Subsequently, nine popular Russian video bloggers published a protest message, demanding that the government change the vaguely formulated Article 282, which punishes “ultra-rightist murderers” exactly the same way as video bloggers making jokes.

↑
Maria Motuznaya
© private image

In summer and autumn 2018, there were repeated protests in Moscow and other cities against the arbitrary prosecution of internet users accused of terrorism and extremism. The protests were triggered by cases like the prosecution of two young women, one aged 18 and the other 19, who spent months in pre-trial detention for suspected membership in a terrorist organisation. The case of the student Maria Motuznaya from Barnaul in southwestern Siberia also attracted attention. Prosecutors threatened her with as much as six years’ imprisonment for a few memes, even though she had long since closed her VKontakte account. One of the pictures showed nuns secretly smoking; on another, Jesus asked the leader of the Russian Orthodox Church, Patriarch Kirill, what time it was–an allusion to the patriarch’s luxury watches. Motuznaya experienced a wave of solidarity when she made her story public via Twitter in July 2018. She learned of others in her city who were also accused of violating Article 282–prompting some media wags to dub Barnaul the “extremism capital”.

[3] The Federal Financial Monitoring Service (Rosfinmonitoring), which has reported directly to the president since 2012, keeps a “list of organisations and persons for which there are indications of participation in extremist activity and terrorism”. Inclusion in this list does not even require a conviction; initiation of criminal proceedings against the individual is sufficient. In early November 2019, the list included more than 9,300 individuals from Russia. Sokolovsky’s name is still registered.

↓
The Investigative Committee in the Altai Republic in Siberia explains in a video aimed at young people how easily they can make themselves liable to prosecution by posting imprudent comments on social networks.
© Screenshot altai-krai.sledcom.ru



The high number of criminal proceedings for alleged extremism or terrorism is not necessarily due to any deliberate strategy by the leadership in the Kremlin. Often, officials on the lower and intermediate levels of the power system are responsible for the arbitrary accusations. "Government officials just want to fill up their statistics, so they create suspects at random", explains Damir Gainutdinov of the human rights organisation *Agora*. The legal regulations can be interpreted so broadly that something objectionable can be found on almost anyone's social media accounts. The Carnegie Moscow Center speaks of a "system error" and points out that this practice is turning completely apolitical people into opposition activists.

The Kremlin apparently noticed this misuse of the laws: on October 3rd 2018, President Putin proposed changes to mitigate the abuse of the controversial Article 282 of the Criminal Code. According to his proposal, criminal proceedings were to be opened only if someone published or disseminated "extremist content" multiple times within a year. A first offence would be punished with fines or detention rather than several years' imprisonment. These changes took effect in January 2019. Some criminal proceedings–for instance, the case against Maria Motuznaya–were consequently closed. Yet the prosecution of such cases has not decreased significantly, according to *Agora* lawyer Gainutdinov. The only difference is that officials are now pressing charges for violating different articles of the Criminal Code.

In autumn 2019, RSF called for the release of several media professionals who were imprisoned for articles they published on the internet. The blogger Alexander Valov from the southern Russian city of Sochi was arrested in January 2018 and held for eleven months before being sentenced to six years in prison and a fine of Rb 700,000 (approx €8,800). In September 2019, a court upheld the unusually harsh sentence. Valov had written critically about the regional administration and the construction of sport facilities for the 2014 Olympic Games. In July 2019, the journalist Rashid Maysigov, who wrote for the news site *Fortanga* (see Chapter 3) was arrested in the North Caucasus Republic of Ingushetia. He is being investigated for alleged drug possession and for treason. Maysigov told his lawyer that he had been tortured in prison. In March 2019, five years after Crimea's annexation by Russia, the Crimean Tatar journalist Remzi Bekirov was arrested for reporting on the persecution of the Tatars in Crimea on the illegal oppositional news page *graniru.org*. He faces life in prison for "organisation of the activities of an association designated as terrorist under Russian law" (Art. 205.5).

↓
Article 282 of the Criminal Code on "incitement of hatred and enmity" is often used to silence critical voices.

In summer 2019, tens of thousands of people in Moscow and other cities protested against the exclusion of oppositional candidates from local elections. These were the biggest protests since 2011/2012. Afterwards, internet users were once again charged for their statements on social networks. In August, the 21-year-old student Yegor Zhukov, who had lambasted the government on his YouTube channel and called for civil disobedience, was imprisoned for one month for participating in the protests and has since been held under house arrest, provisionally until the end of December 2019. In mid-September, he was indicted for "public appeals to extremist activities" (Art. 280.2) and put on the list of suspected supporters of terrorism and extremism. He faces five years in prison. In early September, Vladislav Sinitsa was sentenced to five years in a penal camp for violating Article 282 with a tweet that allegedly called for violence against the families of security officers.

↑
Yegor Zhukov was sent to prison for his blog on YouTube.
© Nowaja Gaseta / Vlad Dokshin

Since 2018, state internet control has increasingly taken aim at larger platforms, as *Agora* shows in its report of February 2019. The government has recognised that this is the only way to monitor communication between users effectively and prevent the propagation of undesirable information. Andrei Soldatov, a journalist specialised in intelligence services and surveillance, made the same observation: "Of course it is easier to control a few hundred companies than hundreds of thousands of users."

↓
Rapper Oxxxymiron campaigning for protesters who were detained during the demonstrations in the summer of 2019.
© picture alliance / Sergei Savostyanov / TASS / dpa

VIOLENCE AGAINST MEDIA PROFESSIONALS

Time and again, online journalists and bloggers in Russia have been the victims of violent attacks. The London-based organisation Index on Censorship counted twenty such incidents in the first six months of 2019 alone. In June, for instance, the blogger Vadim Kharchenko was apparently lured into an ambush in the southwestern Russian city of Krasnodar, where two men injured him with firearms and knives. Kharchenko had reported critically on the local administration and the persecution of activists on his YouTube channel, and had already been targeted by several attacks in the past.

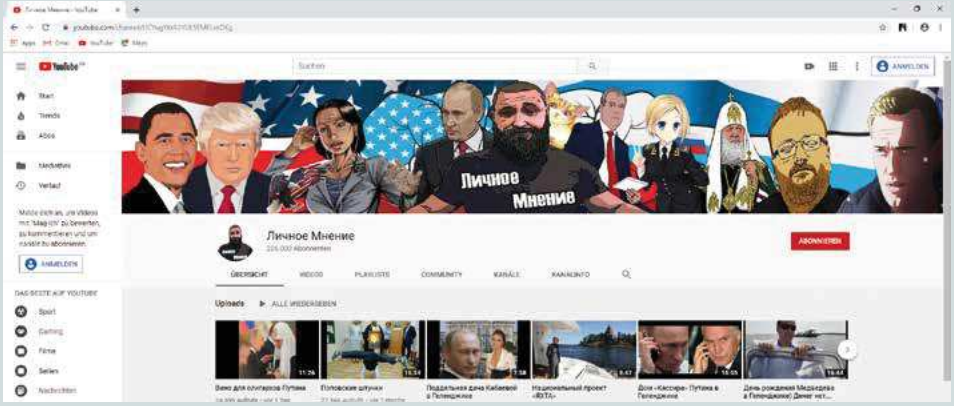
↑
Mediazona publisher Pyotr Verzilov
© picture alliance / Christoph Soeder / dpa-Zentralbild / dpa

In September 2018, the Pussy Riot activist and editor of the news site *Mediazona*, Pyotr Verzilov, was admitted to a hospital in Moscow after a suspected poisoning, and flown out for further treatment in the Charité hospital in Berlin. Prior to the incident, he had been investigating the mysterious death of three Russian journalists in the Central African Republic.

In November 2017, the editor of the independent news portal *Bloknot Volgograda*, Yulia Zavyalova, survived an assassination attempt in Volgograd. The police took action only weeks later in response to massive public pressure. *Bloknot Volgograda*, one of the most popular online media in the region, is known for its critical stance toward the regional rulers and for investigative reports about corruption.

After crimes like this, the culprits are seldom identified and punished; even more rarely are those who contracted the hits held accountable. The human rights organisation *Agora* deplores the "demonstrative refusal of the authorities" to prosecute "particularly the most serious cases of threats or attacks" or to investigate, for instance, employees of the numerous security services. This encourages a climate, the report continues, in which critical journalists and bloggers can be threatened without fear of consequences.

This also applies to the many journalists who are beaten and prevented from doing their job by security officials at demonstrations–most recently at the protests in Moscow before the regional elections in summer 2019, where several media professionals were injured and many temporarily detained by security forces.



→
The YouTube channel of Vadim Kharchenko from Krasnodar
© Screenshot YouTube Личное Мнение

CIVIL SOCIETY FIGHTS BACK

The organisation *Roskomsvoboda* was founded on November 1st 2012, the very day on which the Russian internet blacklist law came into effect. The group fights against internet censorship, and its very name constitutes a deliberate antithesis of the state's media regulator *Roskomnadzor*. *Roskomsvoboda* essentially means "freedom of Russian communications", while the regulatory body includes supervision (Russian: "nadzor") in its very name. *Roskomsvoboda* calls for freedom of information and self-regulation of the internet. The blacklist of blocked websites, to which, according to the will of the media monitoring agency, only authorised providers are allowed to have access, was made public on the organisation's website from the very first day and has been updated constantly ever since–among other reasons, to show how often the crude technology which the body uses for blocking ends up 'inadvertently' blocking unobjectionable websites as well. *Roskomsvoboda* gives users specific instructions on how to protect online communication from surveillance, and how they can circumvent internet censorship using VPNs. *Roskomsvoboda* has launched campaigns against stricter copyright provisions, the blocking of the messaging service Telegram, and since autumn 2019, against facial recognition programs. The activists also appealed for protests against a new law enabling authorities to isolate the Russian internet. With the Blackscreen Report project, launched in summer 2019, *Roskomsvoboda* will systematically document the political persecution of Russian citizens because of their activities in the internet. The NGO is financed in part through the work of its affiliated Digital Rights Center, which provides commercial IT and legal advice for companies and individuals.

↑
The *Roskomsvoboda* team

Around 50 lawyers from all over Russia have joined forces in the international human rights organisation *Agora*. They assist individuals in taking the authorities to court for violations of their basic rights, as chartered in the Russian constitution and the European Convention on Human Rights. *Agora* has brought numerous cases before the European Court of Human Rights in Strasbourg. Among those represented by the organisation are journalist Oleg Kashin and Ukrainian filmmaker Oleg Sentsov, who was released in September 2019 after two years' imprisonment in a Siberian prison camp. One emphasis of *Agora*'s work is on restrictions of freedom of speech on the internet, which are documented in a detailed annual report. Further analyses by the organisation concern such topics as increasing surveillance and whistleblowers in Russia.

←
In its *Blackscreen Report* project, *Roskomsvoboda* documents the government crackdown on citizens for comments on the Internet

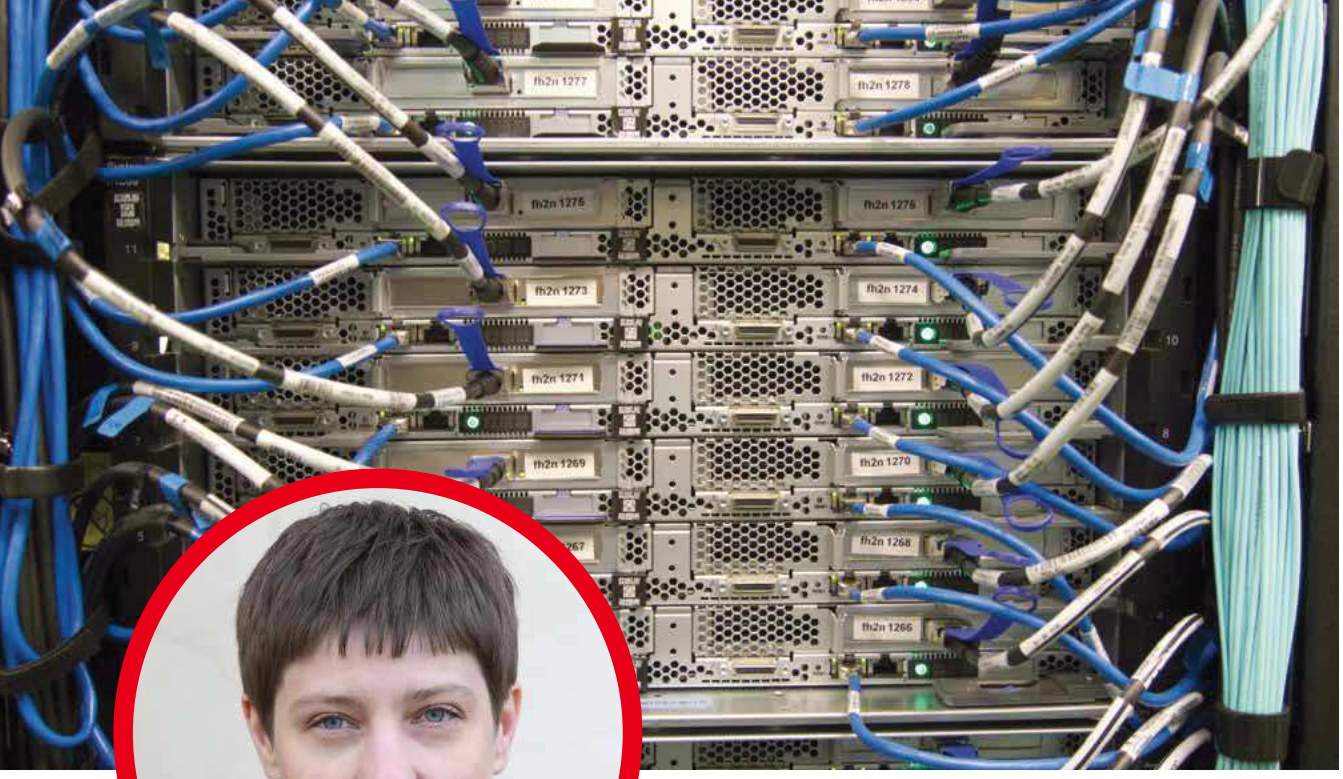
6 THE INTELLIGENCE SERVICE IS READING RIGHT ALONG: THE FIGHT AGAINST ANONYMOUS COMMUNICATION

Since the early 1990s, the state monitoring system SORM has made monitoring the communication of all citizens in Russia possible on a grand scale. On top of this, various laws directed against anonymous or encrypted online communication have been passed since 2014. Yet the implementation of these laws has been sluggish because the required technology is often lacking and many telecommunications operators and internet service providers are reluctant to invest large sums in new equipment. Moreover, many foreign providers of social networks, messengers or anonymization services do not comply with Russian regulations. However, the "sovereign internet law" of May 2019, stipulating that the Russian internet be disconnected from the global internet, marks a new stage of repression. It centralises the control and filtering of online traffic, which is to be the purview of the state's media regulator rather than the providers in the future. Moreover, new surveillance technology is to be introduced throughout the country. The government hopes that the new law will allow it to block banned content and platforms more effectively.

The online communication of users in Russia can be monitored much more intensively than in other, democratically governed countries, which are currently discussing how to regulate the internet. SORM,[1] the Russian system for lawful interception of telecommunications is directly built into the communications infrastructure and enables systematic mass surveillance. The foundation for this was laid by the Soviet security agency, the KGB, in the late 1980s. The organisations that succeeded the KGB further developed SORM in order to be able to tap telephones in the newly created Russian Federation. Part of this entailed compelling telecommunications operators to install devices that were able to store connection data and conversation content. Surveillance was expanded to the internet through the deployment of new technology (SORM-2) in the late 1990s.

[1] SORM is an acronym for the Russian name Система оперативно-разыскных мероприятий (Sistema operativno-razysknych meropriyatiy, English: System for Operative Investigation Measures).

Huge amounts of storage space are needed to implement the law on data retention.
© pixabay



© pixabay

A new generation of devices (SORM-3) made it possible to intercept all kinds of communication (calls over landlines or mobile networks, as well as internet traffic including e-mail and IP telephony) and store them for even longer.[2]

Telecommunications operators and internet service providers in Russia are obligated by law to install SORM technology–known as "black boxes". Through these, the domestic security agency FSB has direct access to citizens' communications data at all times, without having to submit requests to the operators or to present a warrant. To date, however, these devices have been installed by only a fraction of the internet service providers in the country. First of all, there is nowhere near enough state-certified SORM-3 technology available, according to Fabian Burkhardt of the German Institute for International and Security Affairs (SWP) in an interview with RSF. Secondly, small and medium-sized companies claim that they can hardly afford to purchase the expensive equipment.

↑ Irina Borogan (top) and Andrei Soldatov are specialised in the topic of surveillance.
© Konstantin Zavrashin

The journalists Andrei Soldatov and Irina Borogan, who have been researching the subject of surveillance for years, compared SORM with PRISM, the surveillance program of the US National Security Agency exposed by the whistle-blower Edward Snowden. In their book *The Red Web*,[3] they lament the population's indifference to the subject of surveillance. They trace this back to Russia's lack of any reappraisal of the history of Soviet security service, the KGB, and to the lack of any significant institutional reform to its successors. No public debate about the powers of the security services ever took place, they continued; because of the historical legacy, many take state surveillance for granted. In an interview with RSF, Artem Kozlyuk of *Roskomsvoboda* confirmed, "The general public are unaware that internet censorship is a problem. No one understands the particulars–especially the technology."

---

[2] SORM-3 was developed and tested before the 2014 Olympic Games in Sochi.
[3] Andrei Soldatov and Irina Borogan, *The Red Web. The Kremlin's War on the Internet.* (New York: Public Affairs, 2015).

→ Journalist Roman Zakharov was successful with his complaint against mass surveillance before the ECHR. © RSF Germany

↘ US whistleblower Edward Snowden has been living in Russia since 2013. © picture alliance / AP Images

One of the few to strike back against mass surveillance through SORM without just cause was the journalist Roman Zakharov. In 2003, he filed a suit against three mobile communications providers for violating his privacy with the SORM technology they deployed. Meeting with little success in the Russian courts, in 2006, Zakharov brought the case to the European Court of Human Rights in Strasbourg, which issued a widely noted decision in 2015, ruling that SORM violates the privacy rights guaranteed in Article 8 of the European Convention on Human Rights. During the trials, Russian security forces searched Zakharov's home on multiple occasions without prior notice; he was arrested twice. He now lives in exile, where he continues to work as editor-in-chief of the news portal *legalpress.ru*.

Since 2014, various laws have been passed which are directed against anonymous or encrypted online communication: the state's media monitoring agency *Roskomnadzor* set up a new database of what they termed "organisers of dissemination of information" (Russian abbreviation: ORI), with which providers of e-mail and messaging services as well as social networks were required to register. Registration obligates them to save user data and, if requested to do so, make these accessible to law enforcement authorities. A law passed in July 2014 (which took effect in September 2015) stipulates that private data on Russian citizens can no longer be stored abroad, but only on servers in Russia. The Russian government introduced this legislation in the wake of Edward Snowden's leaks, arguing that data protection must be ensured. Furthermore, providers of messaging services were required to open interfaces in their programs to the security services, allowing them to read encrypted messages (See Chapter 2).

At the same time, through the Yarovaya laws, Russia has introduced "unprecedented data retention", stated Dmitry Kononenko of the German-Russian Chamber of Commerce in an interview with RSF. The regulations that took effect on July 1st 2018 are more comprehensive than in almost any other country in the world: connection data (meaning information about who phoned or exchanged messages with whom when) are to be stored for three years; the content of telephone calls, messages, photos or videos for six months. This requires telecommunications operators and internet service providers to invest tremendous amounts in new technology and storage capacity. In addition, they pose the question of how much sense it makes to store huge amounts of data when the bulk of them are encrypted. The implementation of these regulations is being held up; by summer 2019, only a fraction of the countries had installed the required technology.[4] "In the Duma and the government, there are a number of politicians who lack the digital know-how to grasp the effect of their legislation", notes Kononenko.

➲ For comparison: **the data retention law** reintroduced in Germany in late 2015 requires telecommunications operators, as of July 1st 2017, to store communication data on all their customers without occasion for ten weeks, and the locations of mobile phones for four weeks. However, after several complaints from providers, the *Bundesnetzagentur* (Federal Network Agency) suspended the requirement shortly before the law was due to take effect. Now the Court of Justice of the European Union must make a final, legally effective decision. Until that time, connection data may not be stored in Germany without occasion or a concrete suspicion–and this applies to the content of communications in any case.

[4] As for SORM-3, this is partly because government agencies are not able to keep up with certification of the devices. This put providers in a difficult situation: they are formally required to comply with a law which they can implement in practice only partially or not at all–and yet the companies face sanctions for non-compliance. Artem Kozlyuk of *Roskomsvoboda* therefore anticipates more intensive monopolisation on the market for telecommunications operators and internet service providers, in favour of large corporations associated with the government.

← *Roskomsvoboda* head Artem Kozlyuk © private image

Artem Kozlyuk of *Roskomsvoboda* calls it a "major problem that the consequences of a law do not become apparent until years after it is enacted". Generally, several years pass before new regulations are actually implemented. Moreover, the authorities usually apply the laws first to services and platforms used by only a small section of the population, so that blocking them does not cause much protest. Thus, in November 2016, the US professional networking service LinkedIn was blocked when it refused to move its servers to Russia. Since April 2017, the authorities have blocked the walkie-talkie app Zello, which HGV drivers had used to coordinate protests and strikes. The messaging services Imo, Blackberry and Line, as well as the video chat platform VChat were blocked because they did not want to be registered as "organisers of dissemination of information". Around the same time, the messaging services Threema and Telegram joined the register–and they both expressly refused to hand over user data to the authorities and to abandon end-to-end encryption.[5] The attempt by *Roskomnadzor* in spring 2018 to block the messaging service *Telegram*, which is used by 15 million people, failed spectacularly. It caused massive outages in the Russian internet (see box), sending 12,000 out on the streets of Moscow to protest internet censorship. In March 2019, the authorities made a technically more sophisticated attempt to block ProtonMail, a service that offers end-to-end encrypted e-mail traffic–also unsuccessfully.

➲ In **end-to-end encryption,** data are encrypted before they are dispatched from the sender and decrypted after arrival on the recipient's device. Thus, only the two parties communicating with each other have access to the transmitted content–they are hidden from even the providers of the transmission services. In transport encryption, by contrast, data are encrypted only for transfer between a device and the provider, so they are available in non-encrypted form at the start and end of the communication as well as at the nodes of data transmission. So if two people communicate with each other via Facebook, for instance, the communication channel between the two and Facebook is encrypted for transport, but Facebook itself can read the content. End-to-end encryption is used only when the users start a "secret chat" in Facebook Messenger.

Because they offer an opportunity to circumvent internet censorship, the authorities have set their sights on the providers of Virtual Private Networks (VPNs). A law passed in July 2017 (which took effect in November 2017) prohibited VPN providers and anonymization services from allowing access to pages blocked by *Roskomnadzor*. "Of course, this reduces their services to absurdity", says Dmitry Kononenko of the German-Russian Chamber of Commerce. Initially, the law did not have any practical consequences. Not until late March 2019 did the media monitoring agency demand that the ten most popular VPN providers register as "organisers of dissemination of information" and stop allowing their users to access blocked websites. The Russian software company Kaspersky Lab was the only company to consent immediately by allowing its VPN provider Kaspersky Secure Connection to be registered. All other VPN providers refused to comply with *Roskomnadzor*'s request, and several of them shut down all of their servers located on Russian territory in order to protect their data.

➲ **Virtual Private Networks (VPN)** further encrypt internet traffic by building a kind of tunnel around the actual internet connection. This tunnel functions as a kind of privacy screen: data can be neither monitored nor stored by any party outside the VPN connection, and there is no way to influence which websites are opened. Thus, users in Russia can connect via VPN to open even websites that have been blocked by the state's media monitoring agency.

A completely new stage in the government's efforts to control internet content and online communication was reached with the introduction of the "sovereign internet law" in May 2019. This legislation was introduced in response to intensifying confrontations with the US, which designated Russia as one of its main strategic enemies and reserved the right to launch preventative cyberattacks. The law is intended to ensure the independent functioning of the internet in case of–as yet undefined–dangers, and gives the state control of the network infrastructure: in future, internet service providers are to direct all data traffic via internet exchange points (IXPs) registered with the media monitoring agency. In case of emergency, a new control centre will switch to centralised routing.

The law further requires that all internet service providers or operators of internet exchange points install new equipment. The technology behind the new devices, which first have to be certified by the state, will allow the media monitoring agency to route internet traffic centrally in case of emergency and to block websites. So far

[5] Threema messages are encrypted end-to-end by default; in Telegram this function can be configured for "secret chats".

providers have been responsible for blocking websites: they must ensure that they are connected to the state information system and always have the latest version of the official "single register" at their disposal, in order to block all content that is currently blacklisted. By means of the new devices, the media monitoring authority could implement content blocks without the cooperation–or, indeed, knowledge–of the providers. Neither the companies nor the public would have an overall view of which websites the government blocks when and for how long.

The new devices to be installed are reputed to enable Deep Packet Inspection (DPI) throughout the country. This technology allows content to be blocked in a more targeted way than the previous method of blocking IP addresses. Several major mobile communications providers in Russia have been using DPI since the mid-2000s in order to influence the data traffic over their networks. For instance, it allows them to prevent downloads of extremely large audio and video files, and to block IP telephony providers who compete with their own telephone business. However, not even DPI technology can investigate the content of encrypted connections–which make up 85 to 90 percent of internet traffic in Russia today. Countries such as China show that DPI can be used to detect and block anonymization services. The journalist Andrei Soldatov suspects that Russian authorities could use the new devices primarily to suppress the propagation of live videos at protests.

When and in what manner the "sovereign internet law" can actually be implemented everywhere in Russia's internet remains unclear. Originally, the new regulations were supposed to take effect on November 1st 2019–yet at this point in time, most internet service providers did not have the necessary technical equipment at their disposal. According to the news portal *RBC*, surveillance with equipment that supports DPI was initially being tested in the Ural Federal District. In late October, installation of the necessary equipment began at the facilities of "the big four"–the most important Russian telecommunications companies Rostelecom, MTS, MegaFon and VimpelCom–and at several smaller operators, too. The equipment has been activated at intervals on a trial basis, with testing to be completed by the end of 2019. According to the head of *Roskomnadzor*, Alexander Zharov, the purpose of the tests is to ascertain whether the devices block websites reliably, and how they affect transmission speeds and user-friendliness. Only landlines are being tested in this first round; so far, the mobile internet has been excluded.

➲ **Deep Packet Inspection** (DPI) is a method of monitoring and filtering data traffic in the internet. Before large amounts of data are transmitted to the web, they are broken down into small units that can be transmitted more easily (packets), and these packets are labelled with meta-information (such as sender, recipient, size of packet). While conventional packet filters read only the meta-information included in the header of a data packet, applying DPI to non-encrypted communications allows the content of the data packets to be monitored in real time–something like the postal service checking not only the address and return address on a letter before delivery, but also its content.

↑
The Federal Security Service is demanding the keys to decode online communications.
© pixabay / JeongGuHyeok

Russian experts criticise the "sovereign internet law", fearing that it will have negative effects on the IT sector's capacity for innovation. The law stipulates that the state will bear the costs for the new devices, with the December 2018 budget earmarking a total of Rb 30 billion (approx. €400 million) from the Digital Economy national programme for the next three years. However, introducing filter technology that supports DPI throughout the entire country could cost a great deal more, as maintaining the devices and the large servers for data storage is expensive. "The companies are afraid that these costs will ultimately fall to them", explained Artem Kozlyuk in an interview with RSF. "They will pass these costs on to their customers. In the next few years, everything that has to do with the internet will become considerably more expensive–with negative consequences for the economy and for Russian technology companies."

IF ALL ELSE FAILS, SWITCH IT OFF

In extreme cases, Russian authorities do not hesitate to simply block access to the internet–while this has only affected mobile connections so far. In autumn 2018, this became apparent in the North Caucasus Republic of Igushetia, where some of the citizens were protesting against the new border to the neighbouring Chechen Republic. In locations where protest demonstrations took place, the mobile internet was switched off, on several occasions for days at a time. After complaints from users, the mobile communications operators explained that they had been instructed to do so by the government. During the protests in Moscow in summer 2019, too, the mobile internet ceased to function in certain districts of the city. At present, the authorities depend on the cooperation of providers and mobile network operators to enforce such internet blocks. The "sovereign internet law" is intended to make it possible for them to throttle internet access for the entire population at any time–and not only on mobile devices but also over landlines. As Andrei Soldatov, a journalist specialising in surveillance, commented: "No one in the Kremlin believes that the internet can be controlled completely–but preventing protests from spreading from one region to another is absolutely realistic."

↓
A demonstration in Magas, the capital of Ingushetia, against the redrawing of the country's border with neighbouring Chechnya

↑
Software from Russia can be used to analyse phone calls intercepted in Mexico within just a few seconds.
© picture alliance / DUMONT Bildarchiv

SURVEILLANCE TECHNOLOGY EXPORTS

Russian surveillance technology is popular with autocratic regimes worldwide: it costs a fraction of comparable products from China, it requires a less sophisticated IT environment and it makes an impact particularly in combination with repressive laws and intimidation by security agencies. Numerous neighbouring countries have taken on elements of the Russian mass surveilance system over the past two decades–in terms of both technology and laws. Since 2010, the regime in Belarus not only has been using a monitoring system similar to SORM but also Semantic Archive software produced by the Russian company Analytical Business Solutions that evaluates data from media archives, blogs and social networks. In Kyrgyzstan, state monitoring was adapted to the Russian model in 2012 and St Petersburg company Protei quipped telecommunications operators and internet service providers with SORM-3 technology. Providers in Kyrgyzstan are required to retain all communications data for three years, just like in Russia. Kazakhstan also uses SORM technology that supports DPI, enabling the government to monitor data traffic in real time throughout the country. Yet Russian companies' exports extend beyond the successor states of the Soviet Union. Protei also exports to the Middle East (Bahrain, Iraq and Qatar) and Latin America (Cuba, Mexico and Venezuela). SpeechPro, a company specialising in voice and facial recognition, has a branch in the United States and says it sells its technology to over 70 countries including Saudi Arabia, Algeria, Yemen and Turkey. SpeechPro conducted its first national voice recognition project in Mexico in 2010. Government officials and prisoners had to supply voice samples, as did anyone applying for a driver's licence. The company advertises that it takes only seconds to identify an individual whose telephone is tapped. In Ecuador, SpeechPro combined voice recognition and facial recognition shortly afterwards.

THE FAILED ATTEMPT TO BLOCK TELEGRAM

When Pavel Durov joined forces with his older brother Nikolai to develop the messaging service Telegram, he was still head of the social network VKontakte. He had founded the Russian version of Facebook in 2006, which quickly became the most popular platform in the country. Yet Durov ran afoul of the domestic security service FSB when, after the mass protests of 2011, he refused to close the VKontakte pages of several groups that were critical of the Kremlin protests. In late 2013, he refused to hand over the data of Ukrainian activists who belonged to the Euromaidan movement. As VKontakte came under increasing economic pressure, Durov sold his shares in the company and left the country. The new owner of VKontakte was the Kremlin-friendly Mail.ru Group, which has since taken combined ownership of the three most popular social networks (VKontakte, Odnoklassniki and Moi Mir).

The Durov brothers' new project, Telegram, which went online in August 2013, deprived government agencies and security services of access from the outset. The Durovs rented data centres worldwide, in locations including London, San Francisco, Singapore, Dubai and Helsinki, and listed various companies registered in a variety of places as the company's operator. As a result, they were "not obligated to abide by the regulations of Russia, China, Saudi Arabia or similar states", explained Durov.

Telegram was one of the first services to offer communication encrypted end-to-end, which made it an instant hit–not only among activists but also with politicians, who used it for their internal communications. Particularly popular in Russia were the "channels", in which sources, many of them anonymous, propagated allegedly inside information from governmental officials. Fifteen million people in Russia used the service in 2018; it had over 200 million users worldwide. Even Kremlin Spokesperson Dmitry Peskov and the Russian Foreign Office used Telegram for communication with journalists.

The messaging service became a constant provocation for the Russian media monitoring agency. On June 23rd 2017, *Roskomnadzor* threatened to close Telegram down if Durov did not allow his service to be registered as an official "organiser of dissemination of information". Three days later, the domestic security service FSB announced that the men behind the attack on the St Petersburg metro had communicated via Telegram. In the attack on April 3rd 2017, 16 people had been killed and more than 50 injured. The state television channels repeated the

↓
A demonstration in Moscow in April 2018 against the blocking of messaging app Telegram
© dpa

accusations against Telegram so often that some media suspected a targeted campaign against the messaging service. Durov commented laconically: "If terrorism is to be defeated by blocking communication, the entire internet will have to be blocked." On VKontakte he explained that all of the information required for registration in the official list was publicly accessible, but that he would still not hand over the personal data of Telegram users.

In response, the media monitoring authority included Telegram in its register in late June 2017. Just two weeks later, the FSB contacted Durov and demanded the data needed to trace the communications conducted via six specific telephone numbers. Telegram ignored the request and was consequently sentenced to a fine of Rb 800,000 (approx. €12,000) in October 2017; in December, a court in Moscow upheld the sentence. The lawyers of the human rights organisation *Agora*, representing Telegram in Russia, responded by appealing to the Supreme Court–to no avail: In mid-March 2018, the court declared that the domestic security service's demands were lawful. On April 13th 2018, a court in Moscow granted the petition of the media monitoring agency *Roskomnadzor*, and Telegram was officially prohibited in Russia.

↑
Telegram founder Pavel Durov

Ultimately, however, the state leadership was humiliated because the media monitoring agency did not manage to implement the ban on a technical level. They temporarily blocked as many as 20 million IP addresses–"carpet bombing" of the internet, as the business daily Vedomosti quipped. Telegram was hurt less than countless online vendors, mail-order companies and courier services. Even the pages of many online media were temporarily inaccessible. More than 100 companies contacted the human rights organisation *Agora*, requesting legal assistance to receive compensation for massive losses of earnings.

In the meantime, Telegram circumvented the blockade attempts with a clever strategy: after internet providers blocked the first IP addresses, the messaging diverted its traffic to the cloud services of US concerns like Amazon and Google, rapidly switching between thousands of IP addresses. Telegram took advantage of a technology known as "domain fronting" which conceals the actual end point of an internet connection. As a result, most people in Russia had no problems using the messaging, and did not even have to switch to a VPN. On April 30th 2018, around 12,000 people protested the Telegram ban in the centre of Moscow, throwing paper airplanes in the air in allusion to the messaging logo.

One and a half years after the official ban, Telegram remains accessible in wide areas of Russia, and is at least as popular as ever. Telegram has become the third favourite short messaging service, after WhatsApp and Viber. A survey in June 2019 revealed that a full 40 percent of all Russian users now have Telegram installed on their smartphones–15 percent more than the year before. The state leadership is now hoping that improved filtering technology will allow Telegram to be blocked effectively: The "sovereign internet law" of May 2019 requires every internet service provider to install new devices to monitor online traffic. Installing this equipment all over the country is likely to take years, however.

7 PRESSURE ON INTERNET COMPANIES: THE CRUCIAL ROLE OF INTERNATIONAL PLATFORMS

➲ In expert discussions, RSF calls social networks such as Facebook, search engines such as Google or microblogging services such as Twitter information intermediaries. These services can no longer be assigned to the established categories of classical media and mere intermediaries of– usually technical–information. Traditional media prepare journalistic content and decide on the relevance they attach to a particular topic. Intermediaries such as telecommunications operators or internet providers make the technical infrastructure available and transmit signals without evaluating information. Social networks, search engines and similar services are located between these two poles: they also provide infrastructure of their own and generally do not prepare content themselves, but they do evaluate information according to relevance criteria using algorithms.

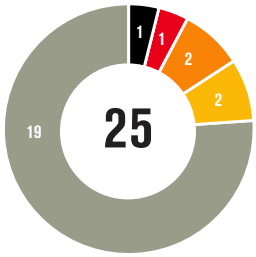
International online platforms have become integral to Russia: WhatsApp is installed on one out of two smartphones and YouTube is one of the country's most popular social networks. The platforms are required by law to store Russian citizens' personal data exclusively on servers in Russia, Google must not display blocked content and messaging services must enable surveillance of encrypted communication. Although hardly any companies comply, for a long time the Russian state's media monitoring agency did not go beyond verbal threats. However, pressure has been mounting on the platforms since 2018: fines have been levied and laws toughened. Whereas Google is cooperating with the authorities to some extent, Twitter and Facebook have refused to do so to date.

Russia is one of the few countries in which domestic online platforms are serious competitors to American services; some of them have even overtaken them in terms of user numbers.[1] International platforms are nevertheless very important in Russia. According to a survey by the independent Levada Centre, just under one third (30 percent) of all Russians use the video portal YouTube, which belongs to the Google corporation. Political bloggers and activists, artists and politicians can produce videos with minimal technical effort and reach hundreds of thousands of people through YouTube. Critical media professionals have been using the platform to address their audience directly since they were dismissed or their programmes were dropped from state television (see Chapter 4). The number of people who have subscribed to the channel of well-known Russian YouTuber Yury Dud is two to three times that of subscribers to the channels of the state television broadcasting across the country. According to the Levada survey, YouTube is ranked third among the most popular social networks in Russia. VKontakte (VK) holds first place; this belongs to the Mail.ru Group, which has ties to the Kremlin. However, VKontakte not only has the most users (42 percent) but was also mentioned most often in 2018 when people were sentenced to prison because of their online activities in social networks: most cases (76 percent) involved statements on VKontakte, as documented by the human rights organisation *Agora*.

[1] In Russia, the search engine Yandex and the social network VKontakte are used by significantly more people than their American counterparts Google and Facebook.

Prison sentences were imposed in 2018 in relation to activities in the following social networks:*

Source: Agora



VKontakte
Odnoklassniki
YouTube
Facebook
Telegram

* All sentences with references to a particular platform were counted.

International online platforms are important channels for independent journalists to reach their audience. Roman Dobrokhotov, founder and editor-in-chief of the website *The Insider*, which specialises in investigative research, told RSF, "We benefit a lot from the 'instant articles' on Facebook. After all, our content cannot be blocked easily if they are part of Facebook. They also bring in well-paid advertising. In other words, they're a source of income." Alexandra Perepelova, editor-in-chief of *TV Dozhd*, said that a significant section of her channel's audience comes through Facebook. Galina Timchenko, founder and publisher of the online magazine *Meduza*, said that social networks and news aggregators such as Google Discover brought *Meduza* most of its readership. International platforms have become even more important since the Russian tech companies Yandex und Mail.ru have no longer been displaying content or websites blocked by the state's media monitoring agency in their search results or through the news aggregators Yandex Zen and Mail.ru Pulse.[2]

The crucial role of international platforms becomes even more clear when it comes to messaging services used by people in Russia for text messaging or telephone calls. According to the Levada Centre, almost half (49 percent) of the population uses the American service WhatsApp, which belongs to Facebook and uses end-to-end encryption for its users' communication by default. Skype is used by 14 percent of Russians, the service Telegram–which is banned in Russia–by 8 percent and Facebook Messenger by 3 percent. These services permit users to opt for end-to-end encryption for chats and calls, which then cannot be intercepted or read by intelligence services or law enforcement authorities in Russia–unless the service providers open interfaces (known as back doors) for them in their programs.

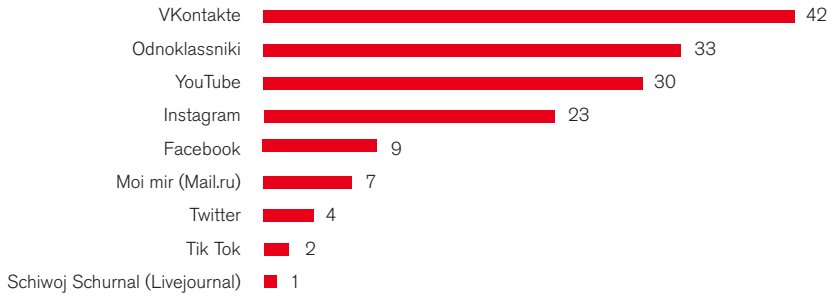
↖
TV journalist Leonid Parfyonov has relaunched his show *Namedni* on YouTube.
© Screenshot YouTube
Parfenon

↑
The Moscow city council pays journalist Irina Shikhman for her YouTube show.
© Screenshot YouTube
А поговорить?

[2] Yandex and Mail.ru are thus implementing Federal Law No. 276-FZ; this entered into force in November 2017 (see Chapter 2).

Use of social networks in Russia*

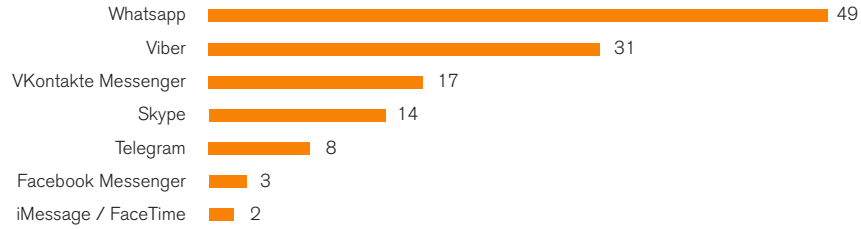
Survey by the Levada Centre, March 2019



* Percentage of the population over 18

What apps on your mobile do you use for calls or messaging?*

Survey by the Levada Centre, March 2019



* Percentage of the population over 18

Since 2014, the Russian parliament has used various laws to set ever tighter limits on the activities of national and international online platforms–at least in theory: operators of social networks and messaging services must register with the state's media monitoring agency as "organisers of dissemination of information" (Federal Law No. 97-FZ) and enable the FSB, Russia's domestic intelligence service, to intercept encrypted communication, too (Federal Law No. 374-FZ). Russian citizens' personal data must be stored exclusively on servers in Russia (Federal Law No. 242-FZ) and search engines must not provide references to content or websites banned in Russia (Federal Law No. 276-FZ, see Chapter 2).

In the first few years after these laws took effect, the state's media monitoring agency *Roskomnadzor* merely issued the regularly repeated threat to international providers such as Google, Twitter and Facebook that they could be blocked if they did not comply with Russian law. Representatives of the platforms regularly travelled to Moscow for talks with *Roskomnadzor*, but no details were ever revealed. "We have not been told anything about who exactly participates in these meetings, what is discussed or even agreed", Artem Kozlyuk of the NGO *Roskomsvoboda* told RSF. *Roskomnadzor*'s threats initially had no serious consequences.

This all changed in 2018. The Russian human rights organisation *Agora*, which documents the status of internet freedom on an annual basis, even speaks of a "fundamental turnaround" in the government's policy: "The pressure on the international platforms is increasing, the days of endless talks and negotiations are coming to an end", according to its February 2019 report. Immediately after the messaging service Telegram was banned, the state's media monitoring agency threatened in April 2018 to block Facebook, too, if it continued to refuse to move its servers to Russia. A law adopted in June 2018 (Federal Law No. 155-FZ) significantly increased the fines for search engine operators if they display banned content or link to this. Google was accordingly sentenced to a fine of Rb 500,000 (approx. €6,700).

It became apparent in January 2019 that Google no longer displays some of the content blocked by *Roskomnadzor* as search results. Although the platform was not yet technically connected with the authority's Unified Register of Prohibited Sites– the blacklist–it did receive daily updates from *Roskomnadzor*, according to Russian media. Whereas Russian providers automatically block content listed in the register, Google staff were said to decide on a case-by-case basis which websites would be blocked. Alexander Zharov, head of *Roskomnadzor*, declared in June 2019 that the authority maintained the closest contact to Google compared with other international platforms. At the same time, he complained that Google did not filter out enough banned websites. Shortly afterwards, the platform was sentenced to another fine, this time amounting to Rb 700,000 (approx. €9,900).

In January 2019, administrative proceedings were initiated against Twitter and Facebook because they violate the law requiring Russian users' data to be stored exclusively on servers in Russia. Both companies were sentenced to a more symbolic fine of Rb 3,000 (approx. €41) each. Shortly before this, Facebook CEO Mark Zuckerberg had declared that, as a matter of principle, Facebook did not operate data centres in countries that abused human rights such as the right to privacy or the freedom of expression. If individual countries blocked the network for this reason, so be it. Whereas Twitter paid the fine by the deadline at the end of August, Facebook did not.

↓
Likes and searches prohibited! NGO *Roskomsvoboda* comments on a law that threatens international platforms with fines in the millions.

YANDEX: A CHAINED HIGH-TECH TIGER

In Russia, Google is merely Yandex's little sister. The most valuable Russian IT company, Yandex plays a dominant role, controlling almost 60 percent of the domestic market. Not only is it the fourth largest search engine in the world, but it also offers music streaming and online translations, a food delivery service and apps ranging from the metro schedule to a road traffic app. Yandex took its own maps and a new platform online before Google did. Yandex.Taxi was launched in 2011; it later took over the American platform Uber's business and is the undisputed market leader in Russia today. In 2018, it entered into a joint venture with the state Sberbank to expand its marketplace and become the Russian counterpart to Amazon. In May 2019, Yandex put its first self-driving cars on the road, competing with Google's subsidiary Waymo. Yandex claims to employ 10,000 staff members, many of whom it recruits through its own School for Data Analysis.

Computer scientist Arkady Volozh, who was born in Kazakhstan, founded the search engine in 1997 with his former schoolmate Ilya Segalovich. They took Yandex public on the New York Stock Exchange in 2011, raising $1.3 billion (approx. €1,2 billion). Since then, the greatest threat to the company has been the political situation in Russia. Ilya Segalovich was actively involved in the protests against Vladimir Putin in 2011/12 but died of cancer shortly afterwards. When the law introducing a blacklist of websites subject to blocking entered into force in November 2012, Yandex lost some of its brightest minds: Lev Gerzhenzon, founder of the news platform, left the company, as did marketing director Elena Kolmanovskaya, who said it "no longer made sense" to work for Yandex. In 2014, President Putin called the internet a "project of the CIA" and insinuated that Yandex maintained connections to foreign intelligence services–whereupon its stock price plummeted.

Tatyana Isayeva, the director of the news platform, left Yandex in 2016 when a new law made news aggregators responsible for the content they disseminated (see Chapter 2). For Yandex, this meant that it had to limit its work to disseminating content from media registered with the Russian state's media monitoring agency. Since then, online portals such as *Meduza*, independent blogs and foreign media have no longer been displayed in the five top news stories on the homepage or in Yandex Zen, a personal recommendation service. In 2017, Ukraine imposed sanctions because of the war with Russia, and Yandex was forced to close its offices in Kiev and Odessa. In July 2019, a draft bill was introduced to parliament limiting foreign stakes in large digital companies to only 20 percent. The stock price tumbled again–until Yandex, whose parent company is registered in the Netherlands, reached a compromise with the state leadership in mid-November 2019: a foundation headquartered in the Russian exclave Kaliningrad is intended to ensure that no investor holds more than 10 percent of the company in the future. If the foundation detects any danger to national security, it can even dismiss Yandex's director for Russia. It is questionable whether the company's innovative power will be retained under these conditions.

←
Yandex founder
Arkady Volozh

↑
The state-owned television channel *Russia-1* can also be watched on smart phones.
© picture alliance / AP Photo

At the same time, the Russian parliament also increased pressure on international platforms. In mid-June 2019, the ruling party, United Russia, introduced a draft bill intended to increase the fines for platforms not obeying Russian laws many times over. For example, companies that store Russian users' personal data on servers outside Russia would be fined up to Rb 18 million (approx. €254,000). "Our experience with Google shows that we can force companies to collaborate with the state if we impose fines", said *Roskomnadzor* head Alexander Zharov. Artem Kozlyuk, director of the NGO *Roskomsvoboda*, said, "This is the agency's new strategy: not as much blocking but higher fines." In an extraordinary session on August 19th 2019, the Council of the State Duma established a Commission on Foreign Interference in Russia's Internal Affairs. The chair of the commission, Vasily Piskarev, accused Google and Facebook of having disseminated banned political advertising and calls for unauthorised demonstrations prior to the controversial regional elections on September 8th 2019 and also supported fines running into the millions. This was common practice internationally and the only means of putting pressure on companies, Piskarev said. Facebook and Google rejected the accusations.

It remained unclear whether and how the Russian government can enforce its demands with respect to the American companies: Facebook, which is used by more than 40 million people in Russia, does not maintain an office in Russia–neither does Twitter–and there is no mutual legal assistance treaty between Russia and the US that would be applicable in this case. This helps the platforms to evade the pressure from the Russian regulatory authorities, at least in part. Yet the fact that those responsible cannot be reached is a problem for independent media professionals: "Although Facebook presents itself as a modern business, it is a very poor service provider as it is practically impossible for people to reach it", complained Roman Dobrokhotov of *The Insider*, for example. On the other hand, he said it was easy to call the Russian provider Yandex, which even provided designated contact persons for media with a certain number of followers.

Representatives of these US companies were not particularly forthcoming when RSF approached them while conducting the research for this report. In light of increasing internet regulation and because of possible danger to staff members, the difficulties of working in Russia are a highly sensitive topic. Consequently, the platforms intentionally refrain from outspoken public statements, instead attempting to find solutions with the Russian authorities diplomatically and behind the scenes. For this reason, they have little interest in discussing these topics in public or granting journalists deeper insights into their work.

PUBLIC CONTROL OF INTERNATIONAL PLATFORMS WORLDWIDE

Global internet platforms are faced with the same dilemma in Russia as in many other countries: since they have gained key importance for social and political debates because of their size, governments are increasingly demanding that the companies do not base their decisions solely on their own "community standards". On the other hand, reference to these community standards is often the only way to ignore state demands to block content, particularly in autocratic states. Consequently, RSF argues that the companies' community standards should be developed further with a view to principles of international law. This could give rise to corporations having a "right to determine who shall be allowed or denied digital access" in line with the national laws of democratic countries–and that simultaneously provides the opportunity to resist laws of authoritarian states that serve to censor and that disregard principles of international law.

In the 2018 report, "Regulierung 2.0", RSF Germany made proposals for public control of platforms such as Facebook, Google and Twitter. RSF Germany thinks that these services are no longer purely private companies, but that they must be specially regulated as an integral element of the modern public sphere. The report includes recommendations to lawmakers for combatting hate and fake news on the internet and controlling the influence of algorithmic systems without limiting press freedom and freedom of expression in the process. RSF advocates grasping the platforms as part of the basic information services that are essential for democratic societies, and enshrining this in law. This would entail greater due diligence and greater transparency requirements for the companies as well as stronger public control. With this report, RSF Germany also responded to the German Network Enforcement Act,[3] which had resulted in excessive blocking of legal content in social networks (overblocking). It also creates the danger that the companies improperly restrict their community standards for fear of fines. That is why RSF Germany proposed, among other things, establishing independent supervisory bodies to monitor the companies' procedures for blocking content.

↓
Inauguration of the Forum on Information and Democracy in Paris in November 2019
© Aurélien Faidy / AutoFocus-prod / RSF

In November 2018, Facebook presented plans for a global oversight board responsible for deciding questions relating to freedom of expression in the social network in the future. RSF Germany participated intensively in the subsequent discussion process, including a two-day workshop in Berlin in June 2019. In mid-September, Facebook published the charter of the new oversight board. It will have 11 to 40 members, assess users' requests for review of Facebook's decisions and provide policy guidance to Facebook. RSF is critical of the fact that the board's recommendations will have little impact on the algorithms with which Facebook filters and curates content on the platform.

Moreover, the charter of the oversight board does address the problem of censorship in countries with authoritarian governments that require platform operators to obey laws that violate the right to freedom of expression. Clear guidelines that prioritise international human rights standards over national laws are lacking here. In September 2019, Facebook updated the values forming the basis for its community standards and reasserted its commitment to free speech. Yet freedom of expression is not enough to guarantee a democratic debate. If manipulated information influences users, this is even detrimental to the process of democratic decision-making.[4]

For this reason, Reporters Without Borders launched the International Initiative on Information and Democracy in September 2018. It intends to establish fundamental principles for the global information and communication space, which is a "common good of humankind".

In November 2018, the International Declaration on Information and Democracy, published by the Commission convened by Reporters Without Borders, received the political support of twelve heads of state and governments during the first edition of the Paris Peace Forum.

A group of 20 like-minded states then drafted the International Partnership on Information and Democracy, which was formally endorsed by a coalition of 30 states on the margins of the UN General Assembly in September 2019.

This Partnership will be implemented by the Forum on Information and Democracy, a new international body led by civil society organisations. The Forum was created in November 2019 by eleven organisations from different regions and fields of expertise. It will issue research-based recommendations for regulation of the information and communication space as well as self-regulation of the actors.

---

[3] The Network Enforcement Act, which was adopted in June 2017 and fully entered into force in January 2018, is intended to combat hate crimes on the internet. It requires operators of platforms with more than 2 million users in Germany to delete or block any "manifestly unlawful content" within 24 hours. Otherwise, fines of up to €50m may apply. In addition, the networks are required to publish biannual reports detailing how they handle complaints and requests for blocking.

[4] Facebook announced in October 2019 that it would label content from state-controlled media in the future.

8 RECOMMENDATIONS

Reporters Without Borders (RSF) calls on the government and parliament of Russia to take the following steps:

- Immediately **free all journalists and bloggers** who are jailed in connection with their journalistic activities online and stop prosecutions based on politically motivated charges of extremism, terrorism or separatism.

- **Repeal** all **laws** that limit or criminally sanction the exercise of the human right to press freedom and freedom of expression in the digital space; implement Russia's obligations under the European Convention on Human Rights and the Russian constitution, in particular Article 29 (**freedom of expression**), Article 23 (**right to privacy**, secrecy of postal communication and telecommunications) and Article 24 (**protection of personal data**).

- **End mass surveillance** without just cause using SORM and revise all laws that allow criminal investigation or security authorities blanket access to digital communications. These changes are to ensure that surveillance measures are implemented only for purposes regulated by law, under supervision of a court and for a limited period of time. They are to be terminated at the end of the period for which they were ordered, and the data stored are to be destroyed after an appropriate period. Persons affected should be informed after the end of the surveillance and should have the legally guaranteed right to take legal action in independent courts against illegitimate surveillance.

- **Put an end to arbitrary online censorship**, particularly temporary mobile network shutdowns in certain regions, and guarantee the free use of the internet at all times and throughout the country.

- **Unblock illegally blocked websites** and stop blocking websites without a judicial decision or the possibility of an appeal to an independent and impartial court of law.

- **Refrain from requiring providers** of messaging or e-mail services **to keep back doors in the programs** open to be able to follow encrypted communications.

- Permit **unrestricted use of VPNs** and anonymizers.

- Stop attempts to fragment the **infrastructure of the internet** by disconnecting Russia from the global internet network.

Reporters Without Borders (RSF) appeals to the governments of democratic states to take the following steps:

- **Consider that their actions** and laws on encrypted communication, anonymization, digital surveillance or regulation of social media **function as signals** internationally; and refrain from adopting laws that undemocratic states can use as pretexts for undermining human rights standards and that can facilitate mass surveillance without just cause or overblocking, for example.

- **Not to delegate the difficult legal weighing of interests** such as that between the individual right to privacy and the right of the public to unimpeded access to information, particularly with a view to the potential consequences in undemocratic states, **to private companies**.

Reporters Without Borders (RSF) calls on the international community to take the following steps:

- **Step up pressure on the Russian government** by taking actions which may raise the cost of its non-compliance with international human rights standards.

- At the next session of the **United Nations** Human Rights Council, a resolution should be adopted that asks the Office of the **UN High Commissioner for Human Rights** to produce a **report** on the situation of human rights, including press freedom and internet censorship, in Russia.

- **The UN Special Rapporteur** on the promotion and protection of the right to freedom of opinion and expression **should submit a report on online censorship** in Russia.

- **The European Parliament should**, as appropriate, **adopt further sanctions** against individuals or companies in Russia that play a prominent role in censoring the internet.

Reporters Without Borders (RSF) recommends that companies such as Facebook, Twitter and Google take the following steps:

- Fulfil their responsibility as **innovation intermediaries** by putting their **community standards** in line with international law, in particular concerning **the right to freedom of expression** (Article 19 of the ICCPR), in order to enshrine the **right to privacy** and sufficient **data protection** therein.

- Conduct **human rights due diligence** and commit to **resisting** any **demands** by states **to censor** the internet or to monitor content in a manner that infringes on human rights; this applies in particular to demands by the Russian authorities that certain content no longer be displayed or disseminated unless this has been ordered by an independent court of law or the content violates human rights.

- **Name contact persons** who publicly comment on company policies in Russia and are readily accessible for queries, particularly for independent media professionals from Russia.

- **Not to store user data** on servers **in Russia** and to make such data available to the authorities only in cases justified under the rule of law.

- Describe in detailed and informative **transparency reports** how often state authorities, including Russian authorities, demanded the removal or blocking of content; how much and which content was removed or blocked; the legal justification for any content removal or blocking; how often demands for removal or blocking of content were rejected; the possible remedies available to users whose content was removed or blocked; how often users made use of these remedies; how often states, including Russia, required information on user data.

- Be **transparent about how data is collected** and used and the impact of this collection on the personalisation of content.

- Not to **participate** in the World Internet Conference in Wuzhen, China, or in initiatives of the Shanghai Cooperation Organisation which promote the idea of state cyber sovereignty and more or less separate state-controlled networks, but rather **in multi-stakeholder initiatives** such as the Internet Governance Forum or the Freedom Online Coalition, which are developing mechanisms for the regulation and self-regulation of free and democratic publics.

Reporters Without Borders (RSF) calls on Russian telephone and internet providers and online platforms to take the following steps:

- **Refuse to grant** criminal prosecution authorities and intelligence services **blanket access** to their customers' communications, but to insist on a court order for surveillance for a limited period of time in every individual case,
- Regularly publish **detailed and informative transparency reports** that state how often authorities have demanded that content be removed or blocked or that user data be turned over, and how the providers and platforms responded to these demands.

Reporters Without Borders (RSF) recommends that journalists to take the following steps:

- Be mindful of data protection and the protection of sources by using services that use **end-to-end encryption** of messages and conversations **by default** (e.g., Signal, Threema and ProtonMail) and avoid using providers that store data in Russia.

Reporters Without Borders (RSF) calls on media worldwide:

- To **publicise all cases** in which the Russian media supervisory authority censors their editorial content on social media, and to use all available legal means to counter such interference.

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

Freedom of expression and information will always be the world's most important freedom. If journalists were not free to report the facts, denounce abuses and alert the public, how would we address/tackle the problem of Child-soldiers, defend women's rights or preserve our environment?

In some countries, torturers stop their atrocious deeds as soon as they are mentioned in the media. In others, corrupt politicians abandon their illegal habits when investigative journalists publish compromising details about their activities.

Still elsewhere, massacres are prevented when the international media focuses its attention and cameras on events.

A FUNDAMENTAL HUMAN RIGHT

Freedom of information is fundamental in any democracy, but nearly half of the world's population has no access to freely reported news and information.

Freedom of expression and information is the first and most important of freedoms. How can we combat atrocities against civilians, tackle the tragedy of child soldiers, defend women's rights or defend our environment if journalists aren't free to report the facts, draw attention to abuses and appeal to the public's conscience?

There are countries where the torturers stopped torturing when the media began talking about them, and corrupt politicians abandoned shady practices when investigative journalists published compromising information.

AN INTERNATIONAL NGO

Based in Paris, Reporters Without Borders (RSF) is an independent NGO with consultative status with the United Nations, UNESCO, the Council of Europe and the International Organization of the Francophonie (OIF). Its foreign sections, its offices in ten cities, including Brussels, Washington, Berlin, Tunis, Rio de Janeiro, and Stockholm, and its network of correspondents in 130 countries give RSF the ability to mobilize support, challenge governments and wield influence both on the ground and in the ministries where media and internet standards and legislation are drafted.

30 YEARS DEFENDING FREEDOM OF INFORMATION

Founded by four journalists in the southern French city Montpellier in 1985, RSF is now one of the world's leading NGOs in the defense and promotion of freedom of information. Registered in France as a non-profit organization since 1995, RSF has distinguished itself in China, by its protests during the 2008 Beijing Olympics; in Africa, by creating the only independent radio station broadcasting to Eritreans in 2009; in Haiti, by creating a media support center after the January 2010 earthquake; and more recently in Syria, by providing training to journalists and bloggers.

REPORTS AND PRESS RELEASES IN MANY LANGUAGES

Every day, RSF issues press releases and reports in French, English, Spanish, Arabic, and Farsi (and often in other languages such as Chinese, Portuguese and Russian) about the state of freedom of information throughout the world and how it is being violated. Its statements in the international media increase public awareness and influence leaders as regards both individual cases and general issues.

LEGAL INFO

REPORTERS WITHOUT BORDERS (RSF) documents violations of press freedom and freedom of information worldwide and alerts the public when journalists or the people they work with are in danger. We campaign for improved security and protection for media representatives. Online and offline we combat censorship, the use and export of surveillance technology, and restrictive media laws.

EXECUTIVE DIRECTOR RSF GERMANY: Christian Mihr
PROJECT MANAGEMENT: Sylvie Ahrens-Urbanek | AUTHOR: Ulrike Gruska
RESEARCH & INVESTIGATIONS: Ulrike Gruska / Gemma Pörzgen
LAYOUT: Anna-Maria Roch | SUPPORT: Anna Hüsmann
Cover photo © Getty Images / Michael Bocchieri

POSTFACH 304108, 10756 BERLIN
TEL.: +49-30 60989533-0
KONTAKT@REPORTER-OHNE-GRENZEN.DE
WWW.REPORTER-OHNE-GRENZEN.DE

INTERNATIONAL SECRETARIAT
CS 90247, 75083 PARIS CEDEX 02
WWW.RSF.ORG

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION