DIGITAL AUTHORITARIANISM IN THE MAKING

Repression and Resistance on the Russian Internet

edited by
Françoise Daucé,
Benjamin Loveluck,
and Francesca Musiani

DIGITAL AUTHORITARIANISM IN THE MAKING

INFORMATION POLICY SERIES

Edited by Sandra Braman

The Information Policy series publishes research on and analysis of significant problems in the field of information policy, including decisions and practices that enable or constrain information, communication, and culture irrespective of the legal siloes in which they have traditionally been located as well as state-law-society interactions. Defining information policy as all laws, regulations, and decision-making principles that affect any form of information creation, processing, flows, and use, the series includes attention to the formal decisions, decision-making processes, and entities of government; the formal and informal decisions, decision-making processes, and entities of private and public sector agents capable of constitutive effects on the nature of society; and the cultural habits and predispositions of governmentality that support and sustain government and governance. The parametric functions of information policy at the boundaries of social, informational, and technological systems are of global importance because they provide the context for all communications, interactions, and social processes.

A complete list of the books in the Information Policy series appears at the back of this book.

DIGITAL AUTHORITARIANISM IN THE MAKING

Repression and Resistance on the Russian Internet

EDITED BY FRANÇOISE DAUCÉ, BENJAMIN LOVELUCK, AND FRANCESCA MUSIANI

The MIT Press
Cambridge, Massachusetts
London, England

The MIT Press
Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139
mitpress.mit.edu

Translated by Paco Libbrecht, with Elizabeth Carey-Libbrecht

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Adobe Garamond and Berthold Akzidenz Grotesk by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data is available.

ISBN: 978-0-262-55367-4

EU Authorised Representative: Easy Access System Europe, Mustamäe tee 50, 10621 Tallinn, Estonia | Email: gpsr.requests@easproject.com

Contents

Series Editor's Introduction

War.

There, I've said it.

In the US we can still say that word, legally. In Russia, since 2022, people cannot. *Digital Authoritarianism in the Making: Repression and Resistance on the Russian Internet* masterfully and systematically tells the story of how Putin shut down free speech and access to information, destroying the internet as a public sphere, beginning in 2011–2012. The research period funded by the grant supporting this research ended just when there was a dramatic escalation of domestic repression concurrent with the invasion of Ukraine in 2022; the concluding chapter comments on developments since that time. Among the many ways in which this book sets a model for doing research in ever-more restrictive environments is its attention to both government and resistance efforts and to policy failures as well as assertions. The book's organization by sector, such as books (libraries and book publishers) and broadcasting, means that particular policies and implementation programs can be seen from multiple directions, adding nuance in addition to ensuring that the entire range of types of restrictions is described.

These authors have humility as well as courage in the face of increasingly oppressive research and living conditions. In the new preface for this revised, updated, and expanded English language edition of *Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012–2022*, the editors note that they were pursuing the "citizen's goal" as well as the scholar's. They conclude, "This book might be, for a while, one of the last contributions gathering several original ethnographies in/about Russia, shedding

empirical light on digitally supported authoritarianism in the twenty-first century" (p. xiv).

Until fairly recently, the Russians could use the internet, which as Ben Peters tells us in *How Not to Network a Nation: The Uneasy History of the Soviet Internet*, was created through private sector efforts and, as we learn from this book, remained essentially private until Putin's efforts to control communications began in 2011–2012. There is a great deal of descriptive material available in public and scholarly literatures about repressive speech conditions, with significant contributions coming not only from journalists, bloggers, self-reports, and researchers, but also from nonprofit advocacy groups such as Reporters without Borders. Even so, this work brings us into quite new territory, for several reasons. Innovations in research methods such as working with geographers to follow communication lines when identifying research subjects, the adaptation of research methods to increasingly repressive conditions, and the multiplicity of methods used (including over a hundred interviews) make this work a methodological model that could valuably be taken up by others.

These authors are also particularly sophisticated theoretically, with multidisciplinary expertise in the analysis of sociotechnical systems and of political sociology. *Digital Authoritarianism in the Making* is conceptually as well as theoretically rich. The authors discuss "crisis" citizenship that develops when the cooperation practices people first learn during a crisis become ongoing, for example. People "digitally cross" when they leave Russia and must figure out how to operate online outside it, using Runet in exile. This is also, though, a book to be read for its details.

Security has not historically been taught in social science research methods courses beyond subject data privacy, but in some places, and in some times, it should be. Noting that the sensitivity of their work increased over time, the researchers paid constant attention to the security of their networks, data, and sources. They not only trained in digital security, but retrained in order to adapt to changing circumstances—as did the entire Russian population. It is not only that the Russian internet (Runet) is not a public sphere, *a place where people can talk* about shared matters of public concern. It is, as author Perrine Poupin puts it, that *people can't even talk at all* about such matters with each other any more. There is a concomitant inability to hear, a "public deafness"

(p. 172) that leaves only two conversational forms—"kitchen talk," among family and friends, and the formal language of government.

As sources of information for this book fled Russia to live in exile, these authors followed them for further interviews in other countries. Those participating in "Runet in exile" have more freedom of speech, but communications with those inside Russia in a manner that protects those inside the country is complex. The Russian government's attempts to make the internet a tool of government—to "sovereignize" it—don't align with geophysical or communicative borders, in another example of the tension between geopolitical and network political citizenship that has been evident since discussions among those involved in technical design of the internet in the 1970s.

As internet service provider (ISPs) prioritized caring for each other over following the law, they developed practices such as setting up dual subnetworks, one of which has the required surveillance box and the other of which does not. Broadcasters, similarly, set up a second broadcasting station that was hidden, so that news could continue to be broadcast while one station was shut down and those broadcasting were beaten. There are new organizational forms, such as the advocacy/investigative/media organization created by Alexei Navalny and relationships created between an e-book corporation and illegal "shadow libraries" to ensure sustained access to books.

The impact of the choices of other nations can be counterintuitive. Sanctions worked in favor of civil society because the government could not get all of the hardware needed to fully implement its policies, creating opportunities for those attempting to work around restrictions on speech, access to information, and internet use.

Space constraints make it impossible to call out other of the myriad discoveries of policy tools, communication work-arounds, defensive techniques, and insights into the sociotechnical systems analyzed by *Digital Authoritarianism in the Making*. Those studying the internet and society will find the book invaluable. Finally, and most fundamentally, this book should inform and inspire the resistance efforts of citizens around the world whose leaders have created or desire to create similarly repressive speech and information worlds.

Sandra Braman

Preface to the English-Language Edition

Françoise Daucé, Benjamin Loveluck, and Francesca Musiani

This book tells stories of digital coercion, of digital resistance, and of the network of actors and tools that address, counter, or foster them in Russia. It is the English translation of a book released by Presses des Mines in the French language, in mid-2023, with the title *Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012–2022*. This book was itself the result of a five-year research project funded by the French National Agency for Research, ResisTIC (*Internet Resisters. Criticism and Evasion in the Face of Digital Coercion in Russia*), conducted between 2018 and 2022. As this translated and revised version of the book sees the light in 2024—and, we hope, will find an international readership in 2025—this preface briefly seeks to introduce why the reach of this work needs, in our view, to be extended to English-speaking audiences and provides some details on what is "revised and expanded" in this English-language edition.

BRINGING THIS WORK TO ENGLISH-SPEAKING AUDIENCES

The focus of this book is how online repression and online resistances interact, and of the effects—both intended and unintended—that related practices have on Internet sovereignty, fragmentation, and freedoms. The phenomena we have examined for five years in Russia within the ResisTIC project provide further evidence of one of the core tenets of digital policy studies today, that is, that digital policy is much more capacious than laws and regulations, to include other structures of power and influence such as private ordering, technical design, and last but not least, user practice—and must be

examined through a multidisciplinary lens. Our willingness to bring this work to broader, English-speaking audiences worldwide stems from the recognition of its potential usefulness to address these core issues of information policy studies, but also of the fact that the digital facets of the Russian regime are a yet-understudied but increasingly central research subject for scholars—as well as a puzzling and deeply disquieting enigma for the citizens of the world.

With this book, we have attempted to tackle two topical issues—namely, the recent evolutions (including the digital ones) of the Russian regime and society, on the one hand, and the various and novel ways in which internet infrastructures are leveraged in order to achieve political ends, on the other.

What we consider to be one of the strongest suits of the book, and one we hope will be most useful for its readership, is the patient and detailed fieldwork that forms the basis of most of its chapters. We have sought to shed light on a set of phenomena that to our knowledge are still understudied; the book was prepared jointly by leading specialists in the political sociology of the Internet and experts in contemporary Russian politics and society. It draws on this in-depth dialogue to contribute to a better understanding of both contemporary Russia and global digital practices.

A SCHOLARLY GOAL, A "CITIZEN'S GOAL"

Of course, we hope that the book will be of theoretical and methodological interest to scholarly audiences, filling an interesting niche with its main focus on online resistance and on yet-understudied social and technical practices used to circumvent constraints. In this sense, the book is bound to spark some discussions on how to study and understand digital resistance in authoritarian regimes. Indeed, we hope that its mix of multifacetedness and multidisciplinarity may provide inspiration for scholars who seek to study similar developments in today's internet governance landscape.

We admittedly have a "citizen's goal" as well with this book: we think that any individual concerned about the future of the internet or their individual rights online, about internet fragmentation, internet sovereignty, surveillance and censorship, or the role of infrastructure and intermediaries

in constraining or promoting online civil liberties, could be interested in this book, and we hope that at least a few will indeed be. Also, the book—despite its clearly delimited recent-history span—aims at shedding light, more broadly, on the political trajectory of contemporary Russian power and in this sense can transcend its focus on the "digital." At a time when massive war is raging in Ukraine, it offers keys to understanding Russia's political trajectory, from peace to war, through the prism of digital practices.

WHAT WAS THERE, WHAT IS NEW

This is a translated work, and as such, we have made the deliberate decision not to revise the book to the point of turning it into something fundamentally "other" than its original version. However, since the end of our fieldwork in 2022, and even more so since the publication of the original book in mid-2023, so much has happened in Russia, and to the world because of Russia, that cannot be entirely set aside.

Thus, we are updating the translated version of the book with (some of) what has happened in between, making this book a "revised, updated, and expanded edition" alongside a translation. In addition to the preface you are currently reading, the English-language version includes a dedicated new conclusion that presents a synthesis of the findings of the book and acts as an overture toward current and future research on the book's themes, first and foremost on the relation between warfare and digital sovereignty. We have also made minor changes to the introduction and revised the chapters for clarity and a few factual updates where needed. All of this was done while keeping in the "translation mode": thus, no substantial revisions of the approach or of the method have been conducted, and no substantial additions to the empirical material has been made.

WHAT 2022 (AND ONWARD) HAS CHANGED IN THE FIELD, AND FOR RESEARCH

Due to funding and organizational constraints, the fieldwork subtending this book concluded in early 2022, just as the world was about to be stunned

and horrified by Russia's massive invasion of Ukraine. Thus, the different stories of coercion and circumvention told by this book still belong, in some way, to a "pre–full scale war" phase in Russia's construction of its own authoritarianism and coercive strategies—a phase when the Putin regime was still displaying a formal, albeit de facto already empty, appearance of democracy to the outside world, while strengthening internally (and often opaquely) its authoritarian grip. Yet all these stories, especially if drawn together, help shed light on the set of preconditions that have, eventually, made the massive invasion of Ukraine possible—and on the sociopolitical, economic, and technical premises of the Putin regime's "crossing the next line" into authoritarianism. In this light, it is our hope that this work, regardless of (and perhaps because of) the precise time span it addresses, will see its value remaining intact across the years, as it offers a varied analysis of a set of primary historical documents and has the potential to be leveraged as a methodological model.

One last point needs to be made on the conditions in which research could, can now, or can no longer, be conducted in today's Russia. While—most importantly and dramatically—the life of Ukrainians in the field has drastically changed with the February 2022 invasion, the work of researchers attempting to study these transformations has changed in depth as well. Notably, it is no longer possible to physically go to Russia or Ukraine on fieldwork missions, and a set of new constraints and precautions is needed to attempt interacting with on-site actors, even those with whom we had previous, and carefully nurtured, established collaborations. Thus, this book might be, for a while, one of the last contributions gathering several original ethnographies in/about Russia, shedding empirical light on digitally supported authoritarianism in the twenty-first century.

It is knowing all this—humbled as scholars by the tasks facing research today, and profoundly worried as citizens by the political context that frames and fuels this research—that we propose this book to you. We hope that you will find it of interest.

Paris, July 2024
The book coeditors

NOTE ON THE AVAILABILITY OF SOURCES

As this field of study evolves, so does the status of several of our online sources. In this book, we would like to acknowledge two issues that are particularly relevant to us from a research point of view as well as a readership point of view:

1. Links to many official websites (generally from the Russian government or its governmental agencies) are not accessible from outside Russia without the use of a virtual private network (VPN). However, the URLs we have provided remain valid.
2. Several media outlets have either closed or been taken down, resulting in two configurations. Some websites are no longer accessible at all. In such instances, we have provided the original URL with a "last accessed" date. Wherever possible, we have also provided an alternative URL via the Internet Archive Wayback Machine.

   We have also acknowledged these issues at each endnote where a URL is cited.

Acknowledgments

We would first and foremost like to thank all the free-internet activists who, despite the risks, agreed to answer our many questions, invited us to attend their meetings, and opened the doors of their cryptofests, privacy days, and other hackathons organized in Russia. Activists from the NGOs Roskomsvoboda, Obshchestvo Zashchity Interneta (Internet Protection Society [OZI]) and Teplitsa Sotsial'nykh Tekhnologi (Social Technologies Greenhouse) were exceptional in the way they shared their technical know-how during this investigation in difficult environments, first in Russia and then in the foreign countries where they found a safe harbor (Latvia, Lithuania, Georgia, etc.).

We also have a debt of gratitude toward the professionals of the public sphere (journalists, bloggers, editors, activists, political actors) and of the internet (*ITichniki*, technicians, developers, access providers, trainers) who testified on the evolution of their working conditions in an increasingly oppressive digital environment. The research presented here was informed by interviews with journalists from numerous media outlets (Grani, Lenta, Gazeta, *Kommersant*, *RBK*, *Ekho Moskvy*, *Novaya Gazeta*, Mediazona, Meduza, Radio Svoboda, Proekt, Takie Dela, The Insider, Arzamas) and editors from several publishing houses. Discussions with activists from the Anti-Corruption Foundation (FBK), founded by the late Aleksei Navalny, were especially enriching.

This list would be incomplete if we failed to thank all the citizens who, in various circumstances, have informed us about their daily or activist digital practices, whether in Moscow, St. Petersburg, or the north of Russia. In the

current context we unfortunately cannot mention their names, as that would add to the danger they face politically, within or outside Russia.

We also owe a great deal to all our colleagues who are conducting research on contemporary digital reconfigurations, whether in authoritarian or democratic contexts. Their contributions during the bimonthly seminars we organized from 2018 to 2021 at the EHESS (School of Advanced Studies in the Social Sciences) in Paris were particularly stimulating as they provided us with shared reference points and advanced our collective work.

This book is the result of research carried out with the support of the French Agence Nationale de la Recherche (ANR) as well as our respective research centers that supported this joint project (Centre for Russian, Caucasian, East European and Central Asian Studies/CERCEC, Centre Internet et Société, i3-Télécom Paris, ILCEA4, and Eur'Orbem). We thank them for their support. We extend our warmest gratitude to Fabrice Demarthon, Thomas da Silva, Marianne Rahmé, and Timofey Balin, who helped us in the various stages of this project.

We thank Silvia Dekorsy and Sandra Rodrigues of Presses des Mines for their kind assistance through the publication process of the original French-language book and for keeping the possibility of an English-language version open. Finally, we wish to warmly thank Paco Libbrecht and Elizabeth Carey-Libbrecht for their high-quality translation, as well as Gita Manaktala and Sandra Braman, respectively, executive editor at-large and Information Policy series editor at the MIT Press, for their kind help and guidance throughout the editorial process.

INTRODUCTION

Françoise Daucé, Benjamin Loveluck, and Francesca Musiani

On February 24, 2022, as the military offensive against Ukraine unfolded, media censorship along with the monitoring and blocking of the internet immediately intensified in Russia. The enlistment of the internet in the service of the Russian state's warmongering suddenly accelerated and allowed the authorities to subdue the public sphere into wartime compliance. The war justified a brutal tightening of the network of restrictions and constraints that were already weighing down on digital infrastructures and actors. Amendments to the legal framework made it even more restrictive, so that any criticism of the army or mention of the term "war" became prohibited (replaced by the official, Orwellian terminology of "special military operation"). This censorship caused many media outlets to cancel potential publications. Criminal cases were opened against independent journalists and opponents of the war, while the Ministry of Justice's register of "foreign agents" grew considerably. The Russian government also blocked international social media platforms (Facebook, Instagram, X/Twitter, and, in 2024, Signal and YouTube) and tightened its control over local actors of the digital industry (VKontakte, Yandex). These decisions came as sanctions prompted many foreign digital operators to leave the country and to disconnect their infrastructures from the Russian network.

How did this authoritarian dynamic come to be in a digital space that was initially free? Compared to China, in particular, where the state has strongly controlled the development of digital information technology from the outset, Russia's trajectory has been singular. Its first steps into connected computing for the general public, in the 2000s, were characterized by intense

entrepreneurial activity, numerous local operators throughout the country, and a very rapid internet penetration rate,[1] in a context of relative laissez-faire. This book seeks to provide insight into the policies restricting the Russian internet, resituating them within their historical context starting in the early 2010s. It also offers a political sociology of the Russian digital space, looking at the actors who have embraced it in order to assert their rights and make their voices heard: access providers, developers, journalists, activists, web professionals and mobilized citizens. The web[2] in Russia was spawned by digital inventors' plural and decentralized initiatives and for many years carried hopes for the democratization of the Russian public sphere. How, then, did state control consolidate its grip on it, adjusting to its particularities and to its defenders' inventiveness over time?

AUTHORITARIANISM AND THE DIGITAL SPHERE

The turn taken by the Russian political regime—starting even before the full-scale war in Ukraine, but especially since then—has revived debates about how best to describe it. As Sergei Guriev and Daniel Treisman (2022) point out, the notion of authoritarianism may seem outdated here. They argue that fear has been superseded by communication, using the concept of "spin dictators" to describe political regimes that rely on manipulating the public debate and simulating democratic mechanisms rather than direct violence. On the other hand, in view of the destruction perpetrated by the Russian army in Ukraine from February 2022 onward and the attendant brutal domestic repression, the notion of authoritarianism may seem to pale, and some observers no longer hesitate to squarely describe the Russian regime as fascist. This is the position of intellectuals like Alexander Motyl (from 2016) and Timothy Snyder (2022), who believe that fascism can be defined here as a popular authoritarian system based on a personal dictatorship and the cult of the leader, as well as the cult of the dead and the myth of a golden age in the imperial past. Others, such as Marlène Laruelle (2021 and 2022), disagree. Laruelle argues that the Russian regime is not fascist because its power does not rely on mobilization of the masses but instead takes advantage of the fragmentation of society. The imperialist dynamic was

nevertheless openly reactivated and focused on Ukraine since the intervention in the Donbass and the annexation of Crimea in 2014.

As David Lewis (2020) points out, Russia has long been presented as a "hybrid regime" that combines elements inherited from an autocratic and totalitarian past (persecution of dissidents, media censorship, elites that are above the law) with features of the international liberal order (integration into the global economy, penetration of liberal norms, adoption of new technologies). Yet Lewis contends that Putinism is rooted primarily in a Schmittian paradigm, with the emergence of a specific form of "illiberal democracy," where legal norms can be violated by the powers that be in the interests of maintaining "order." This well-known postulate establishes a division between friend and foe, where in this case the Russian population is constantly presented as being under threat from critics and minorities, identified as a "fifth column" working for foreign powers and aiming to undermine both Russian "traditional values" and state security. For more than a decade, this distinction has been growing and has served to cast an ever-widening veil of suspicion over all dissenting voices—especially independent journalists, human rights activists, and political opponents.

The fact that the established forms of public expression—the mainstream media especially, but also physical demonstrations—have been the primary targets of government repression since Vladimir Putin's first election twenty-five years ago, is well documented. In this context, the digital space seemed to offer more promising opportunities for all those who sought to find plural information, to express themselves, and to organize—although they had to come up with technical contrivances and take digital detours to do so. They have been helped by many other, less visible actors: computer scientists, developers, network technicians, and web professionals who have constantly invented new ways of getting around both legal hurdles and technical constraints. While some of these actors were primarily concerned with protecting their economic activity, many became politicized in the face of frustrations, obstacles, and intimidation.

These dissenting voices, as well as their many digital mouthpieces, along with their know-how and tools, are the core subject of this book. We have sought to grasp both the constraints on information and communication

in Russia, and the ways in which the actors on the ground seek to break free from them. Irrespective of their technical background and degree of political commitment, "digital rights" have become a palpable issue for all of them. They have had to deal with increasingly complex and deliberately ambivalent legislation, allowing the authorities to implement a form of arbitrariness designed to intimidate users and impose self-censorship online—just as they do in physical space. This has gone hand in hand with technological mechanisms automating publication censorship and the surveillance of personal communication.

Our inquiry into the digital world also enables us to step away from the dialectic of the leader's personal dictatorship against a fragmented people, as it affords an opportunity to think of oppression as a network (Lokot 2020). The war has facilitated the tightening of the Web's many nodes to jeopardize the digital and physical integrity of dissenting citizens. The multiple intersecting constraints spread across the digital space are articulated at various scales and in various places to serve the Russian state's bellicose and imperialist project. Instead of the "vertical of power" or the "horizontal of submission," constraint is here established through the articulation between digital systems and the security apparatus. It plays out in the intermediate spaces of proximity surveillance, the autonomy of local services, arbitrary interpretations of the law, economic incentives to obey, neighbors watching, and so on. Beyond the Russian Federation, this oppressive web is gradually extending to territories and war zones under the domination of the Russian state (inter alia, Crimea and other occupied areas in Ukraine and the dominated territories of Transnistria, Abkhazia, and Ossetia). For those who denounce oppression, the spaces of discreet compromises and freedom are narrowing by the day. Since the beginning of the war, many activists, journalists, and citizens opposing it have been forced to leave Russia to recover their physical and digital integrity abroad. In exile, they have been crossing paths with the millions of Ukrainian citizens who were driven out by the military aggression against their country.

Throughout the world, the development of new information and communication technologies was initially heralded as "liberation technologies" (Diamond 2010), raising hopes of a transition to "internet democracy" (Cardon 2010). These hopes culminated in the "Arab revolutions," in which

digital communication was widely presented as a vector of democratization (Howard and Hussain 2013). The internet has also long been seen as the embodiment of the liberal values of individual autonomy, transparency, openness, and distributed collective organization, with the network model standing in opposition to hierarchical and state-centric paradigms (Loveluck 2015a, 2015b). In stark contrast, deep concerns and disappointment have now set in, in the face of the many threats associated with digital communications—personal data collection and exploitation, surveillance capitalism, the manipulation and destabilization of democratic processes, and so on—as well as a more general reassertion of the state's prerogatives in its governance (Tréguer 2019; Haggart et al. 2021).

Some studies had already dampened the prevailing optimism by showing that autocratic regimes could quite easily accommodate the internet and even use it to serve their own ends (Kalathil and Boas 2003; Boas 2006; Morozov 2011). But it is only more recently, as democracies have faltered globally (Diamond et al. 2016; Waldner and Lust 2018), that the notion of "digital authoritarianism" has emerged to describe the use of information technologies by authoritarian regimes to monitor, oppress, and manipulate societies (Glasius and Michaelsen 2018). Repressive powers seeking to interfere directly with information and communication flows through censorship, arbitrary surveillance, and disinformation are nothing new. However, to exercise control over these new spaces of information, expression, and mobilization—and access new opportunities for repression—they must adapt to their particularities, secure resources, and develop skills (Keremoğlu and Weidmann 2020; Feldstein 2021). Social media platforms, for example, which were once the symbol of digital technologies' emancipatory power, now look far more ambivalent. This is not only because of their own excesses (regarding hate speech, content moderation policies, algorithmic biases, personal data harvesting, etc.) but also because they are vulnerable to forms of co-optation and manipulation that can reinforce autocratic powers' stranglehold on their populations (Gunitsky 2015; Deibert 2019).

China stands out as the most accomplished example of digital authoritarianism. Its state services interfere within infrastructure and services, access is filtered, sophisticated automated censorship mechanisms are deployed, considerable technical and human resources are invested in manipulating

discourse and opinion (*wǔmáo dǎng*, the 50 Cent Party), and surveillance and repression are highly effective (Han 2018; Roberts 2018; Liang et al. 2018). However, the notion of digital authoritarianism has also been used to describe repressive uses of the internet in the Middle East (Jones 2022), Pakistan (Jamil 2021), or Zimbabwe (Mare 2020). Furthermore, some elements of digital authoritarianism are sometimes also apparent in liberal democracies, with mass surveillance practices or cases of censorship (Hintz and Milan 2018), as well as private companies being authorized to sell technical filtering and surveillance solutions to human rights violators[3].

Digital authoritarianism in Russia could initially be described as *low-tech* and *low-cost*, as it did not rely on extensive automated filtering capabilities (Morgus 2018; Lamensch 2021). Instead, it appeared to rely on the instrumentalization of the law, self-censorship, and the intimidation of internet and telephone service providers, private companies, and civil society (Polyakova and Meserole 2019). This did not make it any less effective, however. Compared to the Chinese model, the Russian government's control of the internet has developed in a more reactive and ad hoc manner but is also more decentralized and flexible, and less costly (Howells and Henry 2021). Its methods could well serve as a blueprint for other countries in the future.

THE RUSSIAN INTERNET'S COERCIVE MESH

Unlike the Chinese internet, which included filtering from the outset through its *Great Firewall*, the Russian internet developed freely at first, at many public or private actors' initiative, whether they had technical training or were simply citizens experimenting with and inventing digital tools for their own uses. In the 1990s, after the end of the USSR, the country went through a period of abrupt economic deregulation, which severely affected the population's standard of living but gave free rein to the first Russian internet innovators (local internet providers, computer importers, the first online publishers, etc.). At the time, the political context remained favorable to international collaboration, with free circulation of people and digital goods. Russia was already at war (against its own parliament in 1993 and

against Chechnya in 1994 and again in 1999), but the public media space was poorly regulated and left prey to the excesses of the oligarchic groups that owned the main news media. In contrast, the digital space bore the promise of a virtuous democratization able to escape the games of power and money and based on citizens' horizontal participation.

The digital-political paradox of "half-freedom of speech" (Gelman 2010) was a salient feature of the first decade of the century, after the election of Vladimir Putin to the Russian presidency in 2000. A free internet was rapidly developing, on the one hand, and on the other, vertical and authoritarian political governance was being reinforced. In the early 2000s, the development of the Russian web and its openness to the world raised hopes for democratization and offline mobilization (Gladarev and Lonkila 2012; Etling et al., 2010). The large protest movement against fraud in the parliamentary elections and V. Putin's return to the presidential office (after a game of musical chairs with his former prime minister, Dmitry Medvedev) in the winter of 2011–2012 was a turning point. It showed the web's civic potential, allowing protesters to coordinate their actions, spread their slogans, and structure the movement. It benefited from the development of mobile social media applications, both foreign (LiveJournal, Facebook, Twitter) and domestic (Odnoklassniki, VKontakte).

At the time, the Runet (to be understood as the Russian-speaking internet) was open to the world. Its plasticity allowed it to reach beyond national borders. It was used by citizens throughout the country and by Russian-speaking populations living outside the country's borders (citizens of ex-Soviet states that had become independent, students and expatriates living in Europe or North America, and travelers moving around the world). In distant lands, the Runet connected the Russian diaspora, especially in the US, Israel, and Europe (Fialkova and Yelenevskaya 2005; Morgunova 2012). The richness and quality of its digital content highlighted the diversity of the ideas, projects, and groups that fed it, from the most conservative to the most revolutionary. Yet the very notion of a Runet reflects a gradual retreat into a national imagined community imposed by the ruling elites (Asmolov and Kolozaridi 2017). By addressing all audiences in the "Russian world," the Runet became one among many tools of the Russian authorities'

national and imperial political project in its near and distant foreign lands, even a tool of "cyber imperialism" (Uffelmann 2014). Beyond the Runet and Russian-speaking audiences, the foreign language programs of RT or Sputnik (Audinet 2021) also bear witness to the Russian state's media expansionism, supported by digital tools.

In the early 2010s, increasingly stringent government regulations started undermining online freedoms (Oates 2013; Konradova and Schmidt 2014; Soldatov and Borogan 2015). Russian legislation became more heavy-handed, illustrating the government's will to establish national control within a digital arena that had hitherto eluded it. V. Putin's reelection for a third term in 2012 and then for a fourth in 2018 came with a turn to hard-line politics that was proportional to the head of state's loss of democratic legitimacy. The government's project of "sovereign democracy" stripped the country's institutions—be it the parliament, regional authorities, political parties, or elections themselves—of their substance. Citizens were either encouraged to join in with the authorities' patriotic and reactionary discourse or were marginalized to the fringes of the public sphere to express their discontent or criticism. In this context, the digital space became the main place to articulate alternatives, in all their diversity.

National policies regulating the web expose the coercive ways in which the authorities have chosen to respond to the internet's perceived challenges to Russian sovereignty. This policy of bringing the Runet into line, which has relied especially on a legal arsenal designed to serve the goals of the rulers, has been well documented (Nocetti 2015; Stadnik 2021). Roskomnadzor (RKN), the federal government's communications control agency established in 2008, saw its jurisdiction and scope rapidly expand into areas as diverse as the control of online content, a right to block websites, and the registration of blocked sites on blacklists, with possibilities for significantly increased censorship. This control is based on its extensive network of relations and collaboration with all state security institutions at all levels of federal and regional power. The Ministry of the Interior (MVD), the Federal Security Service (FSB), the judicial institutions, the State Prosecutor's Office, and the various control agencies (health, consumer affairs, youth, tax, etc.) constitute the regalian weave that is meshed through society and relays

directives from the head of the state downward. It can also be supported, at a local level, by conservative associations of citizens who mobilize to maintain order, both online and offline (cyberpatrols, vigilante movements, "patriots," Cossacks—see Daucé et al., 2019).

In the digital space, control and authoritarian governance are exercised above all through the actors who maintain and operate the internet and who offer users connectivity solutions: telecommunication operators, internet service providers, website hosts, search engines, social networking platforms, digital service companies, developers and technicians, algorithm designers, and so on (DeNardis 2012, 2014). New legal and technical constraints are constantly being imposed on them. In the case of censorship, for example, the aim is to force these intermediaries to implement policies the authorities wish to see enforced by holding them accountable in the event of infringements. This approach, known as *intermediary liability* (MacKinnon et al. 2014), is not unique to Russia and has even become widespread in the context of content moderation on platforms (Gillespie 2018). Unlike other countries, however, the Russian legal context is unsteady and easily instrumentalized, leaves little room for checks and balances (constitutional controls), and has few possibilities for appeal (although they do exist). Users themselves can also be easily and directly incriminated, especially on social media platforms such as X/Twitter, Facebook and VKontakte, due to laws setting criminal sentences for mere reposts or *likes* on online publications (Van der Vet 2020).

In recent years, the Russian authorities have sought to better regulate their services by actively moving toward empowering and "sovereignizing" the Runet. This was achieved through the adoption of new laws aimed at countering the influence of foreign companies, better controlling data exchanges with the outside world, and isolating the Russian network in case of "threats." This trend is exemplified by the so-called sovereign internet law, passed in 2019 with the official aim of protecting the country from cyberattacks (Musiani et al. 2019), and the "anti-Apple" law, passed in 2020 to force manufacturers to preinstall "Russian-made" apps on smartphones. Perhaps in anticipation of the fractures that Russian expansionism would inevitably cause, the move to sovereignize the Russian internet includes increased control over interconnections to other countries and the

possibility of isolating the Russian segment from the rest of the internet. It has also seen more advanced automated filtering systems among operators and access providers—namely, packet inspection systems known as TSPUs, or "technical means for countering threats," which can block or throttle traffic by targeting specific protocols, services, or addresses. This desire to make digital borders match geographical ones has gone hand in hand with an increase in network centralization and operator concentration (Limonier 2021). With the accumulation of legal, technical, and economic constraints, the initially widely diverse and relatively independent actors of the Russian internet found themselves enrolled, by will or by force, in the birth of digital authoritarianism and expansionism.

Yet this control policy should not necessarily be understood as being perfectly vertical, coherent, and hierarchical. The laws that apply to online activities are numerous, varied, and constantly changing. Whereas they initially focused on terrorism, child pornography, or suicide prevention, they then turned to "extremist" activities or calls to demonstrate and rapidly saw their perimeter widen while remaining vaguely defined. Their application is often random or arbitrary. Upon close examination of the legislation and its application, what appears is not a centralized domination over the internet but, rather, a multiplicity of partial, fluctuating, and sometimes contradictory types of control. While regulations can be adjusted in various ways to the technical apparatuses (algorithms) or economic characteristics (profiling) of online activity, they always remain imperfect, leaving some latitude for technically agile digital dissidents. At times public authorities even fail at implementing their own repressive internet policy, as evidenced in 2018 by their inability to block the Telegram application within their borders (Ermoshina and Musiani 2021).

FORMS AND LIMITS OF DIGITAL RESISTANCE

Appreciating the diversity of the constraints that apply to the Russian Web and internet is essential to gain an understanding of the many forms of resistance, evasion, and circumvention that have developed as a response. In the 2000s, when the Russian internet was being built, potential technical

restrictions mostly remained invisible to its users (Deibert and Rohozinski 2010). Since the 2010s, the development of citizen activism (Clément et al. 2010) or the large demonstrations against election fraud in 2011 and 2012 (Gabowitsch 2017) have been met with growing repression—which has also triggered the emergence of critical knowledge about the uses of the internet. Activist initiatives and skills have developed, sometimes with the help of digital safety trainers (Bronnikova and Zaytseva 2021), and have contributed to the dissemination of alternative knowledge throughout society to circumvent the barriers that arise online. Opposition activists and independent journalists have learned to harvest open or leaked data to conduct their investigations and expose the corruption of the elites. Discontented citizens have created chat loops on secure applications (Telegram, Signal) to coordinate their actions. Since the early 2010s, technical operators, defenders of internet freedoms, activists, journalists, and ordinary citizens alike have increasingly come up against the state's oppressive turn and the many tightening constraints it has set up on the Russian internet. They have in turn developed critiques and workarounds that, through their heterodox digital practices, constantly challenge the codes of authoritarianism.

This book presents a sociology of the Russian internet based on fieldwork conducted between 2018 and 2022 among movements, organizations, and mobilized citizens who constitute an engaged public in the face of attacks on digital freedoms. It focuses on the multiple digital objects and services that have been at the heart of political controversies and tensions around usage in the Russian online space. It shows the processes through which digital oppression is constructed, by paying close attention to the unfolding forms of criticism, conflict, and circumvention that oppose public and private actors, online supporters of order, and defenders of online freedoms. Academic work on "disobedience" and "resistance" to domination abounds in the fields of history, political science, and sociology. It has shown that institutional order cannot be imposed without some arrangement in the distribution of prescribed roles (Hmed and Laurens 2011). While it is often difficult to identify a coherent and organized expression of resistance, researchers have shown how it can take the form of everyday practices and skills or "*arts de faire*" (de Certeau 1990) through low-intensity, inconspicuous, or

underground actions that belong to the category of "infra-politics" (Scott 2009) or through such practices as avoidance, circumvention, and hacking (Keucheyan and Tessier 2008).

On the internet, new forms of online protest have developed against network surveillance policies throughout the world (Best and Krueger 2008; MacKinnon 2012). Some of these may involve visible public voices and conspicuous "media-activism" (Cardon and Granjon 2013), while others rely on anonymity and obfuscation (Brunton and Nissenbaum 2015). In Russia, efforts to transform the digital landscape include a multiplicity of low-key individual actions, but also some high-profile initiatives that butt heads with the authorities, as illustrated by the trajectory of the cofounder of VKontakte, Pavel Durov. A self-proclaimed libertarian, Durov ran the Facebook-like social network until 2014, before leaving the country under growing pressure to provide intelligence services access to the service. In the meantime, he had founded the Telegram messaging and publication app, which by virtue of its technical particularities, extra-territoriality and lack of cooperation with authorities, has boasted greater resistance to state interventionism, as illustrated by the failed attempt to block it in 2018 (Maréchal 2018; Wijermars and Lokot 2022). Telegram remains one of the few spaces where opposition media can still be accessed in Russia, although the platform has also become one of the main channels for disseminating prowar discourses and anti-Western propaganda. Moreover, the platform has also raised concerns outside Russia for its lack of moderation and failure to answer law enforcement requests for information even for serious offences, as demonstrated by the police custody of Durov in Paris in August 2024 and the criminal investigation that has been launched against him. Ironically, Russian officials seized the opportunity to decry France's alleged assault on freedom of speech and offered the Telegram CEO their support.

In other public confrontations with the authorities, models derived from offline movements and those shaped by networked technologies coexist and become hybrid in nature. For example, in September 2021, during the parliamentary elections, Aleksei Navalny's Anti-Corruption Foundation (FBK) movement offered voters a "smart voting" application that allowed them to identify, in each district, the candidate most likely to beat the representative of the presidential party, United Russia. It fought a fierce technical battle for

the application's survival, which even resulted in an unprecedented injunction made to Google and Apple to remove it from their app stores.[4] Their representatives were threatened with criminal prosecution and, Google's offices were raided by armed bailiffs. Thus, to understand online resistance, it is also important to take into account its technical aspects, hardware, and software—the constantly evolving infrastructure that drives the internet, holds it together or fragments it, and is the site of intense governance battles (DeNardis, 2014).

These kinds of resistance dynamics can be observed in Russia, even though the overall picture is skewed by the increasing weight of authoritarian rule in the country, especially since the outbreak of the full-scale war against Ukraine. Several of the investigations presented in this book take a close look at the infrastructures, technical devices, and interfaces involved in surveillance and censorship, such as internet traffic–filtering devices, news classification algorithms, and surveillance cameras. While these tools of control are often invisible to users, they are exposed by activists and citizens who are confronted with their repressive use. The conflicts surrounding the development of these technologies and their uses show that resistance and circumvention strategies also exist "through the infrastructure" (Daucé and Musiani 2021) as, in the face of the Russian government's expanding grip, direct political confrontation has become increasingly difficult and dangerous.

In addition, various behaviors, which can be considered techno-legal tricks or resistance through practices and uses, have emerged in response to the evolution of the legal framework, whereby Russian "digital resisters" defy the legislator. The fieldwork has helped shed light on individuals and groups, activists or "simple" citizens who are aware of the digital challenges facing public freedoms and engage in advocacy (criticizing laws, drafting alternative regulations), defend repressed users (hiring specialized lawyers, providing support for prosecuted activists), raise awareness of digital security (through trainings, webinars), or simply exploit regulatory loopholes. However, they operate in a context of uncertainty, and their strategies should not necessarily be interpreted as following a coherent and sustainable model.

While many forms of disobedience, circumvention, hacking, or obfuscation are common in the Russian digital space, their rise to political prominence is generally impeded. Among the skilled users who know how to access blocked websites through virtual private networks (VPNs), protect

their private correspondence through encryption, secure their computers through double authentication, and use mirror sites to deceive the censors, few claim to be politically involved in the public sphere. On the contrary, most of them say they "don't do politics." In the face of authoritarian restrictions, the process of avoiding politics is plain to see. A good example of this is the Russian Pirate Party, which founded the publicly "nonpolitical" NGO Roskomsvoboda[5] in 2012 to continue legally defending internet freedom in Russia (Daucé 2022).

Euphemisms and circumvention are the order of the day to access the free internet without arousing the attention of censors or security services. Not all circumvention tools and practices are designed to facilitate access to political content; they also allow users to consume cultural goods such as music, films, or books without paying. One may sometimes wonder whether they do not actually contribute to the acceptability of censorship and to the weakening of the feeling of revolt against attacks on fundamental freedoms. Those who attempt dissent and resistance—whether it be Aleksei Navalny's FBK, the Internet Protection Society (OZI) (Klimarev 2022), or the citizens who mobilized to defend the environment in Shiyes, in the far north (Poupin 2022)—have to face multiple attacks from the authorities. Aleksei Navalny has paid a terrible price: after being harassed for many years, he was first poisoned by the security services in 2020 and then imprisoned in 2021, before meeting his death in custody in early 2024, at the age of forty-seven. Many of his supporters have been forced into exile to escape criminal prosecution. From abroad, they may attempt to renew their political ties and use digital tools to oppose the current Russian government. For those mobilized citizens who remain in Russia, the struggle is harsh; they are under constant threat of online and offline repression.

PRESENTATION AND STRUCTURE OF THE BOOK

This book is informed by fieldwork conducted within a collaborative project funded by the French National Research Agency (ANR).[6] For five years, the project team studied how different actors of the Russian internet adapt to authoritarian and centralizing regulations and how they resist them. It

focused mainly on online resistance and lesser-known social and technical practices used to circumvent constraints.

The book offers a detailed overview of the various studies carried out at the interface of social and political mobilization, digital sovereignty, legal structures, data, and infrastructure—showing how these different dimensions have interacted and evolved, as well as the often very creative and sometimes subversive uses and practices that have developed in their midst. It offers an analysis of the transformations the Russian internet has undergone, from the perspective of different disciplines (sociology, political science, law, and anthropology), actors (NGOs, private companies, public administrations, media, publishers, activists), and objects (cables, platforms, algorithms, data, social networks, posts, blogs, chats, etc.). Over the course of the project, a timeline was also set up that lists the numerous (and sometimes contradictory) events that have defined recent developments in the Russian digital space (with no claims to being fully exhaustive, however). Documenting the oppressive constraints and critiques in defense of digital freedoms that unfolded throughout the 2010s, up until the large-scale Russian invasion of Ukraine in February 2022, it comes as a complement to this book and is available in open access (https://timeline.resistic.fr/).

The analyses presented in the following chapters are based on original quantitative and qualitative data. Close to a hundred interviews were conducted, along with many participant observations, online ethnographies, and digital data collections. In addition to the case studies themselves, a recurring point of attention was to reflexively evaluate the survey methods, especially with respect to certain respondents' vulnerable situations. Engaging in fieldwork in Russia was challenging, as researchers needed to be mindful not to put respondents in a difficult or even dangerous position. The sensitive nature of our investigations only increased over the years, culminating with the profound upheavals from February 2022 onward. Throughout the research, constant attention was paid to the reliability of the communication networks used, to the security of the collected data, and to the protection of archived sources. The members of the project team themselves underwent training in digital security to adjust to the constantly changing context of the investigation. This collective experience has shown

that digital security, beyond any normative and protocol-based vision of it, is primarily the result of ongoing dialogue with stakeholders to collectively negotiate rules for shared safety.

This book first presents the normative and legal framework that governs the Russian internet and that has grown over the years, at the cost of an inflation of rules regulating multiple aspects of digital activities, from the most material (cables) to the most volatile (data) (chapter 1). The analysis then develops from two observation points allowing readers to gain an understanding of digital authoritarianism in action: the content-filtering and traffic-monitoring devices imposed on Internet Service Providers (chapter 2) and news classification algorithms such as that of Yandex (chapter 3).

In the face of these constraints, knowledge is emerging about how to protect oneself from surveillance and controls on the Runet, with one notable case being training provided by digital security specialists to critical activists (chapter 4). Journalists are learning how to work with digital data to conduct their investigations as controls on the media tighten (chapter 5). Publishers and booksellers, for their part, are discovering both the constraints and the opportunities of online book distribution in the face of the political uses of the fight against piracy (chapter 6). These experiences underpin trajectories of learning in which stakeholders gradually move away from technological determinism to reconnect with the subtleties of socially situated knowledge.

In this environment of intersecting constraints and freedoms, critical activists and mobilized citizens are confronted with complex digital challenges, leading them to choose digital tools and practices tailored to their commitments (chapter 7). When digital risks threaten people's physical security, particularly in the wake of Russia's military aggression against Ukraine, only exile allows them to regain physical and digital integrity, which can give rise to new activist commitments from abroad (chapter 8).

NOTES

1. Data from the International Telecommunication Union show that it grew from 15 percent to almost 60 percent between 2005 and 2011 (https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU).

2. We should emphasize the difference between the "internet" and the "web," which are too often used interchangeably in common parlance. The internet is the global system of

interconnected computer networks that use a "common language"—the internet protocol suite—to communicate with one another. The web, or World Wide Web (WWW), is a particular set of applications built on top of the internet, one of the most widely used by end users (along with file sharing and email applications, for example).

3. As did the French companies Amesys and Nexa to Egypt and Libya (Tesquet 2020), and the Israeli company NSO to numerous actors such as the Saudi regime and Mexican drug cartels (Marczak et al. 2018).

4. Anton Troianovski and Adam Satariano, "Google and Apple, under Pressure from Russia, Remove Voting App," *New York Times*, September 17, 2021, https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html.

5. The name of this association is an ironic twist on the name of the Communications Monitoring Agency (Roskomnadzor), which has been changed to the Communications Freedom Agency (Roskomsvoboda).

6. ANR Projet ResisTIC (Internet Resisters. Criticism and Evasion in the Face of Digital Coercion in Russia, 2018–2022), https://www.resistic.fr/.

REFERENCES

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

Audinet, Maxime. 2021. *Russia Today (RT). Un média d'influence au service de l'Etat russe*, INA.

Best, Samuel J., and Brian S. Krueger. 2008. "Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search terms." *Journal of Information Technology and Politics* 5 (2): 191–212.

Boas, Taylor C. 2006. "Weaving the Authoritarian Web. The Control of Internet Use in Nondemocratic Regimes." In *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology*, edited by John Zysman and Abraham Newman. Stanford University Press.

Bronnikova, Olga, and Anna Zaytseva. 2021. "'In Google We Trust'? The Internet Giant as a Subject of Contention and Appropriation for the Russian State and Civil Society." *First Monday* 26 (5).

Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation. A User's Guide for Privacy and Protest*. MIT Press.

Cardon, Dominique. 2010. *La Démocratie Internet. Promesses et limites*. Seuil.

Cardon, Dominique, and Fabien Granjon. 2010. *Médiactivistes*. Presses de Sciences Po.

Clément, Karine, Olga Miriasova, and Andrei Demidov. 2010. *Ot obyvatelei k aktivistam: zarožd*aûšiesiâ *sotsial'nye dviženia v sovremennoj Rossii*. Tri Kvadrata.

Daucé, Françoise. 2022. "Pirater l'autoritarisme. Trajectoires de lutte pour les libertés numériques dans la Russie de V. Poutine (2009–2022)." *Terminal* (134–135).

Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. 2019. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia." *Laboratorium* 11 (3): 46–70.

Daucé, Françoise, and Francesca Musiani, eds. 2021. "Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet: An Introduction." *First Monday* 26 (5).

de Certeau, Michel. 1990. *L'Invention du quotidien* (Vol. 1). Gallimard.

Deibert, Ronald J. 2019. "The Road to Digital Unfreedom: Three Painful Truths about Social Media." *Journal of Democracy* 30 (1): 25–39.

Deibert, Ronald J., and Rafal Rohozinski. 2010. "Control and Subversion in Russian Cyberspace." In *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, edited by Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. MIT Press.

DeNardis, Laura. 2012. "Hidden Levers of Internet Control. An Infrastructure-Based Theory of Internet Governance." *Information, Communication and Society* 15 (5): 720–738.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. Yale University Press.

Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21 (3): 69–83.

Diamond, Larry, Marc F. Plattner, and Christopher Walker, eds. 2016. *Authoritarianism Goes Global. The Challenge to Democracy*. Johns Hopkins University Press.

Ermoshina, Ksenia, and Francesca Musiani. 2021. "The Telegram Ban: How Censorship 'Made in Russia' Faces a Global Internet." *First Monday* 26 (5).

Etling, Bruce, Karina Alexanyan, John Kelly, Robert Faris, John Palfrey, and Urs Gasser. 2010. "Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization." Berkman Center Research Publication no. 2010–11, Harvard. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere_2010.pdf.

Feldstein, Steven. 2021. *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*. Oxford University Press.

Fialkova, Larisa, and Maria N. Yelenevskaya. 2005. "Incipient Soviet Diaspora: Encounters in Cyberspace." *Narodna umjetnost: hrvatski časopis za etnologiju i folkloristiku* 42 (1): 83–99.

Gabowitsch, Mischa. 2017. *Protest in Putin's Russia*. Polity Press.

Gelman, Vladimir. 2010. "The Dynamics of Subnational Authoritarianism (Russia in Comparative Perspective)." *Russian Politics and Law* 48 (2): 7–26.

Gillespie, Tarleton. 2018. *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yale University Press.

Gladarev, Boris, and Markku Lonkila. 2012. "The Role of Social Networking Sites in Civic Activism in Russia and Finland." *Europe-Asia Studies* 64 (8): 1375–1394.

Glasius, Marlies, and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere. Prologue." *International Journal of Communication* 12: 3795–3813.

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

Guriev, Sergei, and Daniel Treisman. 2022. *Spin Dictators. The Changing Face of Tyranny in the 21st Century*. Princeton University Press.

Haggart, Blayne, Natasha Tusikov, and Jan Aart Scholte, eds. 2021. *Power and Authority in Internet Governance. The Return of the State?* Routledge.

Han, Rongbin. 2018. *Contesting Cyberspace in China. Online Expression and Authoritarian Resilience*. Columbia University Press.

Hintz, Arne, and Stefania Milan. 2018. "'Through a Glass, Darkly': Everyday Acts of Authoritarianism in the Liberal West." *International Journal of Communication* 12: 3939–3959.

Hmed, Choukri, and Sylvain Laurens. 2011. "Les résistances à l'institutionnalisation." In *Sociologie de l'institution*, edited by Jacques Lagroye and Michel Offerlé. Belin.

Howard, Philip N., and Muzammil M. Hussain. 2013. *Democracy's Fourth Wave? Digital Media and the Arab Spring*. Oxford University Press.

Howells, Laura, and Laura A. Henry. 2021. "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance." *Communist and Post-Communist Studies* 54 (4): 1–27.

Jamil, Sadia. 2021. "The Rise of Digital Authoritarianism: Evolving Threats to Media and Internet Freedoms in Pakistan." *World of Media–Russian Journal of Journalism and Media Studies* 3: 5–33.

Jones, Marc Owen. 2022. *Digital Authoritarianism in the Middle East. Deception, Disinformation and Social Media*. Hurst.

Kalathil, Shanthi, and Taylor C. Boas. 2003. *Open Networks, Closed Regimes. The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace.

Keremoğlu, Eda, and Nils B. Weidmann. 2020. "How Dictators Control the Internet: A Review Essay." *Comparative Political Studies* 53 (10–11): 1690–1703.

Keucheyan, Razmig, and Laurent Tessier. 2008. "Présentation. De la piraterie au piratage." *Critique* 64 (733–734): 451–457.

Konradova, Natalya, and Schmidt, Henrike. 2014. "From the Utopia of Autonomy to a Political Battlefield: Towards a History of the "Russian Internet." In *Digital Russia. The Language, Culture and Politics of New Media Communication*, edited by Michael S. Gorham, Infunn Lunde, and Martin Paulsen. Routledge.

Lamensch, Marie. 2021. "Authoritarianism Has Been Reinvented for the Digital Age." *Center for International Governance Innovation*, July 9, 2021. https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/.

Laruelle, Marlène. 2021. *Is Russia Fascist? Unraveling Propaganda East and West*. Cornell University Press.

Laruelle, Marlène. 2022. "So, Is Russia Fascist Now? Labels and Policy Implications." *Washington Quarterly* 45 (2): 149–168.

Lewis, David G. 2020. *Russia's New Authoritarianism: Putin and the Politics of Order*. Edinburgh University Press.

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain. 2018. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure." *Policy and Internet* 10 (4): 415–453.

Limonier, Kevin. 2021. "'Vers un Runet souverain'? Perspectives et limites de la stratégie russe de contrôle de l'Internet." *EchoGéo* (56).

Lokot, Tetyana. 2020. "Articulating Networked Citizenship on the Russian Internet: A Case for Competing Affordances." *Social Media + Society* 6 (4).

Loveluck, Benjamin. 2015a. *Réseaux, libertés et contrôle. Une généalogie politique d'internet*. Armand Colin.

Loveluck, Benjamin. 2015b. "The Internet: A Society Against the State? Informational Liberalism and Political Economies of Self-Organization in the Digital Regime." *Réseaux* (192): 235–270.

MacKinnon, Rebecca. 2012. *Consent of the Networked. The World-Wide Struggle for Internet Freedom*. Basic Books.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar, and Hae-in Lim. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2018. "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." Citizen Lab research report no. 113, University of Toronto. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Mare, Admire. 2020. "State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe." *International Journal of Communication* 14: 4244–4263.

Maréchal, Nathalie. 2018. "From Russia with Crypto: A Political History of Telegram." FOCI 18–8th USENIX Workshop on Free and Open Communications on the Internet, Baltimore, MD. https://www.usenix.org/node/220216.

Morgunova, Oksana. 2012. "National Living On-line? Some Aspects of the Russophone e-Diaspora Map." E-diasporas Atlas working paper. http://www.e-diasporas.fr/working-papers/Morgunova-Russophones-EN.pdf.

Morgus, Robert. 2018. "The Spread of Russia's Digital Authoritarianism." In *AI, China, Russia, and the Global Order. Technological, Political, Global, and Creative Perspectives*, edited by Nicholas D. Wright. Air University Press.

Morozov, Evgeny. 2011. *The Net Delusion. The Dark Side of Internet Freedom*. Public Affairs.

Motyl, Alexander J. 2016. "Putin's Russia as a Fascist Political System." *Communist and Post-Communist Studies* 49 (1): 25–36.

Musiani, Francesca, Benjamin Loveluck, Françoise Daucé, and Ksenia Ermoshina. 2019. "Digital Sovereignty: Can Russia Cut Off Its Internet from the Rest of the World?" The Conversation,

October 18. https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952.

Nocetti, Julien. 2015. "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy." *Internet Policy Review* 4 (4).

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

Polyakova, Alina, and Chris Meserole. 2019. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Brookings Policy Brief, Democracy and Disorder Series*. Brookings Foundation. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Poupin, Perrine. 2022. "Conflit contre un projet de méga-décharge à Shies. Enjeux de souveraineté dans le nord-ouest russe à l'ère d'Internet." *Terminal* (134–135).

Roberts, Margaret E. 2018. *Censored. Distraction and Diversion Inside China's Great Firewall*. Princeton University Press.

Scott, James C. 1990. *Domination and the Arts of Resistance. Hidden Transcripts.* Yale University Press.

Snyder, Timothy. 2022. "We Should Say It. Russia Is Fascist." *New York Times*, May 19. https://www.nytimes.com/2022/05/19/opinion/russia-fascism-ukraine-putin.html.

Soldatov, Andreï, and Irina Borogan. 2015. *The Red Web. The Kremlin's Wars on the Internet*. Public Affairs.

Stadnik, Ilona. 2021. "Control by Infrastructure: Political Ambitions Meet Technical Implementations in RuNet." *First Monday* 26 (5).

Tesquet, Olivier. 2020. *À la trace. Enquête sur les nouveaux territoires de la surveillance*. Premier Parallèle.

Tréguer, Félix. 2019. *L'Utopie déchue. Une contre-histoire d'Internet XVe-XXIe siècle*. Fayard.

Uffelmann, Dirk. 2014. "Is There a Russian Cyber Empire?" In *Digital Russia. The Language, Culture and Politics of New Media Communication*, edited by Michael S. Gorham, Ingunn Lunde, and Martin Paulsen. Routledge.

Van der Vet, Freek. 2020. "Imprisoned for a 'Like': The Criminal Prosecution of Social Media Users under Authoritarianism." In *Freedom of Expression in Russia's New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari. Routledge.

Waldner, David, and Ellen Lust. 2018. "Unwelcome Change: Coming to Terms with Democratic Backsliding." *Annual Review of Political Science* 21: 93–113.

Wijermars, Mariëlle and Tetyana Lokot. 2022. "Is Telegram a 'Harbinger of Freedom'? The Performance, Practices, and Perception of Platforms as Political Actors in Authoritarian States," *Post-Soviet Affairs* 38 (1–2): 125–145.

1 DIGITAL SOVEREIGNTY IN RUSSIA: TAKING THE INTERNET CLAMPDOWN TO COURT?

Valéry Kossov

Russian Digital Development Minister Maksut Shadayev declared in 2022, "Russia has achieved digital sovereignty, as most foreign companies have left the market. Now, we are alone."[1] These words seem to conclude a decade in which the Russian authorities have gradually intensified their efforts to tighten their control over the digital ecosystem by framing it within the process of "internet sovereignization." While this process was initially presented as a step toward emancipation from foreign interference, it involved the enactment of numerous new laws, the regulatory functions of which rapidly took a repressive and political turn. At the same time, sovereignization has increasingly resembled isolation and technological autarky, especially since the beginning of the Ukraine invasion.

Yet despite the abundance of legislation governing the digital space, internet law has not been definitively transformed—in Russia as in the rest of the world—into a unified branch of law cutting across its entire scope, from constitutional law through to criminal procedures and administrative, commercial, or banking law (Huet 2012, 9–10). In view of the diversity of objects to regulate and the development of an increasing number of digital practices, the public authorities are having to rethink national regulatory frameworks to ensure that they cover the internet's diverse actors, practices, and activities. In the Russian context, regulations concerning the digital domain are instituted incrementally as their objects emerge and develop on the web—be it information, content and data of various kinds, or commercial relationships. Control is thus becoming a major issue for the authoritarian regime as it seeks to assert its hold on a domain that had seemed out of its

reach in the 2000s. Since Dmitry Medvedev's presidency (2008–2012) and his economic modernization project, the state has sought to regain the lead in the development of new technologies. It has established new structures tasked not only with coordinating the activities of public and private actors but also with supervising and monitoring them.[2]

The return of Vladimir Putin to the presidency and the wave of protests during the legislative and presidential elections of 2011–2012 opened a new era in the state's relationship with the digital ecosystem. It started to focus on its role as a regulator rather than as a coordinator of actors and their activities. The government's discourse already showed signs of a trend toward the sovereignization of the internet, reflected in the state's strengthened control over the national digital domain, especially through legal instruments. Since 2012, the Federal Assembly—the Russian parliament dominated by the ruling United Russia party—has launched legislative initiatives relating to internet regulation at an increasing rate. In a demonstration of the authorities' firm intention to broaden the range of its controlled objects, the number of bills to regulate the digital domain tabled in parliament rose from 5 in 2011 to 114 in 2017.[3]

OBJECTS AND ACTORS OF INTERNET LAW IN RUSSIA

This heterogeneous and tentacular legislation, often enacted through amendments to laws that are already in force, can be divided into three sections according to its scope, reflecting the three areas in which the state seeks to secure its sovereignty:

- Laws to regulate and monitor the flow of information and data
- Laws to control the digital infrastructure
- Laws to regulate the economic activities of private actors.

This classification is not perfect, as the scope of some laws may be broader and cover several areas of application. Yet despite particularities, using the purpose of a law as a classification criterion allows us to deductively sketch out the legislator's internal logic, geared toward digital sovereignty.

The intense legislative process introduced a system of institutional interaction involving several state actors. In 2008, the government agency Roskomnadzor (RKN) was created to monitor the sphere of information and communication and to act as an interface between various public and private actors, with a right to take legal action against infringements as its main tool. RKN's activities have grown and branched out, and the agency now interacts with various government structures, such as the Ministry of Communications, the police, the Investigative Committee, the FSB (Federal Security Service), the Prokuratura (Public Prosecutor's Office), and other internet users and stakeholders. In 2008, the first year after its creation, RKN reported having issued forty-nine warnings to the media for disseminating extremist material, drug propaganda, pornography, or violence.[4] By 2020, the agency had blocked several hundred thousand websites.[5]

USES AND TARGETS OF INTERNET LAW IN RUSSIA

Control by law concerns several sets of targets or subjects of regulation. Thus, the legislation adopted to control the flow of information online is increasingly affecting the media, journalists, activist organizations, and ordinary internet users and is bearing down on the digital industry's various companies (ISPs, operators, owners of traffic exchange points, etc.). The first to be affected were opposition digital media such as Grani.ru and Kasparov.ru, which were banned after the Lugovoi Law was passed in 2013 (398-FZ). Following the enactment in 2012 of Law 139-FZ, which set up a system of blacklists for websites containing illegal information,[6] the Lugovoi Law extended the scope of this ban to include political opposition media blocked by order of the RKN, without a court ruling. These laws additionally entail the obligation for ISPs to block illegal content and to install a box called Revizor for this purpose, which allows RKN to monitor their filtering work (see chapter 2). The Yarovaya laws (374 FZ, 375 FZ), passed in 2016, subsequently introduced the obligation to store users' digital data. They have had an impact on the infrastructure and economy of ISPs, which have been forced to expand their data storage capacities.

The so-called Sovereign Internet Law (90 FZ), which came into force in 2019, allows the state to take control of cross-border traffic points, change routing, and monitor content. The authorities initially claimed that the law was necessary to ensure that the internet would continue to function autonomously in Russia in the event of cuts from abroad.[7] However, their practices have proved to be very far removed from these uses and have impacted both the Russian internet's material infrastructure and the circulation of information on it. The law provides for the installation, at the state's expense, of TSPU equipment[8] at all major operators. This can be used both to automatically block prohibited content by means of deep packet inspection (DPI) technology and to slow traffic down on certain platforms—as Twitter users experienced on March 10, 2021—or to cut off mobile internet services in certain areas at specific times—as in Moscow during the demonstrations in the summer of 2019.[9] Yet this law's implications reach even further, as it provides the state with leverage on Big Tech companies whose resources and profits may suffer from choked traffic. The use of this threat is probably part of the reason why Russian authorities could remove opponent Aleksei Navalny's Smart Vote application from Google and Apple shops during the autumn 2021 parliamentary elections.[10] Finally, the war in Ukraine and the introduction of censorship in Russia made these threats actionable, as X/Twitter was blocked for Russian users and a court decision likening the social media company Meta to an extremist organization also led to the blocking of Facebook and Instagram.[11]

Thus, the takeover of the web's infrastructure through a legal hold on its technical facilities, algorithms, and software allows the state to extend its control over information flows and traffic. Simultaneously, the logic of sovereignization is being taken a step further: the state is seeking to interfere in the economic activities of digital companies, with the aim of securing the ability both to impose legal constraints on their development in the Russian market and to sanction them in case of any infringement and ensure that sanctions are properly enforced. Domestic digital giants such as Yandex, VK (VKontakte), and Mail.ru, which are already in the state's sphere of influence, offer no resistance to court or government decisions. For example, after the Law 208 FZ on news aggregator sites was passed, Yandex changed its

media selection algorithms to prioritize government media (see chapter 3). Similarly, the VK group agrees to hand over users' personal data to security agencies.[12] The situation is trickier with large international companies; as their physical presence on Russian territory is minimal, they are less exposed to coercive measures.

Several laws were adopted in 2021 to tackle this issue and to strengthen the state's control over the Russian digital market. The so-called Landing Law (236-FZ), which came into force in 2021, forces foreign companies to open branches in Russia so that they can be held responsible for their parent companies in Russian courts. Other laws aim to ensure state control over the online advertising market, in order to better monitor taxation on the profits of private players (347-FZ) or to have Russian-made software preinstalled on devices made by major foreign brands when they are intended for the Russian market (425-FZ). The state is pursuing its strategy to further control domestic players through legal or economic coercion mechanisms—including digital media platforms, which play an increasingly important role in the dissemination of information on the internet, to the extent that they are now competing with state-controlled television. Moreover, ever since sanctions were put in place following the annexation of Crimea in 2014, the state has also sought to impose legal constraints on various Western actors in the digital industry (Nocetti 2019).

In addition to operators managing internet infrastructure and large digital companies, the legislation affects a wider range of subjects, including journalists, activists, and ordinary users of online platforms or social media networks. The aim of this regulation is always to limit the circulation of information and exchanges on sensitive issues of a political nature that may challenge the regime, such as elections, or simply on social issues that the state prefers to conceal (domestic violence, ecology, etc.). Their toolbox includes the criminal or administrative prosecution of journalists, activists, or social network users, whose statements the police can interpret as "apology for terrorism" "calls for extremism," "insults to the memory of the Great Patriotic War," or, more recently, "discrediting" the army and other public institutions, as well as disseminating "false information" that undermines public order.[13] In the opinion of lawyers specialized in digital law, investigators'

interpretations of grounds for prosecution can sometimes be very liberal, as these laws define offences with little precision.[14] Cases are based on intelligence derived from the permanent surveillance of Russian social networks and regular monitoring of their foreign counterparts. The range of repressive norms has increased with the introduction of the mechanism of administrative prejudicial action, which allows for internet users to be convicted under criminal law after an initial administrative sanction. Courts often apply sanctions without any regard for the law's nonretroactive nature, which means people can be prosecuted for sharing information that has now become forbidden, even if they did so ten years ago.

Initially, the norms of criminal and administrative law were used selectively. Their application was dependent on the authorities' political agenda and the importance that they attached to any particular case. Then, as the regime stiffened, and especially after the start of the war in Ukraine, the repressive use of these laws became more extensive and targeted a wider range of actors, including independent media, NGOs, and even ordinary users. Two new laws were hastily enacted and signed into effect on March 4 (32-FZ) and March 25, 2022 (63-FZ). These two federal laws introduce amendments to the Code of Administrative Offences and the Criminal Code and provide for various sanctions for the dissemination of information discrediting the Russian army, as well as "false information" about the actions of the Russian army, Rosgvardia troops,[15] the Prosecutor's Office, embassies, and the Ministry of Emergency Situations in what is officially called the "special operation in Ukraine." Casting discredit on the army is now punishable under Article 23.3.3 of the Code of Administrative Offences by fines averaging 35,000 roubles (500 euros). In practice, this is mainly to sanction various antiwar statements published on social media, as well as the very use of the word *vojna* (war) in various contexts. Administrative sanctions also apply to the physical or virtual display of symbols that are considered antiwar, namely green or blue and yellow ribbons.[16] Since March 2022, the number of administrative cases involving alleged discrediting of the military rose steeply to 8,495, of which 1,703 cases were dismissed by the Russian judiciary.[17]

At the same time, the new Article 207.3 of the Criminal Code provides for the prosecution of anyone sharing "false information" or "fake news"

about the activities of the military and other state institutions.[18] The law does not provide a precise definition of "false information." Investigating judges and experts are thus left to assess the nature of the information and the seriousness of offences at their own discretion.[19] According to lawyer Pavel Chikov, this was modeled on the application in practice of Article 207.1, which was introduced into the Criminal Code in 2020 to criminalize the dissemination of Covid-19 disinformation: any data not issued by government sources is considered false.[20] Hence, the police may deem any information about the war that contradicts the Russian Ministry of Defence's communiqués, or even any claim that has not been mentioned by the Ministry, as "deliberately false," and anyone sharing these is liable to face criminal charges. In total, after more than two years of war, the Russian Prosecutor's Office reported 152 criminal cases involving "fake news" about the army and discrediting of the military.[21] Criminal prosecution of Internet users in wartime is not limited to the use of these new laws. Other laws are also put to use, with prosecution grounds such as "apology for terrorism," "extremist activities," "rehabilitation of Nazism," and "high treason" to condemn online activities deemed politically subversive or dissident by the authorities. The use of these laws in the digital domain has thus fueled the general repressive dynamic since February 2022.

This new legislation mainly targets journalists, bloggers, and internet users sharing articles, images, or videos that contradict the Ministry of Defence's claims or reveal facts that official sources fail to mention. Pretexts to hold individuals criminally liable include publishing Russian army casualty figures that do not conform to official statistics or mentioning cases of desertion by soldiers or contract police or casualties among the Ukrainian civilian population—regardless of the online medium used (websites, social networks, Telegram channels).

In the state's strategies to control information spaces, this recourse to administrative or criminal proceedings is combined with complementary legal constraints aimed at intimidating those targeted actors. These include the obligation for NGOs, media outlets, and more recently, individuals recognized as "foreign agents" by the Russian Ministry of Justice to label their publications as "originating from a foreign agent" (272-FZ, 2012; 327-FZ,

2017; 481-FZ, 2020).[22] The Kremlin often denies the repressive nature of these laws.[23] However, in addition to the financial constraints that they entail for the actors concerned, these laws single them out in the Russian public space with a label that carries negative connotations (Baunov 2021). The Ministry of Justice's registers of foreign agents have grown quite quickly, especially since 2022,[24] as the law's perimeter has been extended beyond the field of politics. The notion of engagement in political activities, which is the main ground for labeling an actor as a foreign agent, is very vaguely defined (article [art.] 2.1 of Law 272-FZ), which leaves the authorities free to apply it at their discretion. As a result, in addition to nongovernmental media and NGOs involved in politics, the Ministry of Justice's registers now include politically neutral organizations that do not receive state funding.[25] In addition, administrative sanctions, in the form of fines, for failure to report sources or references in online publications as foreign agents became increasingly common in 2021.[26] In Moscow alone, there have now been hundreds of these cases, targeting media sites, social media, NGOs, and professional associations alike.

The existence of four separate registers of foreign agents (NGOs, media, natural persons, and unregistered associations) makes their control by state bodies problematic and creates confusion in the process of placing actors under this status, with different types of constraints coming into play. In order to rationalize the use of this norm, but also to further tighten its effect on this heterogeneous group of actors, the legislature decided to adopt a new law entitled On the Control of the Activities of Persons under Foreign Influence (Law 255-FZ), which entered into force on December 1, 2022. It packaged the legal provisions relating to the status of foreign agent, which were until then scattered between several laws, and introduced uniform criteria for applying it to natural or legal persons. The law provides for a single register and a standardized procedure to delete names from it. In general, it gives the authorities more leeway in granting this status, as foreign funding will not be the determining criterion. A person can now be declared a foreign agent if they are deemed to have benefitted from "foreign support" in any form, material or immaterial, or to be "under foreign influence." The vagueness of these criteria leaves law enforcement agencies room to interpret

the law on a case-by-case basis. Moreover, if necessary, its application can be extended to the entire Russian population except civil servants, staff of state-owned enterprises, members of political parties, and officials of international organizations. At the same time, the law introduced additional constraints for foreign agents, significantly limiting their civic rights, and especially their voting rights, and provides for a single, well-defined procedure as a way out of this status.[27] The state's strategy thus seems to consist in keeping an eye on any actor likely to express disagreement with official narratives online and to being able to legally remove them from public life around elections or during tense situations, while at the same time providing an "escape route" for those who may be willing to show their allegiance to the regime.

Furthermore, to add to the intimidation, the 2012 Law 272-FZ, supplemented in 2015 and 2021, introduced the notion of "undesirable organizations representing a threat to state security." Media outlets and NGOs that fall under it are simply forbidden to operate on Russian territory, meaning these foreign and Russian companies, media outlets, and NGOs are not allowed to set up branches, carry out financial transactions, or share information online, since their websites are on RKN's blacklist. As in the case of foreign agents, any mention of the organization's name in online publications, whether in press articles or blogs, or on social media must come with a warning. The legal apparatus has been considerably strengthened since 2021. It now provides for significant prison sentences for participants in the activities of "undesirable organizations," which have pushed NGOs, media outlets, and other actors to dissolution or exile (see chapter 8).[28] The Ministry of Justice's register includes political NGOs, such as Otkrytaya Rossiya and foreign observers of the Russian elections, as well as investigative media, such as *Proekt* Media, Bellingcat, and The Insider, religious organizations, and even Bard College, the private American humanities university that had opened an arts faculty at St. Petersburg University.[29]

Finally, even more severe repression can apply to organizations that are labeled as "extremist." Law 114-FZ stipulates that any group can be labeled extremist through a court decision, which entails its dissolution and criminal sanctions for individuals who have funded it or participated in its activities. Penalties also apply for sharing and publicly displaying the organization's

various materials (publications, videos, images, logos, etc.). While the application of these penalties is not an issue in the case of Navalny's NGO, the Anti-Corruption Foundation (FBK), which was categorized as an extremist organization in 2021,[30] the same cannot be said of the company Meta Platforms (Facebook's parent company), which had this status imposed on it on March 22, 2022. The law had never been used against a large multinational, which is why legal experts have many questions about what is likely to lead to criminal sanctions and why users of Meta's social networks and other products, or even its Russian investors, are understandably worried.[31]

The arsenal of legal tools is thus weighing down increasingly heavily on Russian political and social life, affecting digital infrastructures and social actors alike. The scope of the legislation now seems to cover most of the areas the state can regulate, reflecting a will to control the circulation of information within the country. Thus, even before the war, the state had drastically strengthened its control over the internet and over a large part of nongovernmental activities. In the current situation, what are the implications of this legislation for the various players in the Russian digital ecosystem, and how can they deal with this corrupt legal, regulatory, and repressive arsenal?

STRATEGIES TO RESIST AND CIRCUMVENT LEGAL OPPRESSION

While increasingly severe legal constraints, especially in the context of the war in Ukraine, have narrowed the space for media, activists, and freedom of expression in general, the internet in particular has become a prime target for censorship. Although the state's grip on the legal space seems total, with the legislative and judicial powers working for the executive branch, there are still some legal tools companies, media, activists, and users can use to defend themselves, with the help of a handful of NGOs that provide them with legal services. There are currently several organizations defending digital rights: Setevye Svobody (Network Freedoms) the successor to the association Agora,[32] as well as the Digital Rights Center law firm created by lawyers from the NGO Roskomsvoboda. Others, such as the Centre for the Defence of Media Rights, OVD-info, and Pervyï otdel, are more broadly

concerned with protecting the rights of journalists, activists, and ordinary citizens prosecuted by various repressive agencies.

In this tense political context—let alone in wartime—legal actions against the state and its institutions are rare, and the defense of those who are prosecuted is seldom successful. According to one of the activists we interviewed, this is essentially "palliative care" for those who are caught in the state's repressive machinery.[33] Nonetheless, complaints against RKN and other executive structures were regularly filed before the war, with varying degrees of success. Committed lawyers still see this recourse to legal action against the state, or through a complaint against an unknown person, as quite an effective tool, for it can spark public debate around limitations to digital rights or set a judicial precedent.[34] Bringing a case to court attracts media attention and raises public awareness of the consequences of a particular state initiative, especially when it comes to the use of biometric data or facial recognition in video surveillance. Beyond simply winning the case, this strategy of litigation aims to leave a lasting mark on society and to have an effect on the public in general, and on the authorities in particular.

Before the war, Setevye Svobody's lawyers would actively seek out questionable judgments or wrongful convictions of internet users, to challenge them at the European Court of Human Rights (ECHR) after having exhausted the possibilities of appeal before the Russian courts. This was a complicated and often very long procedure, as tedious exchanges with the Russian judiciary were necessary to examine complaints. However, it was an important means of winning cases and establishing a channel of communication between the European and Russian courts, which made it possible to set precedents, make adjustments to judicial practices in Russia, and obtain financial compensation for Russian litigants. Appeals to the Russian judiciary and the ECHR following sentences against internet users for disrespect toward the authorities (Law 30-FZ), for instance, curbed the use of this law by investigative bodies in 2020–2021.[35]

This valuable tool became obsolete after the beginning of the war in Ukraine. On March 16, 2022, the Committee of Ministers of the Council of Europe decided to exclude Russia, which in turn rejected the European Convention on Human Rights and exited the system of protection of rights

and freedoms and the European Court of Human Rights.[36] This exclusion has had a direct impact on Russian litigants, as Russian citizens can no longer apply to the ECHR to gain compensation when their rights have been violated by the state. Formally, Russia retained its EC membership until January 1, 2023, and applications from Russian plaintiffs filed before September 16, 2022 could be considered by the ECHR.[37] However, after opting out of the European Convention on Human Rights, Russia ceased to abide by ECHR decisions delivered during this period, and the Russian Prosecutor's Office has ended its communication with the European court. During the spring of 2022, some Russian lawyers remained convinced that filing complaints with the ECHR during this period made sense and was still a last resort to protect human rights.[38] However, a new bill, tabled in the Duma on May 16, 2022 and enacted on June 11, 2022 (Law 183-FZ), provides for Russia's refusal to enforce ECHR decisions taken after March 16, 2022.[39] Despite its contradictory nature, this law allowed the Russian state to abruptly terminate compensation payments to plaintiffs, whose numbers may have increased significantly since February 24, 2022, given its controversial judicial practices in cases related to military censorship.[40] It also signified a unilateral and rapid break in the relationship between the Russian judiciary and the ECHR.

From a legal point of view, Russia might one day rejoin the Council of Europe and the European Convention on Human Rights system, thereby restoring its status with the ECHR—even though the autarkic penchant that has transpired in the Russian judiciary and normative system's aspirations for sovereignty in recent years and the current political leadership's rhetoric of breaking with international law seem to make this a distant prospect.[41]

To defend their clients, lawyers have other legal tricks up their sleeves. For example, they are sometimes able to invalidate the digital evidence gathered by investigators, based on a technicality. If the investigation report refers to a screenshot of a reprehensible document taken from a desktop computer while the copy of that document attached is a screenshot from the investigator's smartphone, for instance, the court can be compelled to refuse to recognize the evidence's validity.[42] Loopholes like this and many others sometimes enable lawyers to win cases in court. However, those whom we

interviewed recognized that these strategies lose their efficacy in sensitive and politicized cases, in which investigators, prosecutors, and judges are united against the defendants and their attorneys. In these cases, the room for legal resistance is very limited.

Since lawyers are themselves at risk of prosecution, some of their strategies, by anticipation, rely more on circumvention and adaptation than resistance. For instance, some activist organizations, such as Setevye Svobody or Agora International, carry out their activities in the form of a "project," which is neither officially registered as an NGO nor located in a specific place. Thus, they do not have offices that can be searched by the police, and they operate entirely in the virtual space. For instance, they have channels on the Telegram messaging platform that allow them to communicate about the specifics of new laws, their implementation, and case law and to inform colleagues and other interested audiences about rights and legal means of resistance to arbitrary police action. However, this is done in strict compliance with the law, no matter how restrictive it is, so as not to jeopardize their ability to practice off-line as lawyers. Other organizations expatriate, as did the Komanda 29 team (Team 29, an association of journalists and lawyers specializing in open-government cases), which became Pervyï otdel in Georgia. Its founder, the lawyer Ivan Pavlov, moved there after being accused of disclosing investigative material and having his status suspended by the St. Petersburg Chamber of Lawyers.[43] While this last resort strategy primarily serves to avoid individual prosecution, it also allows Russians to remain active from exile while relying on a network of colleagues who have remained in Russia to appear in court.

Individual or collective adaptation strategies involve investments in computer security: VPN use has become quite commonplace, as have data encryption and the use of messaging systems deemed reliable, such as Signal, Telegram, and Wire, and internet users develop individual solutions for protecting data or circumventing blockages. They share these strategies in exchange groups and during collective training webinars or hackathons. Roskomsvoboda's lawyers have organized a school in Moscow that provides training in digital law. This knowledge and expertise circulate internationally, through collaboration with associations defending digital rights in

post-Soviet countries such as Kazakhstan, Kyrgyzstan, and Belarus, and with international associations defending human rights or digital rights, such as the International Network of Civil Liberty Organizations (INCLO) and Access Now, respectively. Even though they do not necessarily involve foreign funding, such collaboration is always risky for Russian organizations, as they could be placed under foreign agent status for participating in training provided by a foreign NGO, which the authorities equate with "non-material foreign assistance" or, more recently, "foreign influence."

Activist circles' repertoire of actions has thus evolved significantly over the past decade as they have adapted to increasingly harsh legislation, online repression, and restrictions on digital rights. Some perspectives concerning their future are coming into focus in an increasingly restrictive legal field, which now seems theoretically able to exclude all freedom of expression from the sovereignized digital space and, more broadly, from the Russian social space.

CONCLUSION

Internet sovereignization in Russia, which has come with legal regulation that is as opaque as it is pervasive and increasingly repressive, has led the legal system to a mono-normative model, with state institutions showing increasing mistrust toward international actors and disdain for those who provide them with access to their rights. In recent years, it has tended increasingly toward mono-normativity (Barraud 2018), a model in which the norms governing cyberspace exclusively originate from the state. Such a normative system significantly pushes back the prospect of internet coregulation and simultaneously affects infrastructures, digital companies, and users. It thus represses the competitive development of digital technologies, but also, and most importantly, the circulation of information and the online activities of independent media and activists, as well as the free expression of users. Thus, recent administrative rulings de facto sanction the very expression of an opinion on the war, which the judiciary interprets as criminal discredit of or disrespect toward the army and state institutions, or even hate speech. As for the Criminal Code, it is used in fake news trials to punish anyone

challenging the official narrative and sharing war-related facts and events online, as the courts see this as a manipulation of public opinion. Admittedly, this repression remains relatively targeted and does not yet take on the same magnitude as in the era of the great Stalinist terror. However, the authoritarian Russian regime is succeeding in instilling fear through these occasionally severe sentences, as some high-profile legal cases are rapidly brought to the attention of the general public via social networks and media. As a result, many Internet users are forced to exercise self-censorship when expressing themselves online. The repressive use of the law is therefore fully in line with the logic of sovereignization of the digital space, which the Kremlin has been pursuing since the early 2010s in a quest to standardize information channels and align them with official sources.

This process of sovereignization reveals the state's lack of interest in horizontal self-organization of the population and in any form of feedback or alternative information from the media, NGOs, and activists. The outlook for these actors is therefore bleak, as in addition to judicial harassment, the state obviously does not provide them with any funding, nor does it encourage private donations from Russian companies. They are therefore forced to find funds abroad, which inevitably leads them to be categorized as foreign agents. The Foreign Agents law will remain a sword of Damocles permanently hanging over concerned actors, whatever their field of activity: investigative journalism, election monitoring, ecology, domestic violence, or women's rights.

This abundance of laws with sometimes obscure and imprecise wording leaves room for misinterpretation of norms, while the lack of clarity in the legislation leads to difficulties in its application. The positivist approach to the use of law that is prevalent in Russia leads to excessive regulation of the smallest issues, thus curtailing the judiciary's autonomy. The intensive production of tailored legislation ordered essentially by the government or the presidential administration reflects the will of only the executive branch, which must then specify the modalities for the execution of these laws through various regulations and circulars, thus bloating legal codes even further (Šul'man, 2020). Furthermore, laws are often passed by members of parliament (MPs) who lack technical or legal expertise and do not

properly consult with professionals who have experience in internet or digital law. This makes it difficult for the police and the courts to understand and interpret these texts. The regulation of the information space by law thus produces a false impression of control while actually introducing confusion and arbitrariness in state institutions. For example, recent so-called military censorship laws leave the police in charge of interpreting and assessing offences, without providing them with precise definitions of "discredit" or "fake news." In a legal space that is presumed to be homogeneous, this results in sentences that can vary from administrative fines to prison time, sometimes for identical offences.

Finally, in its ambition, the legislator sometimes overestimates the development stage and speed of technologies and investments in the digital field. Despite recent advances in DPI boxes and other surveillance and blocking techniques, a number of laws, including the Yarovaya law, are still pending due to a lack of human and technical resources. Other coercive legal provisions are left unenforced, or at least decriminalized because of enforcement issues. Digital and technological sovereignty, as it is presented in discourse, doctrine, and norms, still seems far from being achieved. It even seems to be significantly compromised by the disruption of trade with Western countries as a result of the war. For its part, internet law, which is geared toward sovereignization goals, adopts a coercive model, which does not seem very viable outside its system of technological interdependence and which is coming up against its internal contradictions as it evolves toward greater autarky and isolation in the context of the war and economic sanctions.

NOTES

1. "Mincifry ob"âvilo o dostiženii cifrovogo suvereniteta: inostrannye IT kompanii ušli," *Kommersant*, November 25 2022, https://www.kommersant.ru/doc/5682591.
2. In 2010, in an attempt to attract significant foreign investment, the government created the Skolkovo innovation center in the suburbs of Moscow. This was meant to be a new "Russian Silicon Valley," that would develop and market new technologies (Limonier 2012).
3. Setevye Svobody, "Svoboda Interneta 2020: vtoraâ volna repressij," 2020, https://runet.report/static/core/doc/Свобода%20интернета%202020.%20Вторая%20волна%20репрессий.pdf.

4. RKN 2008 Annual Report, https://digital.gov.ru/ru/events/20581/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
5. RKN 2021 Annual Report https://rkn.gov.ru/plan-and-reports/reports/p449/ (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.").
6. Initially, the aim of Law 139-FZ was to protect young people from online gambling, child pornography, contents encouraging drug use, and incentives to commit suicide.
7. Explanatory note published on the website of the State Duma. "Prinât zakon o suverennom Internete," April 16, 2019, http://duma.gov.ru/news/44551/.
8. *Tehničeskie sredstva protivodejstviâ ugrozam* (technical means for countering threats).
9. "V poslednie gody vlasti 'otrubali' Internet v svoih stranah sotni raz. So vremenem vkus k otključeniäm rastët," Cnews, September 1, 2021, https://www.cnews.ru/news/top/2021-09-01_eksperty_opasayutsya_zloupotreblenij.
10. "Human Rights Advocates Decry Apple, Google Decision to Pull Navalny App as Russia Voting Begins," *Washington Post*, September 17, 2021, https://www.washingtonpost.com/business/2021/09/17/navalny-google-apple-app-russia/.
11. Tverskoy District Court of Moscow ruling no. 02-2473/2022, https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=Meta.
12. Roskomsvoboda Analytical Report, "Vkontakte rasskažet pol'zovatelâm o zaprosah silovikov," August 15 2018, https://roskomsvoboda.org/40933/.
13. The first version of the law (39-FZ) against the dissemination of false information came into force in 2019. Its scope was extended in 2020 to information on the Covid-19 pandemic (100-FZ) and on the Russian army since the beginning of the war in 2022 (63-FZ).
14. Interview with a Roskomsvoboda lawyer conducted on July 19, 2021.
15. Military formations based on Russian Interior Ministry troops, created in 2016 to bolster traditional law enforcement bodies.
16. "'Novgorodcu naznačili obâzatel'nye raboty za razdaču zelënyh lentoček," Bezformata, March 11, 2022, https://velikiynovgorod.bezformata.com/listnews/obyazatelnie-raboti-za-razdachu-zelyonih/103340546/.
17. Statistics from *Kommersant*, https://www.kommersant.ru/doc/6651563.
18. "Federal'nyj zakon o vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj FederaciiF i stat'i 150 i 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii," 63-FZ, 25 March 2022, http://www.consultant.ru/document/cons_doc_LAW_412674/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100009.

19. The three paragraphs of article 207.3 detail the penalties incurred, which start with fines (paragraph 1) and go up to fifteen years imprisonment (paragraph 3) if the imputed acts lead to serious consequences for the functioning of the army or public institutions.

20. "Dezertiroval iz mirnoj žizni v SIZO," *Meduza,* May 17, 2022, https://meduza.io/feature/2022/05/17/dezertiroval-iz-mirnoy-zhizni-v-sizo.

21. Statistics from *RBC*, https://www.rbc.ru/politics/20/02/2023/63f30d769a7947c894f2d066.

22. Among other things, the law provides for a complex system of income and expense accounts that actors categorized as foreign agents must submit to the authorities, as well as other restrictions on the rights of natural persons.

23. During online press conferences, Kremlin representative Dmitry Peskov often insists that the foreign agent status does not impede on the work of media and journalists in Russia. "V Kremle isključili ograničenie raboty Meduzy iz-za statusa inoagenta," *RBC*, April 28, 2021, https://www.rbc.ru/rbcfreenews/60893eb09a79475e858c563e.

24. Lists of media, NGOs, or individuals with foreign agent status can be found on the website of the Ministry of Justice. However, efforts to monitor the use of the law are complicated by the fact that several registers are kept, including foreign media acting as foreign agents, NGOs, and so on. Despite this difficulty, the register of foreign media recognized as "acting as foreign agents" allows us to assess the dynamics of the application of the law in 2021. Website of the Ministry of Justice of the Russian Federation, https://minjust.gov.ru/ru/documents/7755/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")

25. These include, for example, feminist associations and organizations fighting against domestic violence or for the protection of children's rights.

26. Recurrent failure to report can lead to the media outlet's license being withdrawn and its publication blocked. This is why the daily *Novaya Gazeta* decided to suspend its activities on March 28, 2022 after receiving its second warning from RKN regarding its failure to label an NGO as a foreign agent in one of its articles. See editorial statement: https://novayagazeta.ru/articles/2022/03/28/roskomnadzor-soobshchil-chto-vynes-vtoroe-preduprezhdenie-novoi-gazete-news.

27. Media Rights Advocacy Centre report, "Novyj zakon ob inoagentah: čto pomenäetsâ?" *Inoteka*, April 28, 2022, https://inoteka.io/ino/2022/04/28/novyy-zakon-ob-inoagentah-chto-pomenyaetsya.

28. Several members of Mr. Khodorkovsky's NGO Otkrytaâ Rossiâ were convicted post factum in criminal proceedings for participation in an "undesirable organization" after its dissolution in 2021. The police often hold up Facebook reposts of information about the NGO dating from before 2021, and therefore prior to the adoption of the criminal amendments increasing penalties for them. For instance, this was used against former director of Otkrytaâ Rossiâ Andrei Pivovarov, who was sentenced in 2022 to four years in prison.

29. Ministry of Justice Register, https://minjust.gov.ru/ru/documents/7756/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")

30. Most of Navalny's collaborators have been forced to leave Russia. All FBK publications are banned from the internet, and sharing them is punishable by law, as is subscribing to Navalny's Telegram channel and other FBK social networks.

31. RKN has blocked Facebook and Instagram but has left WhatsApp free to use. Users of Meta's social networks are not penalized by default, but it is forbidden to display Meta's logo or to buy its shares on the stock exchange. The situation is still evolving, and in October 2022, the Moscow Prosecutor's Office issued a warning to a Russian Instagram fashion influencer for using the platform, even though her posts had nothing to do with politics or the war. See "Pervoe blogerskoe preduprežhdenie," *Advokackaâ ulica*, October 6, 2022, https://advstreet.ru/columns/pervoe-blogerskoe-preduprezhdenie/.

32. The association Agora was founded in 2005, declared a "foreign agent NGO" in 2014, and liquidated by court decision in 2016. Agora International, which succeeded the dissolved NGO in 2016, has no legal status and is, in the words of its founder, Pavel Tchikov, more of an "interest club" for the defense of human rights than a for-profit organization. See Smirnov Sergei, "Osoznannoe dopuŝenie ugolovnogo dela i tur'my," interview with Pavel Chikov, *Mediazona*, November 28, 2015, https://zona.media/article/2015/26/11/agora-international.

33. Interview of November 19, 2022.

34. Interviews of July 19 and 23, 2021.

35. "Sto nedrugov vlasti: kogo i kak nakazyvaût v Seti," Roskomsvoboda, https://roskomsvoboda.org/post/sto-nedrugov-vlasti-kogo-i-kak-nakazyiv/.

36. "Russian Federation Excluded from the Council of Europe," COE Committee of Ministers Press Room, March 16, 2022, https://www.coe.int/fr/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe.

37. According to article 58, paragraph 1 of the Convention, the parties may only opt out of the Convention after giving six months' notice. In the meantime, all obligations of the parties under the Convention remain effective and unchanged. This is how the ECHR has interpreted the provisions of article 58. "Resolution of the European Court of Human Rights on the Consequences of the Cessation of Membership of the Russian Federation to the Council of Europe in Light of Article 58 of the European Convention on Human Rights,' https://echr.coe.int/Documents/Resolution_ECHR_cessation_membership_Russia_CoE_ENG.pdf.

38. "Napomnit' rossijskim vlastäm odnu važnuû veŝ," interview of Ekaterina Gorbunova with lawyer Dmitry Gurin, *Advokackaâ Ulitsa*, March 24 2022, https://advstreet.ru/interview/napomnit-rossiyskim-vlastyam-odnu-vazhnuyu-veshch/.

39. "Rešeniâ ESPČ ne budut ispolnâtsâ v RF: zakonoproekt," website of lawyer Oleg Anišikov, May 17, 2022, https://europeancourt.ru/2022/05/17/36465/.

40. Some plaintiffs could obtain compensation until January 1, 2023 upon a decision of the Russian Prosecutor's Office.

41. Interview with Dmitry Medvedev to the RIA agency and the RT television channel on March 26, 2022, https://ria.ru/20220326/medvedev-1780208448.html.

42. Interview of June 17, 2022.

43. Pavlova, Zinaida, "Stalo izvestno, čem Sovet AP Sankt Peterburga motiviroval priostanovlenie statusa advokata Ivana Pavlova," *Advokackaâ Gazeta*, April 5, 2022, https://www.advgazeta.ru/novosti/stalo-izvestno-chem-sovet-ap-sankt-peterburga-motiviroval-priostanovlenie-statusa-advokata-ivana-pavlova/.

REFERENCES

Barraud, Boris. 2018. "La corégulation d'Internet (ou comment répondre à la plurinormativité par l'internormativité): Une contribution française." *Les Cahiers de droit* 59 (1): 85–116.

Baunov, Alexandre. 2021. "Inostrannyj agent. Politiko-semantičeskij analiz." Carnegie Russia Eurasia Center, Berlin. October 18. https://carnegieendowment.org/posts/2021/10/inostrannyj-agent-politiko-semanticheskij-analiz.

Huet, Jérôme. 2012. "Le juriste et la communication numérique: Une brève introduction." In *La Communication numérique, un droit, des droits*, edited by Bernard Teyssié. Editions Panthéon-Assas.

Limonier, Kevin. 2012. "Analyse géopolitique des enjeux d'une politique de puissance: Le cas de la science et de l'innovation en Russie." *Hérodote* 146–147 (3): 193–216.

Nocetti, Julien. 2019. "La Russie en quête de son "Internet souverain." INA. June 21. https://larevuedesmedias.ina.fr/la-russie-en-quete-de-son-Internet-souverain.

Šul'man, Ekaterina. 2020. *Praktičeskaâ politologiâ. Posobie po kontaktu s real'nost'û*. ACT.

2 SURVEILLANCE AND CENSORSHIP OF INTERNET INFRASTRUCTURES: MARKETS, REGULATION, AND BLACK BOXES

Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani

From the early 2010s, the development of the Russian internet has characteristically featured strong state interventionism, in terms both of legal instruments and of technical infrastructure. In the context of the Sovereign Runet doctrine, an important part of the authorities' strategy has been to encourage the development of Russian-made technical solutions for censoring and intercepting internet traffic. This has created a thriving market for Russian providers of software and hardware solutions for monitoring and filtering traffic. This chapter offers an analysis of this industry and its effects on internet service providers (ISPs). We look at the controversies surrounding the various technological assemblages that actors of the Russian internet must adopt to comply with current regulations, which are costly and complex to implement and raise many ethical and political concerns.

We first present our approach, which is rooted both in political economy and in the sociology of technology and innovation, and the mixed methods that have been mobilized to collect empirical data. We then draw a distinction between two strategies of information control: online surveillance ("lawful interception") on the one hand and censorship ("traffic filtering") on the other. We thus present two types of devices that were central to the 2016 Yarovaya Law and discuss their influence on the ISP market: surveillance systems called SORM (system for operative investigative activities) that establish a direct link with intelligence agencies and traffic-filtering solutions used to block access to websites blacklisted by the federal media and telecommunications regulatory agency Roskomnadzor (RKN).

We then discuss the additional step that was taken with the 2019 Sovereign Internet law, as all operators must now install a new type of device called a TSPU (technical means for countering threats) on their networks. This includes a deep packet inspection (DPI*)* filter that can analyze data packets, throttle or block access to certain resources, and, as the 2019 law prescribes, limit data traffic within Russia. In 2021, for example, a DPI filter was used to slow down Twitter and to block the voting assistance application that the opposition had offered during the elections. This filtering can be activated remotely, does not require network operators to cooperate, and entirely evades citizen surveillance. This new constraint on ISPs represented a decisive tightening of the authorities' grip on digital infrastructures.

In this chapter, we also analyze the effects of these measures on the balance of the Russian internet market and on its relations with foreign networks and services, and we assess the possibilities of circumventing this system through an array of legal and technical ruses. Finally, we analyze the impact of Russia's invasion of Ukraine on these information-control technologies, showing how international sanctions have exposed the role of major international manufacturers in the techno-legal project of the Sovereign Runet. With the departure of Nokia, IBM, Intel, and Cisco from the Russian telecom market, what is left of these surveillance and censorship boxes?

A SOCIOECONOMIC STUDY OF THE RUSSIAN INTERNET'S "BLACK BOXES"

With over 6,326 licenses issued in 2020 (and 3,461 to 3,940 of them active[1]), the Russian ISP industry showed distinctly strong competition, low prices, and good connectivity quality until the late 2010s, as well as a relatively decentralized topography and a large number of transnational peering agreements. Many Russian ISPs started as "local networks" (*domovaya set'*) and formed active professional communities, resulting in a large number of professional associations, conferences, and forums. Since the mid-2010s, however, the ISP market has undergone increasing legal and infrastructural centralization. From 2017 to 2020,[2] the number of licenses issued for "telematics services" and "data transfer services" decreased (from

9,395 to 8,000 and from 7,035 to 6,326, respectively[3]). Additionally, government initiatives to create a "self-sustaining Russian internet" included the introduction of a "central control point." This involves, among other things, a mandatory register of all transnational cables and peering points that, until then, had not been properly documented by the various government bodies concerned.

In this chapter we discuss surveillance and censorship of the Russian internet from the perspective of their political economy, which sheds light on their inherent logics and workings. In the case of Russia, these aspects of state power have recently been asserted increasingly and in very explicit terms. We show how the "black boxes" imposed on private actors at the level of internet infrastructure through regulatory measures are embedded in (and contribute to) a set of social, economic, and political relations. In doing so, we deconstruct the oversimplified image of direct state control through technology. This affords an understanding of a key aspect of the "global struggle for internet governance" (DeNardis 2014) and of how internet infrastructures themselves can be leveraged to support power relations.

This "turn to infrastructure" in internet governance (Musiani et al. 2016) also presents a more complex picture of the articulation between law and code (Lessig 2006) and between political regimes and their translation into socio-technical and economic practices. The relationship between legal procedures and their technical implementation is a central aspect of internet governance: the behavior of internet users is regulated by the inscription of norms, affordances, and constraints in both technical infrastructures and laws, and policymakers increasingly exploit them to achieve (geo-)political goals (Winseck 2017). This is particularly true in Russia, where law and code interact in a very specific way. Technical solutions often lag behind regulation, as the law seeks to gain control over the infrastructure (see, for example, Ermoshina and Musiani 2017). Moreover, this constant increase of regulations has led to criticism from the ISP community, where some have called it a "security theatre" (Schneier 2003), in which political rhetoric primarily serves underlying commercial opportunities. With import substitution (the preference for domestic companies, put in place long before the full-scale war with Ukraine) as a rule, information control solutions must

be "made in Russia." In this context, Russian internet regulation has created a fully fledged market for censorship and surveillance, shaping competition between different domestic suppliers of infrastructure components and affecting the operations and strategies of ISPs.

Studying these markets allows us to closely analyze the relationship between standardization and competition. Although Russian internet governance is increasingly presented as a matter of national sovereignty, the Russian state remains slow to produce and certify technical surveillance and censorship solutions. Moreover, the context of Russia's invasion of Ukraine in 2022 and the international sanctions adopted in retaliation shed light on the Russian surveillance and censorship industry's reliance on foreign components, infrastructure, and know-how. The results are techno-legal loopholes and gray areas that create both uncertainties and opportunities. Our study of the middlebox market also highlights resistance practices that often develop in response to specific filtering and surveillance techniques and allows us to track and understand the politicization of web professionals.

Our ethnographic methods allow for a detailed examination of the "plugs, settings, sizes and other profoundly mundane aspects of cyberspace" (Star 1999, 379) regarding the three technical solutions discussed in this chapter. These technologies can be seen as "black boxes" (Callon, 2013) in several respects. They are presumed to be technically opaque and serve filtering and surveillance purposes, which places them in the realm of state and commercial secrecy. They do not always resemble clearly identifiable physical boxes (although they sometimes do) but consist, rather, of a multitude of software solutions, distributed technical objects, and techno-legal adjustments that complement existing physical infrastructures. Lastly, they are a focus of controversies related to surveillance and censorship in Russia, generating ambiguities, interpretations, disputes, resistance, and negotiations.

Our study of these activities, which are both specialized and sometimes shrouded in secrecy, presented a number of challenges. These were partly mitigated by adopting a "mixed methods" approach and collecting three main types of material from 2017 to 2019 and again in 2022. First, we conducted fifteen interviews with ISP staff (mainly from small and medium-sized companies with portfolios of five thousand to a hundred thousand

clients), IT experts, internet lawyers, vendors of filtering and DPI equipment, anticensorship and antisurveillance activists, and engineers working at the internet exchange point (IXP) in St. Petersburg. We then conducted five interviews in the summer and autumn of 2022 to update our survey. The interviewees all asked to remain anonymous.

The study was complemented by a web-ethnography and analysis of ISP forums and chatrooms, which were selected and observed throughout the study period. We also conducted an analysis of technical documentation and communication materials produced by vendors of surveillance and censorship solutions: websites, commercial presentations, and materials from specialized professional conferences. Finally, we measured the extent of censorship in 2018 (in partnership with Citizen Lab; see also Valentovich and Ermoshina 2019), to analyze the technical implementation of censorship on the Runet. An analysis using the OONI Explorer tool,[4] as well as analysis of Border Gateway Protocol (BGP) routing data and other traffic metrics, was conducted more recently, in 2022, to assess the impacts of Russia's invasion of Ukraine on Runet connectivity and the accessibility of digital resources.

SORM AND THE SURVEILLANCE MARKET: CONSTRAINTS AND BRICOLAGE

SORM is a system for the lawful interception of telecommunications. It is a distributed object consisting of switches, servers, data storage volumes, extractors, remote control terminals and software. While it must be installed at the operator's expense, it is directly controlled by the Federal Security Service (FSB) and accessed on request by other agencies and police services (tax, customs, border police, etc.). SORM-1 was set up in 1995 for phone tapping and surveillance. It has since evolved into the internet-ready SORM-2 in 1998, and SORM-3 in 2014, which included specifications for the collection of metadata (such as time and date, location, sender, and recipients of messages) and multimedia files.

The latest iteration was defined by the "Yarovaya" laws 374-FZ 4 and 375-FZ passed in 2016, raising a wave of criticism from digital rights and freedoms organizations[5]. After almost two years of discussions due to the

technical complexity of the law, and due to abundant criticism from the ISP community, the regulation was relaxed to some extent. According to the amendment of April 12, 2018, telecom providers must now store metadata for three years and the content of all voice calls, data, images, and text messages for thirty days (instead of the original ninety days), with a 15 percent increase in storage time each year. However, this 15 percent increase requirement has already been postponed twice—first in 2020 in the context of the pandemic and then in March 2022, following international sanctions, revealing both the difficulty of implementing this measure and the inability of the Russian market to propose technological solutions that would allow it to meet the regulators' demands by its own means.[6]

Data stored under the provisions of the Yarovaya Law must be made available to the authorities on request and can be obtained without a warrant or court order. Moreover, online services using encrypted data for messaging, email, or social media must allow the FSB uncoded access to these communications. The new regulation has been strongly criticized, not only because of the extension of the scope of surveillance but also because of the high costs of storing the data.[7] To comply with these regulations, ISPs have long preferred to tinker with existing equipment, as a representative of NORSI-TRANS, a market leader in SORM solutions, plainly stated at the KROS 8 vendor conference in May 2017: "Storing all Internet traffic for six months is not compatible with the economic realities of our country. The only practical solution for SORM is to use the existing equipment, with minimal extensions and a clear technical solution, with no cheating."[8]

Moreover, the SORM certification process is long and complex, as it involves a multitude of institutional actors, each in charge of certifying one or several of the system's components. These have to be tested according to a methodology that must first be validated by the FSB and the Ministry of Communications. The FSB then tests the installation using a simulator, and only then can the three-month certification process begin. In the absence of standardized, state-certified solutions, ISPs simply use existing infrastructures in anticipation of having to invest substantially again when the solutions are released.[9] Furthermore, legal responsibilities for data leakage or

misconfigurations are not clearly defined, and in fact, misconfigurations of SORM boxes are frequent, putting users' personal data at risk. The situation is particularly problematic because of the sensitive nature of the data, the variety of parties involved, and the lack of transparency in the process.

The requirements are tailored to ISPs' size and budget. Large ISPs are required to have SORMs, but smaller ones do not always install SORM boxes and instead respond to FSB requests on an ad hoc basis: "When necessary, the FSB calls or emails us and asks us to tcpdump the traffic for an IP address and share it via ftp."[10] Another long-used strategy, called "outSORMing," involves larger operators renting part of their SORM facilities. This strategy was standardized in 2022 and is now officially recommended by regulators.[11]

The period of relative flexibility allowing ISPs to avoid installing SORMs ended in January 2022, when the new bill, 333–34, on the Russian Tax Code[12] was proposed, introducing stricter penalties for noncompliance with SORM obligations and significantly increasing the cost of a license (which was multiplied by 183!). The package of documents that came with this bill included a study that not only revealed the figures of noncompliance with SORM obligations but also showed that the regulator was very aware of the tricks and circumvention techniques ISPs had used until then, as documented in our previous study (including closing down the company and reopening it with a new license [see Ermoshina et al. 2021]).

Table 2.1
Number of violations and fines per year, 2020–2022

Year	Number of violations	Fine
2020	954	243 fines (3 to 40,000 roubles, total sum 4,000,000 roubles)
2021	1,096	400 fines (3 to 100,000 roubles, total sum of 15,000,000 roubles)
2022 (1st half)	404	95 fines (3 to 100,000 roubles, total sum 3,000,000 roubles)

Source: https://sozd.duma.gov.ru/bill/254008-8 (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our Note on the Availability of Sources.")

CENSORSHIP PRACTICES AND TECHNOLOGIES

With regard to censorship, laws introducing the blocking of web content have been in place since 2012, when the RKN introduced a blacklist of banned web pages, and ISPs were co-opted under Russian jurisdiction to implement blocking (Sivetc 2020). The regulation was introduced in the wake of the 2011–2012 protests against election irregularities, which led to a reshaping of the digital media landscape. Its full implications became apparent, however, during the 2014 war in Ukraine, which became a testing ground for the Russian authorities' tightening of information control, including on annexed territories.

Our interviews show that as early as 2008–2009, ISPs received ad hoc instructions to block access to specific websites (gambling, pornography, drug dealing). The introduction of a centralized blacklist made it more difficult for ISPs to ignore such instructions and defend themselves in court. However, the precise requirements for blocking methods were not published until March 2018, with Law 149-FZ, Article 10, which defined the technical parameters of standardized "blocking pages" and a detailed set of technical recommendations for content filtering.

Freedom of expression advocates have severely criticized the blacklisting principle, as the "illegal" categories of content are vaguely defined, which leads to arbitrary decisions. In addition, the lack of judicial oversight facilitates the blacklisting of opposition websites on political grounds. These measures initially triggered a series of inventive initiatives that exploited the mechanism of the domain name system as a tool of protest, a famous example of which is the controversy surrounding Maksim Moshkow's online library, which was blocked in 2012. Moshkow, a Russian internet pioneer, had spearheaded major internet media projects (such as Gazeta.ru). Lib.ru, also known as the Maksim Moshkow Library, began operating in November 1994 and had become the largest and most comprehensive Russian-language electronic library.

Moshkow's response to the blocking of his library was to exploit a vulnerability in the web censorship mechanism, which made it possible to block the Ministry of Justice's main website. Since many ISPs automatically blocked all IP addresses from the "A-Record"[13] of a blacklisted Domain Name System

(DNS), Moshkow simply modified his website's A-Record to include the Ministry of Justice's IP address.[14] Following the same principle, in 2017, a number of DNS-based guerrilla attacks took place, blocking government bank and service sites and several DNS root servers. Activists used the RKN blacklist as a starting point: they bought some orphan domain names whose subscription had expired but were still listed and proceeded to modify their A-Records. Exploiting the same vulnerability, on May 6, 2018, developer and hacker Leonid Evdokimov wrote "Digital Resistance" in Morse code on the graphics of blocked ISPs (figure 2.1).

These actions have had consequences on the regulation and implementation of censorship and on the way blacklists are maintained. Before Evdokimov's action, in April 2018, the blacklist had 5,136 orphaned domain names that could be used to replicate a DNS attack, whereas by May 13, 2018 it had only 204 such domain names. Some of our respondents were critical of this side effect, arguing that these activists had ultimately helped RKN improve its management of internet censorship.

Despite the criticism of censorship by civil society actors and by some ISPs, Russian operators still have to implement these regulatory measures, which affect their business and, to some extent, challenge the values of openness that they might defend. Like SORM, solutions for blocking sites are hybrid objects and can take different forms: ISP homemade scripts, hardware solutions, cloud-based solutions, and DPI-type software. For a long time, ISPs had a choice of blocking options and methods. As the director of

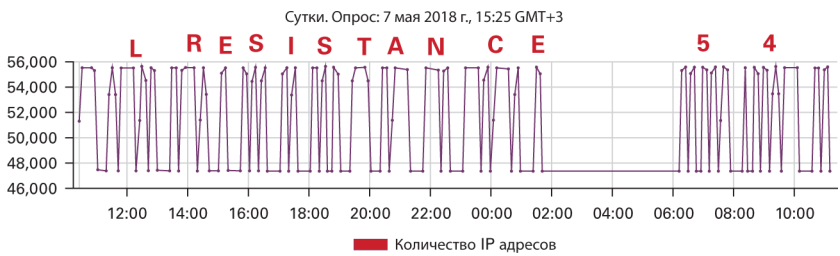

Figure 2.1

L. Evdokimov's Morse code message. *Source:* Independent host, expert, and activist for the free RuNet Phil Kulin's website (https://usher2.club/articles/msg-digitalresistance/).[15] The image is licensed under CC BY 4.0 (http://creativecommons.org/licenses/by/4.0/).

SkyDNS, a provider of traffic filtering solutions, pointed out, "There was a kind of technology vacuum—it was 'block as you like'. RKN couldn't advise ISPs on solutions for fear of falling foul of antitrust laws. But very soon there were several complaints from administrators of websites that had been blocked by mistake. . . . So they started to impose URL blocking. ISPs used to write their scripts themselves, but that's not very common anymore, because they risk being penalized."[16] Manual blocking became too difficult as the blacklist grew longer. In addition, ISPs often criticized this blocking list for its multiple inaccuracies and messy and misleading structure. An informal survey on an ISP forum[17] shows that the most-used methods were IP blocking and DPI.

Some ISPs sought to avoid large investments in filtering solutions. As a result, they did not block blacklisted sites consistently across different networks. In December 2016, to better control the blacklist's uniform application, RKN introduced another technical solution: the automatic system Revizor (AS Revizor).[18] Since the addition of Revizor, and due to its numerous malfunctions, the distribution of accountability for blocking errors has often proved controversial and problematic. As the president of the Internet Protection Society (OZI), Mikhail Klimarev, explains, "Suppose I'm a small ISP and I buy pre-filtered traffic from Rostelecom. I install Revizor, but something is not blocked. Who should pay the fine? Rostelecom or me? Rostelecom will say that I have configured the equipment incorrectly at the local level."[19] In this context of legal uncertainty and lack of specifications, a market for website-blocking solutions has cropped up. Unlike SORM manufacturers, which are mainly state contractors, most filtering equipment manufacturers (such as SkyDNS, Ruspromsoft, and Carbonsoft) previously offered commercial solutions for billing or parental control, although some companies (such as CyberFilter) were created specifically to meet RKN's requirements.

Our interviews with ISP staff and our analysis of forums allowed us to identify at least fourteen filtering solutions. For a long time, ISPs were confused by the market, which had two clear leaders, Carbon Reductor and SKAT. However, with the aim of stabilizing and standardizing blocking procedures, and supposedly as requested by ISPs, RKN conducted a massive trial of thirteen solutions (August 2017–March 2018), in which they benchmarked a series of parameters—for example, the proportion of "extremist"

and "other content" that had not been blocked. RKN then produced a ranking, the results of which were published on its website.[20]

Overall, the Russian censorship market shows a variety of trends and strategies to deal with regulators' requirements. Providers of filtering solutions compete fiercely to offer cheaper or more effective products, while large ISPs sometimes avoid blocking everything to attract more customers. Noncompliance can thus be presented as a commercial argument: manufacturers integrate features to simultaneously avoid being fined for having failed to block websites and minimize the impact of censorship on service quality. For example, when Telegram was blocked in 2018, collateral effects included blocks on Amazon, Google, and other popular websites. Carbon Reductor then offered ISPs a package that allowed them to provide their customers with access to platforms such as YouTube or Gmail without being detected by Revizor and fined by RKN.

Generally speaking, between 2012 and the end of 2018, censorship in Russia was not homogeneous, and ISPs developed ways to avoid complying with it, for both economic and technical reasons. Our interviews and analysis of the forums show that ISPs share a form of care for their networks and despise external interventions in their facilities, especially when they are imposed by the regulators, whom they consider incompetent. As a result, they have developed numerous circumvention strategies and "network tricks," which we have explored in more detail elsewhere (Ermoshina and Musiani 2021). One of these is the practice of selective censorship, which aims to deceive Revizor. The director of SkyDNS explained in an interview with us: "Some operators only apply censorship on a separate subnet they call a 'sandbox', where they install Revizor. And for their end-users, they fashion another network where there is little censorship, if any at all. For their part, network administrators or hosting services engage in technical tricks; for example, when Revizor IP addresses are identified, a blocking page is sent in response." Other strategies involve legal resistance. The OrderCom organization supports ISPs that oppose RKN-mandated decisions and fines, with some success: in 2016, 15 percent of decisions were overturned. ISPs also challenge what they consider to be errors resulting from the use of Revizor, providing certified true copies of blocked pages. However, out of

33,533 court decisions issued from 2012 to 2017, only forty-six cases were successfully overturned[21].

TSPUS AND THE CENTRALIZATION OF CONTROL

After a period of semifreedom for ISPs and Runet users, a new legal and technical apparatus was introduced in 2019 with the Runet Stability law (known to the general public as the Sovereign Runet law). ISPs and civil society actors were initially very skeptical of this law, as they doubted the government's technological ability to implement it effectively, and its opacity and complexity made it tricky to interpret. The law itself comprises around thirty regulatory acts that define "threats to the stability of the internet" or assign new responsibilities to Roskomnadzor, such as monitoring traffic exchange points (IXPs) or establishing an exhaustive list of cross-border cables (which had still not been completed at the end of 2022).

Analyzing the press reports and specialized Telegram channels, we found that experts involved in the "Free Runet" struggle perceived this law as a "regulator's dream" and saw a discrepancy between technological reality and legislative imagination: "The regulator sees Net regulation as some kind of central control point, a big screen in a bunker and a lot of people with headphones. They really think that's what it looks like. Its like watching a demiurge drawing their childhood dreams."[22] Other experts have linked the Sovereignty Law to the ineffective attempts to block Telegram in 2018 or to the 2016 Yarovaya Law, which was amended and largely watered down due to the lack of technical means to implement it. The principle of sovereignty "through infrastructure," according to which any information control instrument should be made in Russia came back to bite its promoters, as Russia did not produce technological solutions capable of complying with its own injunctions.

Despite its critics and sceptics, the 2019 law has nevertheless truly changed the ways in which the Runet is controlled, on several levels. First, RKN's perimeter of control over communication infrastructure has been radically expanded. In particular, the obligation to provide client information (including traffic volume, autonomous system numbers, owner contact

details, etc.) has been extended to internet exchange points (IXPs), which were still excluded from these provisions in November 2019 when we spoke to a representative of Piter IX, the St. Petersburg IXP. Since 2020, RKN has started to list operators with cross-border infrastructure.

As mentioned above, about fifteen companies offered traffic censorship and filtering solutions, seven of which had been tested and certified by RKN. ISPs were able to circumvent their obligations, as they were responsible for choosing, implementing, and maintaining their filtering and monitoring solutions. A range of technical and legal tricks allowed them to minimize control over networks and thus to defend a certain vision of the "free" Runet. Traffic measurements carried out in February to April 2018 using the OONI Probe software (developed by the Open Observatory of Network Interference) confirmed that ISPs enjoyed this relative freedom. With more than 200,000 measurements conducted using local testers, we provided evidence of inconsistencies in the blocking of websites on the official RKN blacklist (Valentovich and Ermoshina 2019).

However, the 2019 law recommends installing a single solution called TSPU (technical means for countering threats), which combines hardware with DPI-type software. While the DPI solutions are manufactured in Russia (mainly by RDP.ru, owned by Rostelecom, or by Carbonsoft), the hardware part of the TSPU is not entirely Russian. Commonly used solutions are produced by Intel, Huawei, or Supermicro, and network cards are manufactured by Mellanox or Intel. The TSPU is not a single box; it is an assemblage of devices and software solutions recommended by RKN (figure 2.2). An example of a TSPU assemblage could be an EcoDPI filter manufactured by RDP, a Huawei server, an Eltex commutator switch, a Silicom switch, a Fiber Trade optical module, and "Kontinent" encryption software. To this day, there is no certification for the assembly work.

TSPUs are installed by FSB- and RKN-authorized agents and are usually located in locked cages, so ISPs have limited access to them. Their purchase and installation are paid for by the state, but maintenance remains at the ISP's expense. The law provides for a fine for violations of TSPUs' installation, operation, and updating rules of up to 500,000 roubles (about 6,400 euros). In the event of a breakdown, the ISP is held responsible and

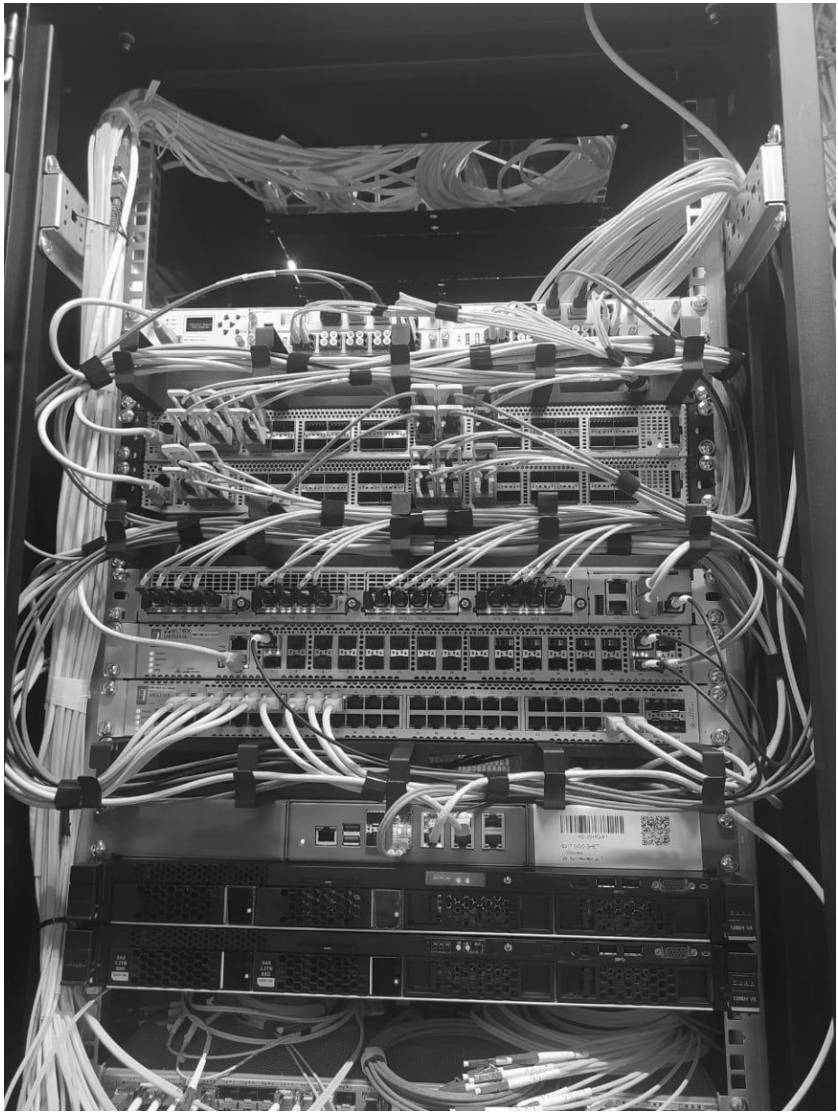

Figure 2.2
TSPU installation for 40Gb/sec. *Source:* Personal archive of Mikhail Klimarev.

penalized—even if it is due to RKN's intervention. This limits ISPs' room to maneuver and curtails their ability to avoid filtering traffic.

TSPUs can be used to block certain VPNs (ExpressVPN, RedShield, NordVPN, etc.) and to slow down certain services, which Twitter experienced in 2021. In autumn 2021, they were used for massive extrajudicial blockings, which included the online shopping service Avito.ru, the servers of the game World of Tanks, GoogleDocs, Apple Music, Recaptcha, Telegra.ph, and so on. These services were blocked by the TSPU during the parliamentary elections to stop the distribution of Aleksei Navalny's SmartVote application, which called for citizens to vote for opposition candidates. These services were not included in the register of blocked sites and were therefore blocked without a court decision. Moreover, the introduction of the TSPU has affected the transparency of censorship. While the blacklist allows for traceability and some degree of citizen monitoring of censorship and its application (especially by the NGO Roskomsvoboda), there is to date no list of sites blocked by TSPUs.[23]

According to the Main Radio Frequency Centre director, Sergey Tyomniy, small providers with speeds of up to 10 Gbit/second are not required by law to install a TSPU.[24] However, while the large number of small providers with relatively low bandwidth is a distinctive feature of the Russian ISP market, their combined traffic accounts for only 5 percent of all traffic in the country.[25] In their case, the onus falls on operators upstream from them to filter contents. Yet even some large operators, such as MTS, consider TSPUs to be a "threat to the connectivity, stability and proper functioning of the Runet."[26] ISPs are thus developing new stratagems, especially at the legal level. During RKN's forced census of ISPs in December 2021, Dmitry Galushko, a lawyer who specializes in defending ISPs, advised on his Telegram channel that bandwidth should be declared at less than 10 Gbit/second.[27] As for technological resistance, lately it has shifted to the development of traffic obfuscation protocols (Shadowsocks, OBFS4, Cloak) and new generations of "multiprotocol" VPNs that mask traffic (AmnesiaVPN and Roskomsvoboda's CensorTracker).

Another workaround proposed by ISPs is to create "internet consumer cooperatives" to avoid the need to install TSPUs and SORM.[28] This confirms

the intentions that representatives of several small ISPs in St. Petersburg had already mentioned in the interviews we conducted with them in 2019, when they spoke of their strategies in case of an actual activation of "Tcheburnet" (a word used by free RuNet advocates to describe the Sovereign Runet project, composed from the name *tcheburashka*, a character from a Soviet cartoon, a mythical animal that exists only in Russia, and "net" for "internet"): "We're going to go back to local networks, but also maybe experiment with administrative bricolage like cooperatives, associations or Internet enthusiasts' clubs, to share connectivity with very small circles of family, friends or loyal customers. But I imagine that, in general, if their Sovereign Runet plan really works, only a minority will be able to afford access to the global Internet, a minority that has the necessary technical skills and equipment."[29]

THE EFFECTS OF RUSSIA'S INVASION OF UKRAINE ON THE INFORMATION CONTROL INFRASTRUCTURE

Russia's invasion of Ukraine in February 2022 led to an intensification of measures claimed to "combat external threats" (as defined by the 2019 law: threat to stability, threat to connectivity, threat to security). Our analysis of press reports and specialized Telegram channels reveals the rise of alarmist discourse about a potential disconnection of the Runet, tightening controls on it, and the acceleration of the "autonomous" Runet project. Inspections were carried out at ISP offices between February and August 2022. On June 8, 2022, a draft amendment to Law 333, Part 2 of the Tax Code, was proposed, introducing fines for the lack of a SORM installation; the amount of the fine depends on the ISP's annual profits but should in all cases be at least 1 million roubles (approximately 12,800 euros).

Tests were conducted in August 2022 to check Russian ISPs' ability to respond to attacks on routing carried out via the Border Gateway Protocol (BGP). Further trials were conducted in 2022 to test DNS servers located within the country. Several new types of satellites (e.g., Gonets M and Skif D) have recently been launched to provide satellite connectivity and defense for radio frequencies. Another measure to implement the plan for the Runet's technological autonomy and digital sovereignty is the development of Russia's own

certification authorities.[30] Although this was announced in September 2022, on November 22, 2022, Sberbank, the Russian savings bank, purchased a certificate from the Greek certification authority Harica,[31] showing that, despite the rhetoric about sovereignty and despite the international sanctions against Russia, the Russian central bank continues to use European certificates. Moreover, the country's various administrative services have not synchronized their transition to certificates that are made in Russia. In late October 2022, services such as Nalog.ru[32] (taxes), Gosuslugi,[33] and Revizor were still using certificates issued by Let's Encrypt, a Californian certification authority.

It turns out that the Sovereign Runet project is itself dependent on foreign solutions—and especially American and Chinese ones—even for tools like Revizor. While it has diminishing points of connection and infrastructural dependence, these remain embedded in its foundation. Paradoxically, the context of international sanctions calls into question the realization of the Sovereign Runet project. Our analyses of the technical documentation for "special" communications solutions (for the Russian military) developed by Protei ST (a Russian manufacturer of DPI, SORM, and other filtering, monitoring, billing, and teleconferencing devices and software solutions) show a dependency on Intel processors, which can no longer be exported to Russia.

The sanctions even affected long-term and seemingly sustainable collaborations. A noteworthy example of this is relationships with Taiwanese manufacturers involved in the production of Baikal processors—which, ironically, were presented as being made in Russia. However, despite international sanctions on dual-use electronic components (those that can be used for military purposes), "parallel" import schemes have been set up at several levels. Not only have individual ISPs taken this initiative to continue to find Cisco, Juniper, or Mikrotik solutions, mostly on eBay and via Kazakhstan, SORM manufacturers have gone about it even more systematically and openly, as they publicly announced at the KROS 2022 conference. Parallel imports, in turn, impact the costs of SORM solutions, which have risen by 20 percent, and manufacturing times, which have increased to three to four weeks.[34]

The obligation to implement SORM and filtering solutions was extended to the occupied territories of Ukraine (Zaporizhzhia and the occupied regions of Luhansk and Donetsk), but their actual implementation

was pushed back to 2026 (according to Laws 5, 6, 7, and 8 FZ, which allow for a transition period). However, despite the lack of a legal framework and a standardized technological procedure, in November 2022, ISPs in the occupied regions of Ukraine received an order from the local Ministries of Communication requiring ISPs to block, slow down or "partially degrade" services for Google, YouTube, Zoom, Facebook, Twitter, Viber, and Instagram and to send reports with evidence to RKN. Instructions were sent to explain how to set up these blocks and verify their effectiveness. The licenses of ISPs that refused to block or slow down these services may be withdrawn.

Russian manufacturers of SORM and DPI boxes are exploring new markets, especially in Asia and Africa: Uzbekistan, Tajikistan, Kazakhstan, Kyrgyzstan, Iran, and Afghanistan (where Vas Expert and Protei solutions are sold and installed). Russia is thus exporting its vision of sovereignty through infrastructure, while antiwar activists, journalists, and developers are going into exile in these same regions. However, the flight of technical experts is also a factor that impacts the SORM and DPI markets.

Finally, as we have shown above, the ISP market is undergoing rapid centralization. This is happening primarily at the infrastructure level, with "outsourcing" or "upstream filtering" schemes that render small ISPs dependent on larger ones, from whom they rent infrastructure parts or buy traffic in transit. It is also taking place at the legal level, as the decline in the number of licenses issued illustrates (figure 2.3). The cost of entering the market is now 1.5 million roubles for licenses that include SORM.

CONCLUSION

A thriving market for censorship and surveillance has opened up in recent years for Russian providers of hardware and software solutions for blocking and filtering traffic. This chapter describes some of the controversial technologies at the heart of this market and shows the ecosystem of actors and socio-technical processes at work around them. It also shows how central this market's development is to the implementation of the coercive, authoritarian, and centralizing strategy that underpins the Russian state's conception of digital sovereignty.

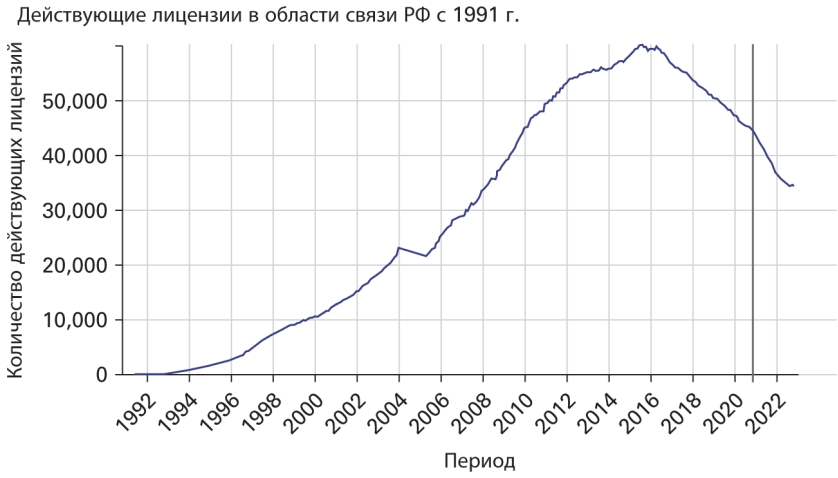

Figure 2.3

Active licenses issued in the telecommunications sector of the Russian Federation since 1991. *Source:* https://ifreedomlab.net/connectivity-rating/licenses-russia/.

A previous study of this surveillance and censorship technologies market, running from 2012 to 2019 (Ermoshina et al. 2022), showed the distributed and sometimes inconsistent nature of the Russian model of information control, which afforded ISPs some room to maneuver. Recent developments, especially relating to TSPUs, suggest that this is not as clearcut now as it was then. However, despite the considerable legal and technical adjustments that followed the introduction of TSPUs, state control over Russian networks remains incomplete. As RKN director Andrei Lipov pointed out, while 100 percent of mobile operators have installed TSPUs, only 60 percent of landline internet service providers are equipped with them. Serguey Khutortsev, director of the Centre for Observation of Communication Networks, spoke of 860 "TSPU nodes" by 2022 and promised 1,360 by 2023.[35] However, in a survey of ISPs conducted on December 22, 2021, only 19 percent of the respondents had installed a TSPU, 3 percent had signed the implementation plan, 48 percent had not yet done so, 14 percent were not going to do so, and 21 percent expressed their intention to "opt for a 'grey' strategy."[36]

As this example and many others presented throughout this chapter show, studies of this market continue to produce valid illustrations of the

diversity of constraints exerted on the Russian internet. An understanding of these constraints is in turn essential if we are to grasp the many forms of resistance, evasion, and circumvention that have developed in response to them. In this ecosystem, economic rationality is strictly linked to the interpretation of techno-legal norms and to the players' ability to navigate or oppose these norms.

NOTES

1. ISPs themselves offer different ways of analyzing the market. For instance, a study by a group of ISP employees in December 2017 found that there were 3,940 active ISPs (https://habr.com/en/post/345258/), whereas according to RKN, only 3,461 ISPs reported to the regulator in 2018 (https://rkn.gov.ru/news/rsoc/news70316.htm). (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
2. This index is no longer updated by the Internet Protection Society (OZI, a Russian digital freedom NGO).
3. According to OZI data.
4. Open Observatory of Network Interference, an open-source project monitoring internet censorship worldwide, supported by a network of volunteers (https://explorer.ooni.org/).
5. See, for example, the reaction of the Electronic Frontier Foundation to the Yarovaya law: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.
6. On March 28, 2022, the regulators made another change to the law, allowing streaming services and online radio and television channels not to store traffic.
7. According to official government figures published on December 8, 2022, "The cost of SORM equipment depends on bandwidth and connection speed. For example, for a speed of 0–3 Gbit/second the cost of the equipment varies between 2 and 4.5 million roubles, for 3–6 Gbit/second—between 3 and 6 million rubles, for 6–10 Gbit/second—between 4 and 7.5 million roubles. In addition, these prices include implementation and configuration work, data storage for 3 years and warranty for 1 year" (https://sozd.duma.gov.ru/bill/254008-8). (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
8. Telegram channel ZaTelekom, message published on May 25, 2017 at 10:04 (https://t.me/zatelecom/192).
9. Intervention by an ISP on the Nag.ru forum, November 4, 2015.
10. Interview with Aleks Lomakin, director of the Alternative ISPs Association, August 28, 2018.
11. See the Duma's website: https://sozd.duma.gov.ru/bill/254008-8. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")

12. "Tax Code of the Russian Federation (Part Two)" dated August 5, 2000, N 117-FZ (as amended on December 28, 2024, as amended on January 1, 2025), available (in Russian language only) at http://www.consultant.ru/document/cons_doc_LAW_28165/a3cd0bcff028f127a00fa0aa61842f4ff13ffafb/.
13. The A-Record serves to associate IP addresses with a domain name.
14. https://tjournal.ru/46700-moshkov-minjust (Tjournal was blocked in Russia in March 2022 and it deleted its website; 2023 and 2024 snapshots retrieved on the Wayback Machine report a 404 error. Please refer to our Note on the Availability of Sources.")
15. This website kept a graphical record of blocked IP addresses for a long time. It became a privileged source of data for the media and regulators and was frequently consulted, including by Roskomnadzor agents. Hence Leonid Evdokimov's choice to display his message on this graph.
16. Interview of November 22, 2018.
17. https://forum.nag.ru/index.php?/topic/79886-blokirovka-saytov-provayderami/
18. An investigation carried out by ValdikSS, a hacker and activist associated with Roskomsvoboda who conducted a detailed analysis of the Revizor AS box, showed that the tender for its development was won by MFI-Soft, a company also involved in the production of SORM systems. Production costs for Revizor have been estimated at 84 million roubles (about US$1.14 million), but the state is supplying the devices to ISPs (see https://habr.com/ru/post/282087/).
19. Interview with Mikhail Klimarev, September 14, 2018.
20. https://rkn.gov.ru/communication/p922/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
21. See the study conducted by digital law and policy specialist Serguey Hovyadinov (https://rankingdigitalrights.org/2018/07/19/russia-telcos-fail-to-respect-users-rights/).
22. Interview with Phil Kulin on the Fontanka website, May 30, 2019 (https://www.fontanka.ru/2019/05/30/058/).
23. https://roskomsvoboda.org/ru/cards/card/tspu-blokrovki-runet/
24. Video of Sergej Tëmnij's presentation at the MUSE Operators Conference on September 22, 2022, https://t.me/ordercomru/3588.
25. According to the Interfax news agency, June 15, 2021, https://www.interfax.ru/russia/772325.
26. *Kommersant*, July 29, 2021, https://www.kommersant.ru/doc/4919761?query=%D0%B4%D0%BC%D0%B8%D1%82%D1%80%D0%B8%D0%B9%20%D0%B3%D0%B0%D0%BB%D1%83%D1%88%D0%BA%D0%BE.
27. https://t.me/ordercomru/2794
28. See discussions on the Nag.ru forum: https://forum.nag.ru/index.php?/topic/146324-uslugi-svyazi-bez-sorm-revizor-i-tp/page/3/#comment-1599314

29. Interview with D., on 14 November 2019.

30. An SSL certificate is a digital certificate that is associated with a domain name or URL. It establishes the link between a website and its owner with certainty and thus makes it possible to secure electronic exchanges. Certificates are issued by certification authorities, whose reputation and renown depend on how long they have been operational and agreements with the most popular OS and browsers. In the context of the transition to the sovereign Runet, the development of Russian certification authorities would be a major decision in terms of infrastructure.

31. https://crt.sh/?id=8043006484

32. https://t.me/zatelecom/24122

33. https://t.me/zatelecom/24122

34. SORM manufacturers' conference at KROS 2022 (https://youtu.be/nZmbsYTfCNM).

35. See Serguey Khutortsev's presentation video at the 'Spektr-Forum 2022' cybersecurity conference (https://t.me/ordercomru/3811).

36. Telegram channel of OrderCom, a legal firm specializing in defending the interests of ISPs against RKN administrative proceedings (https://t.me/ordercomru/2822).

REFERENCES

Callon, Michel. 2013. "Qu'est-ce qu'un Agencement Marchand?" In *Sociologie des agencements marchands. Textes choisis*, edited by Madeleine Akrich, Sophie Dubuisson-Quellier, Catherine Grandclément, Antoine Hennion, Bruno Latour, Alexandre Mallard, Cécile Méadel, Fabian Muniesa, Vololona Rabeharisoa, and Michel Callon. Presses des Mines.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. Yale University Press.

Ermoshina, Ksenia, Benjamin Loveluck, and Francesca Musiani. 2021. "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia." *Journal of Information Technology and Politics* 19 (1): 18–33.

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

Ermoshina, Ksenia, and Francesca Musiani. 2021. "Ruser sur les Réseaux: Résistances 'par l'Infrastructure' des Fournisseurs d'Accès Internet en Russie." *Quaderni* (103): 53–70.

Lessig, Lawrence. 2006. *Code. Version 2.0*. Basic Books.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2016. *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan.

Schneier, Bruce. 2003. *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Copernicus Books.

Sivetc, Liudmila. 2020. "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges." In *Freedom of Expression in Russia's New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari. Routledge.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43 (3): 377–391.

Valentovich, Igor, and Ksenia Ermoshina. 2019. "Measuring Internet Censorship in Disputed Areas: An Examination of Online Media Filtering in Russia and Crimea During the 2018 Presidential Elections." Open Technology Foundation report. https://public.opentech.fund/documents/Measuring_Internet_Censorship_in_Disputed_Areas_Crimea_Russia_ICFP.pdf.

Winseck, Dwayne. 2017. "The Geopolitical Economy of the Internet Infrastructure." *Journal of Information Policy* 7: 228–267.

3 DISCIPLINING THE DIGITAL PUBLIC SPACE: THE YANDEX.NEWS AGGREGATOR

Françoise Daucé and Benjamin Loveluck

Since Russia's military attack on Ukraine in February 2022, surveillance and propaganda have been at the heart of a war in which controlling public opinion is a strategic target. In this context, information flows, which were already tightly controlled by repressive legislation, institutions, and technical devices before the war broke out (see chapters 1 and 2), are increasingly restricted. Large digital companies that play a role in broadcasting online content (media, social networks, blog platforms, and news aggregators) are especially closely monitored. This is the case of the Russian digital industry's flagship, Yandex, whose search engine and news aggregator have been a focus of increasingly close attention from Russian leaders since the early 2010s. Through controversies, legal constraints, and technical limitations, Yandex.Novosti—Yandex.News, the Russian equivalent of Google News, which was launched in 2004[1]—saw its news service increasingly regulated until it eventually lost all autonomy. After the war broke out, this process of political control reached its conclusion with the transfer of Yandex.News to the VKontakte (VK) platform (the Russian equivalent of Facebook), which is itself owned by the Gazprom-Media group, under the direct supervision of Vladimir Putin's presidential administration.[2] The sale of the service to VK was the final stage in a dynamic of intensifying supervision over the aggregator, which began in the early 2010s.

Russia is one of the few countries in the world where Google has never really dominated the online search industry. Yandex (short for Yet Another iNDEX) is the name Arkady Volozh and Ilya Segalovich gave to the Russian-language full-text search technologies they developed at Comptek

International. The Yandex.ru search engine was launched in 1997—around the same time as Google but in a very different economic context—and contextual advertising was added to it the following year. In 2000, Yandex became a privately held global company incorporated in the Netherlands, and it has been listed on the NASDAQ since 2011. Until 2022, it was Russia's largest technology company, with its diversified revenue streams—such as taxi services, food delivery, video games, and music streaming—having more than tripled in five years, from 60 billion roubles in 2015 to 218 billion roubles in 2020.[3] Yandex has long enjoyed a certain degree of autonomy, and its founders have even expressed political disagreement with the Kremlin at various times. However, as a champion of the national economy and a key player in the organization of information, the company has been under intense scrutiny. This was the case, for instance, after the 2011–2012 election fraud protests and then during the annexation of Crimea in 2014, which was a more general turning point for Russia, with a considerable increase in government control over the media, the internet, and civil society (Oates 2013; Soldatov and Borogan 2015; Wijermars and Lehtisaari 2020). In this context, the Yandex.News aggregator, in particular, has been targeted.

We will begin this chapter by outlining the general workings of a news aggregator and the vulnerabilities that have been identified in these systems. Initially, search engines and recommendation systems were designed as tools to manage the diversity of online content. However, these platforms are also strategically positioned in society and have become key intermediaries for channeling information to citizens, thus exercising a form of power through their ability to shape people's perception of social reality. We have used Google News, which most readers are likely familiar with, as a model to outline these aggregators' role and responsibilities. The issues raised by automated news recommendation are part of a broader set of questions about search engines and social media platforms' role in ensuring information diversity (Helberger 2019) and their ability to shape the public sphere through "algorithmic gatekeeping" (Napoli 2014; Nechushtai and Lewis 2019). News curation algorithms are often criticized for being opaque and difficult to explain (Pasquale 2015; Saurwein et al. 2015) and, although their creators have long claimed to be neutral to some extent, issues related

to news prioritization have proved to be not only technical and commercial but also political.

Yandex.News partly falls under this type of criticism. In the second part of this chapter we will discuss the particularities of its system and the debates it raised in the 2010s. Controversies surrounding socio-technical systems have been found to be ideal tools for investigating political issues (Latour 2005; Marres 2007). In Russia, the attention garnered by the aggregator and the controversies surrounding it shed light on this algorithmic black box's role as a contested producer of meaning (Bucher 2016) and a complement to other sources of information such as television (Alyukov 2021). Until 2022, Yandex (unlike Google) consistently displayed five news items selected by the aggregator on its homepage, which guaranteed a large audience. In 2016, laws targeting news aggregators forced Yandex to restrict the results displayed on its news page (Daucé 2017). Three rival interpretations of what constitutes "good" aggregation results emerged: Yandex's conception of it as the "objective" result of its algorithms' operations; the authorities' counterpoint accusing Yandex.News of promoting "unpatriotic," "fake," or problematic news; and finally, the definitions put forward by journalists, editors, and search engine optimization (SEO) professionals who criticize the platform based on their sense of what is considered "newsworthy."

In the third part of this chapter, we have complemented this controversy-based approach with an audit of the algorithm itself,[4] carried out using reverse engineering methods (Kitchin 2016; Seaver 2019). This shows the gap between the diversity of Russian online media resources and the narrowness of the media samples represented on Yandex.News rankings, which are exclusively dominated by a set of fourteen media outlets (news agencies, state-funded media, and private publications that are "loyal" to the government) (Daucé and Loveluck 2021). When the open war against Ukraine broke out in February 2022, it became even more obvious that the algorithm was being used to push warmongering narratives. This led to its transfer to direct state control.

The story of Yandex provides an extraordinary case study of "governance by algorithms" (Musiani 2013; Just and Latzer 2017; see also Gillespie 2018) and furthers our understanding of how news recommendation systems can be vulnerable to bias (Kulshrestha et al. 2019; Trielli and Diakopoulos

2019) or to subtle or less subtle forms of political filtering (Jiang 2014; Dovbysh et al. 2022). The case of Yandex also allows us to understand the peculiarities of Russian digital policy as an assertion of "digital sovereignty" (Nocetti 2015; Musiani et al. 2019). It uncovers the new "codes of conduct"—involving both computer code and legal code (Lessig 1999)—that can be implemented in the networked public spheres of contemporary societies. It sheds light both on the strategic nature of search platforms and algorithms today (Pasquale 2015) and on the ways in which the Russian government has sought to assert its dominance over internet governance as a dimension of "information security" (Maréchal 2017). Finally, it illustrates how digital infrastructures can be reined in to indirectly regulate online speech (Sivetc, 2019).

ALGORITHMIC GATEKEEPING IN DIGITAL MEDIA ECOSYSTEMS: CONTEXT AND IMPLICATIONS

The Yandex.News aggregator is an automated news recommendation system, the Russian counterpart to the Google News aggregator. Initially, the service aimed to provide an overview of news trends, presenting its users with "clusters" of related articles. In the case of Google News, languages and country editions were developed, and features such as email alerts, personalization, and news article recommendations were added. By 2022, its service indexed tens of thousands of news sites around the world and was interwoven with Google's web search engine.

In general, recommendation systems cover a wide range of applications, from e-commerce to music, movies, and news (Jannach et al. 2011; Ricci et al. 2015). They involve automated filtering, which usually relies on a set of parameters, as well as user actions (backlinks, clicks, searches, choices, preferences, etc.) to identify a selection of information that is likely to be of interest to any given user or their peers. More specifically, news recommendation systems may be based primarily on an analysis of the content itself (the nature of publications, including their "freshness," for example) or on the activity generated by this content (click-through rates, social media engagement metrics such as likes and shares, etc.), on forms of "collaborative

filtering" and the detection of common themes of interest in a given community, or even on user preferences—in which case the aggregated news is personalized based on the behavioral data collected (Karimi et al. 2018). In general, news recommendation systems combine these approaches to varying degrees in ways that also depend on how trackable their users are (for example, whether they are logged in or otherwise identified as a unique user).

Aside from relevance metrics and their combination with the selection of content in which other people have expressed an interest, news article recommendations also require a *qualitative* selection process. This aspect is more difficult to define, as it involves searching for items that are not necessarily within the user's immediate reach or direct focus. One of the key quality metrics is drawn from the diversity of news that an aggregator can provide. While this criterion can partly be assessed in terms of user satisfaction, it also points to much broader concerns surrounding the media's role and responsibility as a central institution of democracy, which is supposed to properly inform citizens and provide a diverse public forum for debating ideas and opinions (Helberger 2019).

Furthermore, key parameters of this diversity include aspects such as the variety of topics covered, as well as the diversity of editorial policies, ideological perspectives, narrative genres, and so on (Helberger et al. 2018). There are related concerns regarding automated recommendation systems' ability to be biased against certain types of content and to underrepresent them in their results (Kulshrestha et al. 2019). Even when they appear diverse overall, they may leave out key topics (a major corruption scandal, for instance) or lend some topics comparatively less weight (politics versus sports, for example), or editorial choices may downplay their importance (including by focusing on less crucial but more entertaining aspects of a story).

From the outset, the "politics of search engines" have been presented as decisive factors in the shaping of the public sphere (Introna and Nissenbaum 2000). News aggregators, which offer visibility to "automatically" selected information, have likewise come under intense scrutiny, due to their increasingly central role and growing power within media ecosystems. Publishers have become increasingly dependent on digital platforms (Nielsen and Ganter 2018), as these intermediaries have themselves become gatekeepers alongside

journalists (Napoli 2014), leveraging user behavior to shape an overall picture of "curated information flows" (Thorson and Wells 2015, 2016).

Google and Yandex both present their services as "neutral," but these claims to objectivity have drawn criticism. Google's search engines are suspected of trapping users in "filter bubbles" and "echo chambers" (Pariser 2011; Bozdag 2013). These services are accused of undermining the public sphere by keeping certain types of information or alternative perspectives out of sight and sometimes reinforcing their users' prejudices or biases. Search algorithms and automated recommendation systems have also been accused of promoting outrage and conspiracy theories, with YouTube's algorithm, for example, being described as "the great radicalizer."[5] However, the veracity of these claims is difficult to assess precisely (Flaxman et al. 2016; Bruns 2019), especially in the case of search engines (which, for example, have actually been shown to increase information diversity; see [Fletcher and Nielsen 2018]). In the case of Google News, even its personalization features do not seem to reduce information diversity (Haim et al. 2018). Although individual filter bubbles may be difficult to assess empirically, "algorithmic news curation still represents a concern for source diversity since it can concentrate societal attention on a narrow range of privileged outlets" (Trielli and Diakopoulos 2019, 3).

DISCIPLINING THE ALGORITHM TO CONTROL THE NEWS

Before examining the case of Yandex.News, it should be noted that the relationship between Google News and news organizations is likewise complex and has also generated controversy. Aggregators offer visibility for news content in exchange for access to publications, and although Google News is a traffic provider (Calzada and Gil 2020), it can also be seen as a media outlet in its own right, as it benefits from the content provided by news media (headlines and text excerpts).[6] Beyond copyright and business model issues, news aggregators affect the ways in which news is published. Content must meet the criteria their algorithms put forward in terms of relevance, freshness, update frequency, metadata, backlinks, mobile compatibility, and so on. Writers deploy search engine optimization (SEO) strategies to

ensure that their content is effectively referenced and promoted, constantly monitoring audience analytics to understand what works and what does not, which stories gain traction and which do not. In order to be "picked up" by platforms, news websites need to adapt their content and publishing strategies to the amount of traffic (and therefore advertising revenue) they attract. This, of course, has a direct impact on the work of journalists and on conventional conceptions of newsworthiness or noteworthiness (Boyer 2013; Belair-Gagnon and Holton 2018; Diakopoulos 2019a).

The algorithms these platforms develop can thus be argued to act as an "invisible hand" that designates relevant topics and pushes selected news outlets to the forefront by virtue of sometimes unfathomable criteria. It thus affects the very core of journalism, as professionals adjust the form and nature of the content they publish to fit these bills (Brake 2017; Christin 2020). The role algorithms play in sorting news, directing visibility and attention, framing issues, and setting agendas is increasingly being called into question, especially as "trending algorithms may reflect back what is popular while raising awareness among an even broader set of people, in effect helping to conjure an interested public around an issue. On the other hand, questions may reasonably be raised when a newsfeed fails to notify its users of important civil unrest while continuing to amuse and divert attention to popular events" (Diakopoulos 2019a, 183). Moreover, the impact of search engines on user choices and preferences can be far-reaching. In a series of controlled experiments, it has even been shown to sway undecided voters (Epstein and Robertson 2015).

Given its central role in news dissemination today, Google is regularly suspected of giving visibility to illegitimate sources (such as the controversial image forum 4chan after the 2017 Las Vegas shooting[7]) or of being politically biased in favor of certain types of news sources (deemed "left-wing" by their critics) (Diakopoulos 2019b). It has also been argued that the traffic referenced by search engines appears to mainly benefit a small number of already highly visible media outlets, thus entrenching existing media hierarchies and undermining claims to greater pluralism (Hindman 2008, 2018; Hong and Kim 2018). This may also be the case with news aggregation: it has been shown that only five news organizations account for almost half of all

news recommended on Google News and that mainstream media are prevalent in recommendations (Nechushtai and Lewis 2019 see also Bui, 2010).

In the Russian political context, the issues raised by the Yandex.News aggregator, while similar in nature, are even more acute. How can aggregation bias be identified in an oppressive political context? Can results be manipulated for political reasons, either by directly interfering with them or by misleading the algorithm? How has political control over the prioritization of news gradually been developed? How can a manipulated tool be criticized or circumvented in a context where political freedoms have disappeared? In order to answer these questions, we studied the controversies that arise around the aggregator, which in turn enabled us to gain an understanding of the political burdens this service bears.

YANDEX.NEWS IN POLITICAL CONTROVERSIES IN RUSSIA

Since 2004, Yandex.News presented a selection of topics and articles that were intended to reflect the issues most widely covered in Russian media at any given time. The service was developed by a team of computer scientists and linguists working on news recognition and extraction software. At its launch, Yandex.News claimed that the algorithm worked "without human intervention" to gather news published by partner media into topics through the algorithm's "clustering" function. The robot analyzed keywords and facts and grouped them into topics using three main criteria: citation rate, novelty, and degree of information.[8]

Lev Gershenzon[9] led the Yandex.News development team from 2004, when Yandex employed only about two hundred people in total. At the time, Google News already existed, but according to Gershenzon, "At Yandex, we were better and more attractive to users. That's why we put the Top 5 on the main page, which Google never tried to do."[10] Until September 2022, a box with five news items was permanently featured on the Yandex search engine's homepage, thus guaranteeing a massive daily audience for this small selection of news items and driving considerable traffic to the featured publications (figure 3.1).

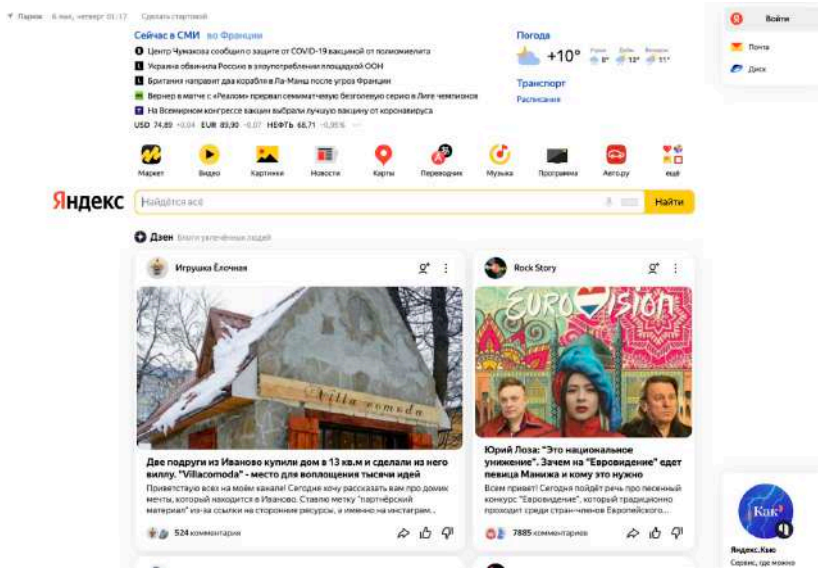

Figure 3.1
Yandex homepage, screenshot, March 11, 2021. The "Top 5" news items retrieved from Yandex.News are at the top, just above the search bar.

Although Google also offers a selection of "Top Stories" in its search engine, these are linked to specific searches and only appear with the rest of the results after a query has been entered. The Top 5 is therefore key to understanding how the whole Yandex platform works as a news recommendation system. Yandex Chief Technology Officer Grigori Bakunov commented in 2017 that the "daily audience of the five news items that appear on the Yandex homepage is the same as the homepage's—that is, about 20 million people, depending on the day. Six million people visit the Yandex.News page daily."[11]

YANDEX.NEWS AT THE HEART OF POLITICAL CONTROL

According to Russian journalists, until the early 2010s "Yandex and the Kremlin represented two different Russias with little overlap."[12] Yandex cofounder Ilya Segalovich and some of his colleagues actively participated in the election

fraud protests in 2011 and 2012. Since then, however, the Russian government has applied increased pressure on the company (Oates 2013; Soldatov and Borogan 2015). Yandex is seen as a key national asset that ensures the country a degree of independence from foreign (and especially US) web companies. Its activities are controlled by a web of political, legal, technical, and economic constraints (Vendil Pallin 2017). In 2009, Yandex's owners sold a "golden share" (priority share) to Sberbank, the state-controlled Russian savings bank, thus giving the state de facto veto power over strategic issues.[13] Although this move attracted criticism, relative loyalty to the state has also brought the company some benefits. Yandex won an antitrust dispute against Google and has benefited from the mandatory preinstallation of Russian software on smartphones since 2021.[14]

Multiple controversies emerged, however, around the aggregator after 2012, which gradually ended the belief in its objectivity. The year 2012 was a decisive time for freedom of expression and internet regulation in Russia (Lonkila et al. 2020). The authorities responded violently to the waves of electoral fraud protests—which followed the Arab Spring—and launched a gradual tightening of regulations on public speech (Denisova 2017). Since then, Yandex.News has been the specific target of various political challenges, new legislation, and editorial constraints on independent media. Among those measures, one of the most significant was the establishment by law in 2012 of a blacklist of censored websites, which ISPs have since been required to prevent access to. It originally targeted illegal gambling, child pornography, information related to the production and distribution of drugs, and information encouraging suicide. However, the notion of "prohibited information" was later extended to "incitement to illegal actions" and "promotion of extremism," and was used in 2014 to block independent sites such as Grani.ru, Kasparov.ru, and opposition leader Aleksei Navalny's blog on LiveJournal. The blacklist is managed and regularly updated by the government's communication- and media-monitoring agency, Roskomnadzor, which also licenses mass media in Russia. Blocked websites thus started disappearing from Yandex.News rankings.

The government's grip on the public sphere intensified again in 2014, during the conflict with Ukraine and the occupation of Crimea. The

authorities launched media campaigns involving both the state media and E. Prigozhin's now infamous "troll factory," to fuel support for pro-Russian views and undermine the credibility of pro-Ukrainian voices (Fedor 2015; Mejias and Vokuev 2017). Those were the days of Snowden's revelations regarding US intelligence agencies' internet surveillance operations, and Putin leveraged this to claim that Yandex was created under Western influence and that the internet in general was a "special CIA project." The authorities especially targeted Yandex.News and accused it of being biased for having given visibility to information that deviated from official narratives. Drawing comparisons with the Kyiv protests that led to regime change in Ukraine, the pro-Kremlin website *Pravda.ru* asked, "Is Yandex stirring up a 'Maidan' in Russia?"[15] The newspaper took exception to the headlines chosen by the aggregator and claimed that it was necessary to legally regulate its activity. In May 2014, Kremlin spokesman Dmitry Peskov announced that Yandex.News had to be registered as a mass media outlet, which would put it under the control of Roskomnadzor.

A 2016 law specifically targeting Yandex.News extended state control to news aggregators. Those that drew over a million daily visitors became legally responsible for the results they published and henceforth risked heavy fines for violations, unless the media outlets they selected their news from were officially registered with Roskomnadzor. Yandex.News set up formal "partnership" agreements with 6,700 media outlets in 2016, before the law came into force on January 1, 2017. All unregistered media (including dissident voices such as *Mediazona*) and foreign media (such as the Russian-language BBC and media in exile such as Meduza) were then removed from Yandex.News's Top 5. After the law was passed, Tatyana Isaeva, who had headed Yandex.News since 2012, announced that she was leaving the company. In an interview with Meduza, she argued that the law had rendered her work obsolete and that the very purpose of an aggregator—to highlight important news and make different points of view available to the user—was undermined: "The aggregator is really meant to cover the image (of news) at a glance. If that picture is reduced to a single viewpoint, it's hard to see why an aggregator is needed."[16]

Even after this law came into effect, the authorities continued to criticize Yandex's aggregator. In August 2019, Russian Duma deputies accused Yandex

of spreading "fake news" after an inaccurate article in the daily *Kommersant* topped the Yandex.News selection. The article claimed that the Duma was considering a ban on old vehicles, which caused widespread outrage and led representatives to clarify that this was a recommendation only for business vehicles and not for personal vehicles. However, the information remained at the top of the list even after it had been debunked, leading some representatives to criticize the news aggregator. MP Andrei Isaev accused Yandex of "deliberately exacerbating the social and political situation" and of "foreign interference." Adalbi Shkhagoshev said he had called Yandex CEO Elena Bunina to ask her to revise the news aggregator's algorithm—to which Yandex responded by threatening to shut down its aggregation service.[17] This scandal came at a difficult political time for the government, with opposition movements demonstrating over the summer against the refusal to let them register for the Moscow Duma elections.

YANDEX.NEWS DISCREDITED IN THE MEDIA

Since 2012, independent journalists and political activists have denounced the aggregator's gradual takeover by advocates of a "patriotic" position (legislators, regional administrations, official media, etc.). Leading online freedom advocates who initially supported the Yandex.News aggregator became skeptical about its ability to remain immune to political intervention. They gathered evidence to expose its partiality and claimed that Yandex.News rankings were biased in favor of the government and that the bias may come from the aggregator itself, which concealed information about the opposition, or from official actors who had learned to trick its algorithm. This suspicion was strengthened by observers who, at specific events, noted a discrepancy between their common-sense assessment of what mattered most and the selection provided by Yandex's machine.

According to a journalist at *Kommersant*, "The algorithm is leveraged by newspapers serving the authorities, who publish information that is pushed towards the top."[18] Their techniques consisted in pushing the limits of search engine optimization (SEO) and playing with Yandex.News's algorithms by artificially creating multiple sources of information. This could be

understood as a way to exploit the platform's vulnerabilities in order to gain increased visibility. The strategies of "junk news" websites follow a similar logic, when they increase their "discoverability" in the Google search engine (through keyword optimization, this time) for the purpose of disinformation (Bradshaw 2019). These attempts to shape search results are as old as online searching itself, and algorithms are usually updated at regular intervals to counter such manipulations—with no lasting success.

For example, according to an investigation by the newspaper *RBK*,[19] during the 2014 Moscow City Duma elections, dozens of unknown media sites published the same information about the alleged success of Moscow's mayor and candidate for reelection Sergei Sobyanin, and this item showed up among the first results on Yandex.News. According to this investigation, several hundred local newspapers, institutional websites, and government agencies (many of them newly established) were registered in Yandex's "database of media and official sources." Information in favor of the Moscow mayor was allegedly passed on to these media and websites by a company called Moscow Information Technologies, which is owned by Moscow's municipal authorities. Before publishing it on their websites, it appears that these local outlets rephrased the news item to ensure that the Yandex algorithm would not identify their articles as duplicates.

In March 2017, major protests took place in Moscow and across Russia after Aleksei Navalny's Anti-Corruption Foundation (FBK) published an investigative report showing multiple examples of alleged embezzlement by former Prime Minister Dmitry Medvedev. A thousand people were arrested in Moscow but, surprisingly, according to journalist Aleksei Kovalev, the protests were barely mentioned on the Yandex.News homepage or even on their local news feed for Moscow.[20] Yandex argued that its algorithms had not been tampered with but that this was a consequence of the law on aggregators that had drastically reduced the number of sources available—which illustrated how the law had produced a mechanism of indirect control (Wijermars 2021).

Political suspicions against the news aggregator resurfaced in April 2020, when the Russian technology website TJournal showed that a search for Aleksei Navalny's name on the Yandex search engine and Yandex.News services yielded only negative content.[21] When asked about it by TJournal,

Yandex claimed that the focus on negative publications about Navalny was an "experiment." In 2021, after Navalny's return from Germany and his imprisonment, protests broke out in Moscow. Activists pointed out Yandex.News' discretion around these events. In 2018, an activist close to Navalny had already told us that "Yandex.News transmits state propaganda. The aggregator has been destroyed." Some observers pointed out that Yandex avoided conflicts with state authorities to secure its many lucrative activities (Yandex.Taxi, Yandex.Eda, etc.).[22]

OBJECTIVIZING THE CONSTRAINT

During the month of June 2020, to put these suspicions to the test, we conducted a quantitative analysis of the news selected by Yandex.News and presented in the Top 5 news stories on the Yandex homepage. We systematically collected news items from June 1 to 30, 2020.[23] Over this period, all the items listed in the Top 5 came from a small group of only fourteen media outlets—an extremely small sample considering that over seven thousand sources were listed in the Yandex.News database. We then extended the collection period to December 2020 and obtained the same results, with the same fourteen media outlets appearing in the Top 5 over this period (Daucé and Loveluck 2021). The data strikingly show the concentration of news on Yandex.News from a handful of large media players: state-owned news agencies, state-funded media, and mainstream newspapers and online publications.

While certain media outlets have also been found to be overrepresented on Google News (Schroeder and Kralemann 2005; Haim et al. 2018), this is not to the same extent as on Yandex.News. The range of outlets featured on the latter is much narrower than the one Nechushtai and Lewis (2019) found on Google News in the US, for example. There, although a small selection of fourteen sources is also very prevalent in the aggregator's results, a "long tail" of other publications is also featured. In an examination of Google Top Stories in the US, Trielli and Diakopoulos (2019) found that only twenty news sources accounted for more than half of the articles featured and that this selection of outlets showed a "left-wing ideological bias." However, here

again, a considerable long tail of over 650 other news sources appeared at least once in the second half of the 6,302 links collected over a month.

In Russia, although there are nuances to be found between these fourteen main media outlets, there is no doubt that only "loyal" media outlets have access to Yandex rankings. Most of these publications have ties to the Kremlin: they are either state-funded or owned by "loyalist" personalities or entities and therefore indirectly managed by the authorities. Since 2014, the Russian media landscape has generally been divided into state and private independent media—the boundaries between which are blurred and debatable. The state media are clearly identified (*RIA Novosti*, *RT*, *Rossijskaia Gazeta*, *TASS*, *Interfax*). Alongside these, a number of "loyal private patriotic" media can be identified, which refers to the general news media that have been transformed from within by the departure and replacement of their editorial teams between 2012 and 2014 (*Izvestia*, *Lenta.ru*, *Gazeta.ru*). While an official facade remains, they have suffered hostile interventions, and their teams have been replaced by loyalist journalists (Chupin and Daucé 2017; Daucé 2020; Kovalev 2020). Finally, "loyal private liberal" media refers to business media that were considered liberal but whose political departments were reorganized between 2018 and 2020 (this mainly concerns *RBK*, *Kommersant*, and *Vedomosti*). Yandex.News operates in the context of an economic and political reshaping of the Russian media sphere, where a variety of constraints have narrowed down the media spectrum (Wijermars and Lehtisaari 2020). As a result, the main sources on which the Yandex.News (now DZen.News) algorithm relies to outline the daily news online have been profoundly modified. Conversely, independent media outlets were gradually sidelined, as Yandex.News no longer redirected traffic their way, which reduced their advertising revenue and narrowed down their audience, making them less viable commercially (Kovalev, 2020; Wijermars, 2021).

THE UNEQUAL WAR OF THE AGGREGATORS

Even before the war against Ukraine broke out, many observers pointed to the algorithm's loss of legitimacy in the eyes of journalists and web professionals

and developers, who had started to look for ways to circumvent it. Some of them felt that the service had become meaningless. As Lev Gershenzon noted in 2016, "Aggregators only make sense . . . when there is something to aggregate. If all the independent, interesting, and professional publications at the federal level can be counted on the fingers of one hand, aggregating and processing them does not require sophisticated technology—you can just bookmark them."[24] It seems like Yandex executives themselves had considered shutting it down. According to journalist A. Plyushchev, of *Ekho Moskvy* radio (closed in March 2022), "You know, I spoke once with A. Volozh, the director of Yandex, and this was before the law on aggregators was passed. And he told me that if the law was passed, he would close the service. . . . Well, the law was softened a bit, and the service, as you can see, didn't close. I still have my doubts that this is the right decision. Because, well, I think that, unfortunately, the state has done everything to manipulate both the media and search engine extraction."[25] In May 2018, he wrote an open letter to Yandex CEO Elena Bunina, advising her to close the Yandex. News service or rename it Yandex.Propaganda.

With Yandex.News being thus compromised, plans to develop an alternative aggregator emerged. In 2019, Telegram founder Pavel Durov announced from abroad his intention to develop a news aggregator on his platform: "We have a chance to create the first efficient and free news aggregator in the history of the Internet. . . . We can start recommending articles from the Recommended Articles block after reading each article in Telegram, gradually bringing it into service with an hourly selection and a global search on all the news in the world."[26] Durov claimed that, unlike services located in Russia, his aggregator would evade the grip of Russian security services and political censorship. He invited Yandex.News developers to participate in the creation of his service and announced the launch of a contest, the Data Clustering Contest,[27] aimed at kickstarting the development of an aggregation algorithm on the platform. Although the contest was held, the launch of the aggregator was delayed, and the promised service had not gone live when the war broke out.

From February 2022 onward, the war fueled these controversies surrounding the algorithm. As early as February 27, 2022, Lev Gershenzon,

from abroad, published a long text on Facebook in which he denounced the ills of Yandex's news aggregator:

> Now every day, the war between Russia and Ukraine is possible because there are no mass antiwar demonstrations in Russian cities. And they are not happening not only because of the danger of exit repression (huge admiration to everyone who goes out anyway), but mainly because the vast majority of the population does not know that Russian troops are waging a full-scale war on the fourth day. Yandex plays a leading role in ensuring this ignorance, along with television—a website and applications with a news block, 5 news, "on the main". . . . Every hour and day that (it) works the way (it) does now is waging war.

On 1 March, he wrote again:

> Today is the sixth day of the war between Russia and Ukraine, a day on which residential areas, dormitories and maternity hospitals in Kharkiv are fired on with multiple rocket attacks. 11 dead, dozens injured. Today is the sixth day that, on the main page of Yandex, at least 30 million Russian users are seeing that there is no war, that there are not thousands of dead Russian soldiers, that there are not dozens of civilians killed by Russian bombing, that there are not dozens of prisoners, that there is not huge destruction in various Ukrainian cities. The fact that a significant part of the Russian population may believe that there is no war is the basis and the driving force of this war. Today, Yandex is a key element in hiding information about the war.

The post was liked over 3,700 times and followed by numerous comments.

Lev Gershenzon subsequently announced that he would create an alternative news aggregator without censorship[28] to display the diversity of content and points of view available online. The new aggregator was designed by a volunteer team of about twenty people who had worked together for Yandex, with the hope of eventually finding revenue streams to fund the project. In August 2022, the alternative aggregator was launched under the name The True Story (https://thetruestory.news) and was blocked four days later in Russia at the request of Roskomnadzor. It remains accessible only abroad, or in Russia only to VPN users. Representatives of the Russian government immediately denounced the new aggregator. The deputy chairman of the state Duma Committee on Economic Policy, Artyom Kiryanov, commented,

> The news aggregator The True Story has been used to spread panic and false information without reflecting an objective picture of the world. It presents itself as an independent platform. But . . . why is there only negative content in the rankings? . . . The answer may lie in the history of its creation, and especially of Lev Gershenzon, the man who created The True Story. Apparently, it was an attempt to create a channel for the information war against Russia, where the main objective is not to objectively present information, but to promote fake news and spread panic.[29]

The new aggregator collects data from media officially registered in Russia (*RBK*, *Kommersant'*, *Vedomosti*, Fontanka, Interfax) as well as from many sites categorized as "foreign agents" or banned in Russia (Doxa, Meduza, Radio Svoboda, RTVI, Golos Ameriki, *Novaïa Gazeta*, etc.). Its audience remains modest, as it is not backed by a search engine. In November 2022, it had around 20,000 subscribers on its Telegram channel. However, this new aggregator is arousing the interest of free internet advocates. To increase its visibility, a partnership project with the Internet Protection Society (OZI) aims to display it on the homepage of a VPN that the association promotes.[30]

CONCLUSION

The recent history of Yandex.News in Russia brings to light the way in which platform regulation can be used to implement a form of governance by algorithms in the public sphere. Initially presented as a technical means of "objectively" reporting on the diversity of online content, the aggregator fueled various techno-political controversies in the 2010s. The authorities criticized it for promoting "unpatriotic" or "fake" news, while journalists, web professionals, and users pointed out that inconvenient truths were unlikely to reach the top of the rankings. The 2016 legislation on news aggregators, which allows the service to display only officially registered sources, sent a clear signal that the government was intent on domesticating the platform to limit the visibility of dissent and discontent in the public sphere. This regulation took place in a complex digital ecosystem, where various levels of control are articulated together, including Yandex.News and

other platforms, the telecommunications watchdog Roskomnadzor, and the media and journalists themselves.

The various types of evidence presented in this research—public controversies, a cursory audit of the algorithm, and a study of official literature—indicate that Yandex, as a news recommendation system, had to abide by both legal and technical codes of conduct that ensured that the information it promoted and amplified remained under control. For example, in 2020, the service gave visibility to only fourteen media outlets, which were themselves closely monitored by the Russian authorities through Roskomnadzor. The tight government control over the algorithm's rankings is evident in comparison to Google News, which while it gives pride of place to a small selection of major media outlets, also shows a long tail of diverse publications and, in any case, does not display a selection of news on its search engine homepage by default. Thus, Yandex.News, and now DZen.News, gradually came to display only a mere façade of information pluralism. It no longer reflects the diversity of the content that still circulates in the Russian digital sphere. The aggregator appears to be an important cog in the authorities' control apparatus, which covers the entire Russian media ecosystem. The authorities justify these efforts to control the media agenda and assert their sovereignty over the public sphere by condemning information they label unpatriotic, false, or otherwise problematic.

Faced with new obstacles, media actors and information professionals developed a critical view of the role and workings of platforms and their algorithms, shedding light on the politics at stake around these key infrastructures. With Russia's war on Ukraine, the political stranglehold on the aggregator Yandex.News became obvious when it was taken over by the government-owned company VKontakte. In an increasingly threatening context, many journalists and Russian internet specialists have chosen exile. They are now looking for alternative channels to disseminate information and often turn to social media such as Telegram or X/Twitter. Caught in an unequal power struggle, some of them, around L. Gershenzon, are still nourishing hopes that algorithms could serve their cause and help to bring peace in Ukraine, with an alternative aggregator free to report the "real story."

NOTES

1. K. Bhaat, "And Now, News," *Google Official Blog*, January 23, 2006, https://googleblog.blogspot.com/2006/01/and-now-news.html.
2. Since August 2022, the former Yandex homepage and Yandex.News now redirect, respectively, to DZen.ru and DZen.ru/news (property of VK), while the Yandex search engine stripped of its news features can still be accessed via the ya.ru domain.
3. Yandex 2020 financial results (https://ir.yandex/financial-releases?year=2020andreport=q4).
4. We thank Fabrice Demarthon (CNRS/CERCEC) for his help in extracting the databases and scraping the results from the main page of Yandex.News.
5. Z. Tufekci, "YouTube, the Great Radicalizer," *New York Times*, March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html; see also (O'Callaghan et al. 2015).
6. This has led to heated debate in most countries, which have generally reached an agreement except in Spain, where the service is closed due to the introduction of a "link tax" that obliges Google to pay a fee for displaying text excerpts.
7. A. Robertson, "After Its 4chan Slip-up, Is It Time for Google to Drop Top Stories?," *The Verge*, October 3, 2017, https://www.theverge.com/2017/10/3/16413082/google-4chan-las-vegas-shooting-top-stories-algorithm-mistake.
8. These principles were presented on a page that can no longer be accessed but was last crawled by the Internet Archive's Wayback Machine on April 4, 2022: https://web.archive.org/web/20220404033424/https://yandex.ru/promo/news/index.
9. Graduate of the Chair of Theoretical and Computational Linguistics of the Moscow University of Social Sciences (RGGU).
10. L. Gershenzon, interview with the authors, January 2020.
11. "Protesty ne v tope," Radio Svoboda—Krym Realii, March 29, 2017, https://ru.krymr.com/a/28397904.html.
12. E. Osetinskaia, "Yandex, a Russian Success Story and Putin's High-Tech Tiger," editorial for *The Moscow Times*, September 27, 2017, https://themoscowtimes.com/articles/yandex-a-russian-success-story-and-putins-high-tech-tiger-59029.
13. M. Seddon, "Yandex Agrees Restructuring with Kremlin," *Financial Times*, November 28, 2019, https://www.ft.com/content/999e3ca6-09db-11ea-bb52-34c8d9dc6d84.
14. On March 16, 2021, the Duma passed a law setting fines for the sale of phones, tablets, and computers without preinstalled Russian applications. Amendment to Article 14.8 of the Code of Administrative Offences (https://sozd.duma.gov.ru/bill/757430-7). (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
15. "Yandex 'ražigaet' Majdan v Rossii?" *Pravda,* http://www.pravda.ru/topic/yandex-617/.

16. Interview with Tatyana Isaeva published in *Meduza*, October 24, 2016, https://meduza.io/feature/2016/10/24/oschuscheniya-chto-ot-mediasredy-otstali-net.

17. "Deputaty popali v Yandex.Novosti," *Kommersant'*, August 16, 2019, https://lenta.ru/news/2019/08/16/ya_novosti/.

18. Interview with D., journalist, Moscow, September 2019.

19. Zh. Ulânova and D. Luganskaâ, "Rassledovanie RBK: kak činovniki perehitrili Yandex," РБК, October 22, 2014, http://top.rbc.ru/technology_and_media/22/10/2014/5447a659cbb20f1d5d33b94d.

20. A. Kovalev, "'Hear No Evil, See No Evil, Report No Evil," *Moscow Times*, March 27, 2017, https://www.themoscowtimes.com/2017/03/27/hear-no-evil-see-no-evil-report-no-evil-a57550.

21. "Yandex vsemi svoimi servisami risuet obraz Naval'nogo," *TJournal*, April 26, 2020, archived at https://web.archive.org/web/20211105034206/https://tjournal.ru/news/162614-yandeks-vsemi-svoimi-servisami-risuet-obraz-navalnogo. (Tjournal was blocked in Russia in March 2022 and it deleted its website. However, this publication can be accessed at https://web.archive.org/web/20211105034206/https://tjournal.ru/news/162614-yandeks-vsemi-svoimi-servisami-risuet-obraz-navalnogo. Please refer to our "Note on the Availability of Sources.")

22. Apart from its web search engine, Yandex has developed a host of other services such as a web portal and an email service, as well as more specific businesses such as Yandex.Taxi (passenger transport by taxi, which merged with Uber in 2017), Yandex.Karty (maps and geolocation), Yandex.Music (music streaming), and Yandex.Eda (food delivery).

23. We automatically collected Yandex.News rankings every two hours and listed a total of 3,011 references. The data were collected on a server based in France, but we controlled for possible personalization and localization features by checking the news results displayed for a user based in Russia at different times and found no difference.

24. L. Gershenzon, "Nothing to aggregate," Republic, April 20, 2016, https://republic.ru/posts/66965.

25. Interview with Aleksandr Plyushchev, Moscow, March 2019.

26. https://www.vedomosti.ru/technology/articles/2019/06/07/803708-durov-sozdast.

27. The first stage of the competition took place in November 2019 and the second in May 2020.

28. https://holod.media/2022/05/17/gershenzon-yandex/.

29. Facebook post by Lev Gershenzon, September 14, 2022.

30. Interview with an OZI official, Paris, November 2022.

REFERENCES

Alyukov, Maxim. 2021. "News Reception and Authoritarian Control in a Hybrid Media System: Russian TV Viewers and the Russia-Ukraine Conflict." *Politics* 44 (3): 400–419.

Belair-Gagnon, Valerie, and Avery E. Holton. 2018. "Boundary Work, Interloper Media, and Analytics in Newsrooms: An Analysis of the Roles of Web Analytics Companies in News Production." *Digital Journalism* 6 (4): 492–508.

Boyer, Dominic. 2013. *The Life Informatic. Newsmaking in the Digital Era*. Cornell University Press.

Bozdag, Engin. 2013. "Bias in Algorithmic Filtering and Personalization." *Ethics and Information Technology* 15 (3): 209–227.

Bradshaw, Samantha. 2019. "Disinformation Optimised: Gaming Search Engine Algorithms to Amplify Junk News." *Internet Policy Review* 8 (4): 1–24.

Brake, David R. 2017. "The Invisible Hand of the Unaccountable Algorithm: How Google, Facebook and Other Tech Companies Are Changing Journalism." In *Digital Technology and Journalism. An International Comparative Perspective*, edited by Jingrong Tong and Shih-Hung Lo. Palgrave Macmillan.

Bruns, Axel. 2019. *Are Filter Bubbles Real?* Polity Press.

Bucher, Taina. 2016. "Neither Black nor Box: Ways of Knowing Algorithms." In *Innovative Methods in Media and Communication Research,* edited by Sebastian Kubitschko and Anne Kaun. Palgrave Macmillan.

Bui, CamLy. 2010. "How Online Gatekeepers Guard Our View. News Portals' Inclusion and Ranking of Media and Events." *Global Media Journal* 9 (16): 1–41.

Calzada, Joan, and Ricard Gil. 2020. "What Do News Aggregators Do? Evidence from Google News in Spain and Germany." *Marketing Science* 39 (1): 134–167.

Christin, Angèle. 2020. *Metrics at Work. Journalism and the Contested Meaning of Algorithms*. Princeton University Press.

Chupin, Ivan, and Françoise Daucé. 2017. "Termination of Journalists' Employment in Russia: Political Conflicts and Ordinary Negotiation Procedures in Newsrooms." *Laboratorium: Russian Review of Social Research* 9 (2): 39–58.

Daucé, Françoise. 2017. "Political Conflicts around the Internet in Russia: The Case of Yandex. Novosti." *Laboratorium: Russian Review of Social Research* 9 (2): 112–32.

Daucé, Françoise. 2020. "Disguising the Internet? Website Design and Control in Russia." *Digital Icons* 20. https://www.digitalicons.org/issue20/disguising-the-Internet-website-design-and-control-in-russia.

Daucé, Françoise, and Benjamin Loveluck. 2021. "Codes of Conduct for Algorithmic News Recommendation: The Yandex.News Controversy in Russia." *First Monday* 26 (5). https://firstmonday.org/ojs/index.php/fm/article/view/11708.

Denisova, Anastasia. 2017. "Democracy, Protest and Public Sphere in Russia after the 2011–2012 Anti-government Protests: Digital Media at Stake." *Media, Culture and Society* 39 (7): 976–994.

Diakopoulos, Nicholas. 2019a. *Automating the News. How Algorithms are Rewriting the Media*. Harvard University Press.

Diakopoulos, Nicholas. 2019b. "Audit Suggests Google Favors a Small Number of Major Outlets." *Columbia Journalism Review*. May 10. https://www.cjr.org/tow_center/google-news-algorithm.php.

Dovbysh, Olga, Mariëlle Wijermars, and Mykola Makhortykh. 2022. "How to Reach Nirvana: Yandex, News Personalisation, and the Future of Russian Journalistic Media." *Digital Journalism* 10(10): 1855–1874.

Epstein, Robert, and Ronald E. Robertson. 2015. "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections." *Proceedings of the National Academy of Sciences of the United States of America* 112 (33): E4512-E4521.

Fedor, Julie, ed. 2015. "Russian Media and the War in Ukraine." *Journal of Soviet and Post-Soviet Politics and Society* 1 (special issue).

Flaxman, Seth, Sharad Goel, and Justin M. Rao. 2016. "Filter Bubbles, Echo Chambers, and Online News Consumption." *Public Opinion Quarterly* 80 (S1): 298–320.

Fletcher, Richard, and Rasmus Kleis Nielsen. 2018. "Automated Serendipity: The Effect of Using Search Engines on News Repertoire Balance and Diversity." *Digital Journalism* 6 (8): 976–989.

Gillespie, Tarleton. 2018. "Regulation of and by Platforms." In *The SAGE Handbook of Social Media*, edited by Jean Burgess, Alice Marwick and Thomas Poell. Sage.

Haim, Mario, Andreas Graefe, and Hans-Bernd Brosius. 2018. "Burst of the Filter Bubble? Effects of Personalization on the Diversity of Google News." *Digital Journalism* 6 (3): 330–343.

Helberger, Natali. 2019. "On the Democratic Role of News Recommenders." *Digital Journalism* 7 (8): 993–1012.

Helberger, Natali, Kari Karppinen, and Lucia D'Acunto. 2018. "Exposure Diversity as a Design Principle for Recommender Systems." *Information, Communication and Society* 21 (2): 191–207.

Hindman, Matthew S. 2008. *The Myth of Digital Democracy*. Princeton University Press.

Hindman, Matthew S. 2018. *The Internet Trap. How the Digital Economy Builds Monopolies and Undermines Democracy*. Princeton University Press.

Hong, Sounman, and Nayeong Kim. 2018. "Will the Internet Promote Democracy? Search Engines, Concentration of Online News Readership, and e-Democracy." *Journal of Information Technology and Politics* 15 (4): 388–399.

Introna, Lucas, and Helen Nissenbaum. 2000. "Shaping the Web: Why the Politics of Search Engines Matters." *The Information Society* 16 (3): 169–185.

Jannach, Dietmar, Markus Zanker, Alexander Felfernig, and Gerhard Friedrich. 2011. *Recommender Systems. An Introduction*. Cambridge University Press.

Jiang, Min. 2014. "The Business and Politics of Search Engines: A Comparative Study of Baidu and Google's Search Results of Internet Events in China." *New Media and Society* 16 (2): 212–233.

Just, Natascha, and Michael Latzer. 2017. "Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet." *Media, Culture and Society* 39 (2): 238–258.

Karimi, Mozhgan, Dietmar Jannach, and Michael Jugovac. 2018. "News Recommender Systems: Survey and Roads Ahead." *Information Processing and Management* 54 (6): 1203–1227.

Kitchin, Rob. 2016. "Thinking Critically about and Researching Algorithms." *Information, Communication and Society* 20 (1): 14–29.

Kovalev, Alexey. 2020. "The Political Economics of News Making in Russian Media: Ownership, Clickbait and Censorship." *Journalism* 22 (12): 2906–2918.

Kulshrestha, Juhi, Motahhare Eslami, Johnnatan Messias, Muhammad Bilal Zafar, Saptarshi Ghosh, Krishna P. Gummadi, and Karrie Karahalios. 2019. "Search Bias Quantification: Investigating Political Bias in Social Media and Web Search." *Information Retrieval Journal* 22 (1–2): 188–227.

Latour, Bruno. 2005. *Reassembling the Social. An Introduction to Actor-Network-Theory*. Oxford University Press.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. Basic Books.

Lonkila, Markku, Larisa Shpakovskaya, and Philip Torchinsky. 2020. "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet." In *Freedom of Expression in Russia's New Mediasphere,* edited by Mariëlle Wijermars and Katja Lehtisaari. Routledge.

Maréchal, Nathalie. 2017. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication* 5 (1): 29–41.

Marres, Noortje. 2007. "The Issues Deserve more Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy." *Social Studies of Science* 37 (5): 759–780.

Mejias, Ulises A., and Nikolai E. Vokuev. 2017. "Disinformation and the Media: The Case of Russia and Ukraine." *Media, Culture and Society* 39 (7): 1027–1042.

Musiani, Francesca. 2013. "Governance by Algorithms." *Internet Policy Review* 2 (3).

Musiani, Francesca, Benjamin Loveluck, Françoise Daucé, and Ksenia Ermoshina. 2019. "'Digital Sovereignty': Can Russia Cut Off Its Internet from the Rest of the World?" The Conversation. October 28. https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-Internet-from-the-rest-of-the-world-125952.

Napoli, Philip M. 2014. "Automated Media: An Institutional Theory Perspective on Algorithmic Media Production and Consumption." *Communication Theory* 24 (3): 340–360.

Nechushtai, Efrat, and Seth C. Lewis. 2019. "What Kind of News Gatekeepers Do We Want Machines to Be? Filter Bubbles, Fragmentation, and the Normative Dimensions of Algorithmic Recommendations." *Computers in Human Behavior* 90: 298–307.

Nielsen, Rasmus Kleis, and Sarah Anne Ganter. 2018. "Dealing with Digital Intermediaries: A Case Study of the Relations between Publishers and Platforms." *New Media and Society* 20 (4): 1600–1617.

Nocetti, Julien. 2015. "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy." *Internet Policy Review* 4 (4).

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

O'Callaghan, Derek, Derek Greene, Maura Conway, Joe Carthy, and Pádraig Cunningham. 2015. "Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems." *Social Science Computer Review* 33 (4): 459–478.

Pariser, Eli. 2011. *The Filter Bubble. What the Internet Is Hiding from You*. Penguin Press.

Pasquale, Frank. 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press.

Ricci, Francesco, Lior Rokach, and Bracha Shapira. 2015. *Recommender Systems Handbook*. Springer.

Saurwein, Florian, Natascha Just, and Michael Latzer. 2015. "Governance of Algorithms: Options and Limitations." *Info* 17 (6): 35–49.

Schroeder, Roland, and Moritz Kralemann. 2005. "Journalism ex Machina: Google News Germany and Its News Selection Processes." *Journalism Studies* 6 (2): 245–247.

Seaver, Nick. 2019. "Knowing Algorithms." In *DigitalSTS. A Field Guide for Science and Technology Studies*, edited by Janet Vertesi and David Ribes. Princeton University Press.

Sivetc, Liudmila. 2019. "State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners." *International Journal of Law and Information Technology* 27 (1): 28–49.

Soldatov, Andrei, and Irina Borogan. 2015. *The Red Web. The Kremlin's Wars on the Internet*. PublicAffairs.

Thorson, Kjerstin and Chris Wells. 2015. "How Gatekeeping Still Matters: Understanding Media Effects in an Era of Curated Flows." In *Gatekeeping in Transition*, edited by Timothy Vos and François Heinderyckx. Routledge.

Thorson, Kjerstin and Chris Wells. 2016. "Curated Flows: A Framework for Mapping Media Exposure in the Digital Age." *Communication Theory* 26 (3): 309–328.

Trielli, Daniel, and Nicholas Diakopoulos. 2019. "Search as News Curator: The Role of Google in Shaping Attention to News Information." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, edited by Stephen Brewster and Geraldine Fitzpatrick, ACM, New York.

Vendil Pallin, Carolina. 2017. "Internet Control through Ownership: The Case of Russia." *Post-Soviet Affairs* 33 (1): 16–33.

Wijermars, Mariëlle. 2021. "Russia's Law 'On News Aggregators': Control the News Feed, Control the News." *Journalism* 22 (12): 2938–2954.

Wijermars, Mariëlle, and Katja Lehtisaari, eds. 2020. *Freedom of Expression in Russia's New Mediasphere*. Routledge.

4 DIGITAL SECURITY TRAINING: GAFAM/MAGMA, DATA PROTECTION, AND ENCRYPTION

Olga Bronnikova, Ksenia Ermoshina, and Anna Zaytseva

> We write to express our concerns about growing calls to interfere with the Russian people's access to the Internet, which we fear will hurt individuals attempting to organize in opposition to the war, report openly and honestly on events in Russia, and access information about what is happening in Ukraine and abroad. These measures could also unnecessarily facilitate further repression by the Russian government. . . . Overly broad restrictions on the access of the Russian people to the Internet would further isolate the embattled pro-democracy and anti-war activists, and impede the ability of NGOs, human rights groups, journalists, and attorneys inside and outside Russia to provide critical information to citizens about the current state of affairs and their rights. These actions would inadvertently speed up what the Kremlin has set out to achieve through its "sovereign Internet" tools—a complete and total control of information space inside Russia[1].

This petition, signed by over fifty human rights and internet freedom organizations, was published by the NGO Access Now on March 10, 2022. It was prompted by restrictions and cuts in access to the services of certain US technology companies in Russia (major internet service providers (ISPs) such as Cogent and Lumen and platforms such as Slack, YouTube, Google Pay, and AppStore) starting the day after the Kremlin launched a full-scale war on Ukraine. This appeal highlights the main antagonism between the state and a part of civil society, as well as a third key player, the GAFAM/MAGMA platforms[2] that have come to represent access to free information, seen as a tool to fight back against state censorship. Our fieldwork sheds light on this antagonism from another angle—that of digital security, which is

perceived as a central issue in the relations between dissenting civil society actors and the Russian state. As the latter takes an authoritarian and dictatorial turn, and deploys "information security" measures—a notion that, in the Russian doctrine, entails controlling information flows and dismantling any independent political or social force—civil society actors are compelled to use digital security tools and practices developed abroad to shield themselves from these attacks.

This chapter sheds light on the ways in which, by learning and through evolving digital security practices, some dissenting actors of Russian civil society have come to adapt to or circumvent the multiple legal, police, and technical constraints that growing digital authoritarianism places on their activities. To this end, we focus on the role of the tools and infrastructure provided by transnational technology companies.

Our analysis is based on field research conducted between 2018 and 2022. We met with digital security trainers and free internet activists as well as attendees of their training courses, both in Russia and in exile: independent journalists (at media outlets not controlled by the state), human rights advocates,[3] and environmentalist and anticorruption activists (at Transparency International or Alekseï Navalny's Anti-Corruption Foundation). While they also constitute a dissenting section of civil society, anarchists and radical leftist do not attend these training courses. As they have been the target of repression for longer and navigate quicker through a culture of semi-clandestinity, they have forged a different culture around digital security (which, among other things, is distinctly critical of GAFAM/MAGMA and interested in open-source solutions). Although they are not the focus of our discussion, we will sometimes use these activists as a point of comparison to highlight the specific features of the practices of anticorruption activists, human rights advocates, and independent journalists.

This chapter is based on a "multisite" survey that sheds light on the international nature of the tools and practices of digital self-defense. In addition to Moscow and St. Petersburg, we conducted fieldwork in Minsk, Belarus, in 2019. Belarusian trainers are important actors in the security training ecosystem within the post-Soviet space, due to the scale of repression in the country and the know-how they have therefore acquired. Other key

players include international organizations such as Access Now, Frontline Defenders, the Civil Rights Center, and Reporters Without Borders, whose representatives we interviewed in Russia, Prague, Berlin, Paris, and online. We have established relationships of trust with spokespersons of NGOs campaigning for the free internet, such as Roskomsvoboda, the Centre for Digital Rights, and the Internet Protection Society (OZI), as well as with members of the Social Technology Greenhouse (Teplitsa), a civic tech project that offers technological solutions to the political and organizational problems of NGOs in Russia. Since 2019, in a context of increasingly violent repression, which reached unprecedented levels after February 24, 2022, many of these activists have had to leave Russia. We met them in places of exile such as Warsaw, Tbilisi, and Vilnius.

We also took part in events that our interviewees organized around these issues, such as the Privacy Day forum in Minsk and Moscow, Internet Without Borders in various places of exile, digital security training organized online and offline by various organizations, a hackathon coordinated by the Internet Protection Society (OZI), one of the objectives of which was to propose a security device, and so on. In addition to semistructured interviews and participant observations, we monitored the Telegram channels of some key players in the field of digital freedoms and security and analyzed digital security guides targeted at civil society, as well as security advice videos posted on YouTube by these organizations. Were also put this fieldwork into perspective with a survey conducted under the European Nextleap project in 2016–2018 on the uses of end-to-end secure messaging (Ermoshina and Musiani 2018, 2022), as well as a study of the evolution of digital security training course formats that included a series of interviews with trainers, conducted in 2020.

To gain a better understanding of the evolution of practices, we first analyze how, in the Russian political context, the very notion of "digital security" has come to refer essentially to practices of self-defense against the state and is used in contrast to "information security," a term that belongs to the lexicon of Russian official discourse. We then explain the ecosystem of security training, which brings together several types of actors and covers different geographical scales, as well as the evolving methods and forms

these training endeavors adopt in light of the mounting constraints placed on members of civil society who are critical of the authorities. Finally, we examine the most recent reconfigurations in digital security practices following the start of the Russian invasion of Ukraine, the de facto imposition of martial law in Russia, and the mass exile of which many of the actors involved in our research were part.

"INFORMATION SECURITY" VERSUS "DIGITAL SECURITY"

To understand the particularity of the learning process of digital security and its tentative construction in the discourses and practices of civil society actors, we should first place it in the context of the growing adversity that shapes it. Among the people we met, the term *cifrovaâ bezopasnost*, which is modeled on the English term "digital security," is used more than "information security" (*informacionnaâ bezopasnost*). However, the latter more broadly predominates, with the national search engine Yandex yielding seventeen thousand results for it and only eight thousand for the former. This may be because "information security" is a broader term that, according to its Russian Wikipedia page, refers to "the practice of preventing unauthorized access to or use, disclosure, alteration, study, recording, or destruction of information," "regardless of the form the data may take, electronic or physical."[4] "Digital security," on the other hand, is described as only referring to "the protection of computer systems and networks from attacks by malicious actors."[5]

Information Security

In context, however, the two terms often appear to be interchangeable, except for specific uses of the term "information security" in government documents—and most notably in the Information Security Doctrines of 2000 and 2016. The second Doctrine, unlike the first, is based on the concept of national security (2015) adopted by the State Security Council following the annexation of Crimea, the outbreak of war in Donbass, and several Western sanctions packages. The state discourse on information security has also been shaped by the Snowden revelations of 2013. Highlighting the mass

surveillance that the NSA had carried out around the world from the US, these revelations gave further substance to the Russian authorities' argument in favor of reining in the Runet and protecting it from external threats that had become more plausible. This claim of state authority over cyberspace now seems to be part of an overarching framework for the interpretation of cybersecurity that, in turn, evidences a clear trend toward the militarization of methods, sometimes going as far as to foreshadow an impending cyber arms race (Ristolainen 2017).

The Russian approach fits squarely into this general trend. The Russian term for "cyberspace" seems quite specific at first sight: instead of being limited to the internet and digital networks, the notion of information space (*informacionnoie prostranstvo*) encompasses all media, including print and other audiovisual outlets. Thus, it "is not a field of action in itself, but an extension of the state's various political, economic or military fields of action" (Limonier, 2016, 132). In the US doctrine, cyberspace and cybersecurity also encompass different levels, ranging from the infrastructure layer to the soft power of media discourses and even motion picture fictions. The true particularity of the Russian approach lies in the defensive and reactive genesis of the term "information security," which was constructed in relation to the notion of informational confrontation (*informacionnoe protivoborstvo*) (Doktrina 2016). This confrontation pits Russia against NATO member states, primarily the US, countries that the Information Security Doctrine refers to as "certain states" that use their "advanced information technologies" to "undermine strategic stability," employing means of "technical surveillance against Russian state bodies, scientific organizations and enterprises of the military-industrial complex," as well as "destabilizing the internal political and social situation," "undermining sovereignty and territorial integrity," and "eroding traditional Russian spiritual and moral values." To thus destabilize Russia, the enemy ("certain states" and their "special services") uses "means of information and psychological influence" and act through "religious, ethnic and human rights organizations, as well as individual groups of citizens." It makes "extensive use of information technologies," including the media, which disseminate a "biased assessment of the state policy of the Russian Federation" (Doktrina 2016).

The state's discourse on information security, as well as the resulting legislative acts and judicial practices (which we will describe in further detail below), thus ultimately establish information space as a battleground of primary importance. As a result, the infrastructures of the global internet (dominated by US-registered companies), as well as foreign or independent media and civil society organizations, are seen as diversionary tools in the hands of certain hostile states, threatening national security and aiming to destabilize the world order more globally.

To counter these groups, Russian authorities assert the importance of technological sovereignty as a priority for national and information security. However, as this is difficult and costly to implement in the medium and long term, dissenting actors of civil society become the easiest targets to hit in this struggle for national security. In this context of the state's quest for digital sovereignty (Bronnikova et al. 2022), these actors, who have felt targeted from the mid-2010s onward and therefore seek security or mere survival, turn to digital services and networks provided by US multinationals, which enjoy more autonomy from the Russian authorities—or at least used to.

Digital Security

With the development of surveillance practices and intensifying repression, civil society activists are increasingly turning to foreign platforms, which are considered more secure than their Russian counterparts (VKontakte, Mail.ru, Yandex). The range of activist groups and collectives affected by authoritarian coercion has grown wider. Since the early 2010s, the state's palette of repression has continuously expanded, resulting in a range of legal and technical measures against journalists from independent media, NGOs, and human rights activists. After the demonstrations of 2011–2012 against the rigged elections, which the Russian authorities claim were fomented by foreign governments and foundations, the legislature frantically produced a proliferation of liberticidal laws.

In 2018, the FIDH (Fédération Internationale pour les Droits Humains) listed "fifty anti-democratic laws" that had come into force in Russia over six years, between 2012 and 2018 (FIDH 2018), including the law on "foreign agents," which targets organizations financed wholly or partly from abroad,

amendments to the law on terrorism and extremism that are systematically used against protestors, the law limiting public gatherings, and the law on "undesirable organizations," which allows the state to prohibit the activities of troublesome foreign organizations. While these laws do not directly concern the digital space, they nonetheless place it under scrutiny in order to incriminate professionals in the public sphere who openly take a stand against the authorities' arbitrary actions or even exchange information confidentially on platforms such as VKontakte, on which the police are increasingly present. Associations defending digital freedom, such as the Internet Protection Society (OZI) and Agora (renamed Setevye Svobody—Digital Freedoms), which have been documenting digital rights violations in Russia for several years, point to the role played by Russian platforms in implementing surveillance and controls over their users' speech (Lokot 2020). These associations have reported thousands of cases of administrative or criminal incrimination for merely reposting or even privately exchanging information considered extremist. This digital repression was taken to an unprecedented scale after the start of the Russian invasion of Ukraine on February 24, 2022. Since then, thousands of ordinary, nonmilitant people have been punished for posting messages criticizing the war on their social networks.

In addition, independent journalists and activists are subject to violent raids in which all their equipment is systematically seized. Chapter 8 of this book provides a detailed account of the form these raids take and their consequences. They often occur after activists have participated in protest actions during which they were identified through surveillance systems—which are highly developed in major Russian cities—or through the circulation of images on social media. Unprotected or poorly protected personal data, which endangers journalists' informants and NGO aid beneficiaries, regularly end up in the hands of the authorities, allowing them to further amplify the repression.

Faced with these dangers, digital rights advocates, security trainers, and opposition bloggers are calling on civil society actors to withdraw from Russian services, primarily VKontakte, in favor of their transnational counterparts, such as Facebook or X/Twitter, or decentralized and self-hosted platforms such as Mastodon.

Thus, from 2016–2017 onward, human rights advocates and independent journalists have embraced a concept of digital security as a set of self-defense practices regarding the Russian state, which radical left-wing circles had integrated from 2010–2012. However, unlike the latter, which aspire to open-source solutions such as XMPP (instant messaging protocol), Tor (decentralized and anonymized communications network), PGP (encryption software) or Briar (distributed encrypted messaging), and refuse the private solutions offered by US technology companies, human rights defenders are gradually coming to perceive these companies as "natural allies in their struggle for survival." Their positive perception of the services offered by Big Tech players is related to the efforts these companies have made, especially since the Snowden revelations, to cultivate their image as defenders of human rights (Google is particularly involved in this process). Moreover, international experts in digital security also advise using their services and present them as a reliable alternative to services controlled by authoritarian states (Bronnikova and Zaytseva 2021). Their trust is based on regular monitoring of the transparency reports published by Google and other GAFAM/MAGMAs. In contrast to the criticism European or American activists voice regarding these dominant digital platforms, users from authoritarian countries in the post-Soviet space relativize the risks associated with their use, given the ongoing confrontation between Russia and Belarus, on the one hand, and Western states and companies on the other. A Belarusian trainer who had worked with citizens of several countries in the post-Soviet space, including Russia, commented that "while for the countries . . . participating in the five eyes intelligence alliance,[6] 80–90% of the authorities' requests for information are met, for Russia these figures are only a few percent and, for Belarus, it's 0%."[7]

Beyond this preference for GAFAM/MAGMA services in Russia and other post-Soviet countries, large organizations and international NGOs specializing in supporting independent civil society are gradually prioritizing the development of digital and physical security skills. Civil society is becoming one of the preferred targets of state authorities and various parastatal militias in "high-risk" national contexts—a term used to denote several authoritarian regimes, such as those of Iran, China, Pakistan, Venezuela, and

Eritrea, among others. The digital, physical, and psychological risks faced by civil society actors have led international NGOs specializing in the protection of human rights advocates and digital freedoms (such as Frontline Defenders, Access Now, and the Electronic Frontier Foundation) to double down on security training courses and to encourage donors (such as the Open Technology Fund, the Ford Foundation, and the US State Department's Bureau of Democracy, Human Rights and Labor [DRL]) to provide massive funding for such courses.

DIGITAL SECURITY TRAINING

These training courses designed for civil society are part of a complex ecosystem combining local, national, and international scales. We will first describe this system as it has developed from the 2010s onward, along with its key actors, and then look at its teaching approaches and evolving methods, shaped through a series of practical trials and errors.

The Ecosystem

There are at least three distinct types of actors within the digital security training ecosystem (apart from their beneficiaries, associations, and activists): trainers, specialized NGOs, and donor organizations. Most digital security experts and trainers work on an outsourced consulting basis. Very few Russian NGOs and media outlets can afford to employ their own digital security specialist (or even just a system administrator); their funds are both insufficient and, in any case, earmarked "per project," which precludes having someone on the payroll indefinitely.

The relationship between these experts and NGOs is mediated by international organizations specialized in supporting human rights advocates and journalists around the world. There are essentially two types of organizations of this kind. The first type, consisting of both governmental and nongovernmental organizations,[8] act as donors. They provide funding over a period of a few months to several years for a particular program carried out by a local NGO and have a say in its budgetary expenditure. These organizations may recommend digital security training or an audit to an NGO and refer

it to one of the specialist digital security NGOs, which are the second main type of international actor. These are US-based (Electronic Frontier Foundation, Access Now), Canadian (eQualit.ie), and European (Huridocs, Tactical Tech, Frontline Defenders, Civil Rights Defenders) organizations, which operate internationally and specialize in technical—including IT—and legal support for human rights activists and journalists. While they do not provide funds, they do provide activists with protection tools, including digital ones, long-term practical assistance, reliable infrastructure (hosting, maintenance of mail or email servers, setting up VPNs), training, and small grants. They organize specialized events, "trainer training," conferences, and forums. Digital security support granted to NGOs can take several forms, ranging from ad hoc advice given by digital security experts paid for by one of the aforementioned human rights NGOs to more or less specialized training, computer security fellowships, or funding by an NGO for long-term assistance from an external expert with a specific objective. Finally, as we have shown elsewhere (Bronnikova and Zaytseva 2021), aside from international NGOs, large IT companies (such as Google and Microsoft) can also play a role in equipping associations' offices and providing digital security tools. This has been done in the framework of programs such as TechSoup, which until February 2022, was coordinated in Russia by the Social Technology Greenhouse association.

Associations do not always spontaneously voice specific requests for training. Often, a security incident, such as sensitive information leaks following a phishing attack or distributed denial of service (DDoS) attacks revealing website vulnerabilities, will make them turn to organizations such as Access Now or Frontline Defenders to request emergency assistance. These organizations then send their digital security advisor on-site to identify vulnerabilities and protection needs. This audit can lead them to apply for a grant from the donor organizations and/or digital security training.

Formats and Methods

Training can be delivered in several formats. Either it is a thematic training course for several organizations (represented by one or several members, often including an IT administrator) or individual activists, focused on a

particular challenge that is seen to be important in the field (e.g., "being a journalist in conflict zones" or "business travel abroad"). Or it is a training course for a single association in its entirety, which may last several days. The trainer goes on-site and starts with a security audit (risk analysis and needs assessment), which involves talking separately with the organization's management and IT manager, before going around to different staff to establish a list of hot spots and then moving on to a collective debriefing. This training results in the development of a threat model and the creation of an organization's own security protocol, which members of the organization are asked to follow:

> We had a very rigorous audit of our internal communications, use of smartphones and computers, working with instant messaging, encryption of data and devices. We were strongly recommended a certain type of instant messaging with encryption, for example Signal or Telegram. VKontakte.ru messaging has been permanently banned, although until three years ago some of our employees used VKontakte to communicate. The use of smartphones for sensitive communications has been banned. If a person starts talking on the phone, they can be reprimanded and reminded of the protocol to follow.[9]

Yet, apart from reprimands, there is little that organizations can do about those who ignore these instructions.[10] Given the significant lack of human resources, the high turnover in associations, and the considerable proportion of voluntary work, disciplinary measures such as dismissal, withdrawal of bonuses, or restriction of access to information, which are commonplace in the private sector, can hardly apply.

It is therefore crucial that the trainer's teaching be persuasive, personal, and tailored to each case. Some say that to develop recommendations that work and a security protocol that will be followed, it is important to base them on the history of security incidents that organizations and their individual members have faced. The primary factor determining the way users will apply digital protection tools is this personal experience of security breaches and their consequences, much more than their level of technical competence (Kang et al. 2015) Thus, lessons drawn from real-life examples of (anonymized) security incidents are fed into digital security training and

manuals. Various scenarios and role-playing games also inform these trainings and have even led to the development of an innovative "holistic security" methodology. This methodology, which is especially promoted by international organizations such as Frontline Defenders, shows their will to move away from the risk management methods developed in the private sector, which are deemed to be ill-suited to the world of activism and human rights NGOs.

The holistic security approach is a result of the reflexive and critical work carried out by the international community of trainers who share their experiences at specialized conventions such as the Internet Freedom Festival or RightsCon (organized by the NGO Access Now). The holistic approach differs from the tool-centered approach in particular, in which training courses are built primarily around recommendations for specific encryption tools or protocols (e.g. Tor, Signal, or PGP), irrespective of the precise context and threat model facing the individuals in question. The focus has therefore shifted to "integrating digital self-defence issues into more holistic approaches to security" (Hankey and O'Clunaigh 2013). The central role of the digital aspect of old training models was widely criticized by trainers, who began to prioritize the psychological, legal, and physical aspects, constructing security not as a stabilized and well-defined object but as an ongoing relational and contextual "work in progress" (Ermoshina and Musiani 2018). This, in turn, has had an impact on the funding and content of educational material (best practice guides). Russian trainers, among others, were very receptive to the holistic approach, given the legal and political context of their country. The most common risk for them is not a sophisticated computer attack but the seizure of electronic devices and the use of torture and various forms of psychological pressure to access data. Thus, psychological, physical, and legal aspects started to take center stage in training courses, which now focus on real-life situations.

> Here's an exercise I present to my trainees: you get your office door forced open, and what happens next, what are your different points of view? The VeraCrypt software is certainly a part of your defence and not the least, but it is probably also your door that is forced open, and the video surveillance that would have recorded all this and been sent somewhere to the security company, so that

there is a video record of this violence. From a psychological point of view, how do you react to the stress caused by this violence? And then from a legal point of view, if we have a flash drive in our pocket, do the police, with their search warrant, have the right to search our pockets?[11]

At the end of these courses the trainers may, for example, recommend not using complex cryptographic tools but simply installing a strong armored door and a surveillance camera at the office entrance.

AFTER THE RUSSIAN FULL-SCALE INVASION OF UKRAINE: NEW CHALLENGES AND THE REORGANIZATION OF PRACTICES

The Russian human and political rights situation, already tough before 2022, further deteriorated after the beginning of the full-scale invasion. Civil society actors were burdened by new laws and regulations on public expression. Specific censorship was introduced for all issues related in any way whatsoever to the invasion of Ukraine. Against the backdrop of the war, other laws have been passed, such as the law banning the "advertising" of LGBTQ+ identities to the entire Russian population, not just to minors. Surveillance was strengthened around online discussions that could undermine the integrity of the Russian territory. Finally, the harshest repression since the end of the USSR now targets all those who criticize Russian domestic and/or foreign policy.

Anonymity and Privacy under Debate

In this context, digital security trainers have raised the issue of anonymity, a longstanding subject of debate in activist circles, in radical terms. They now seem to fear that they, in turn, will also be targeted by the state, like the lawyers defending victims of state prosecution who have been threatened for "discrediting the Russian army" after uttering the word "war" in court.[12] They also worry about the safety of trainees who "still believe that we should remain like knights with our visors open."[13] Once in exile, these people think they are protected from the Russian authorities' arbitrary violence: "They don't take into account the dangers that their publications on VKontakte

represent for their social circles in Russia or for the people who re-post their publications. They also fail to understand that pressure on their relatives in Russia is a means to reach exiles."[14] Some activists prepare their relatives for possible searches: "I sent my mother instructions about the searches. I subscribed her to OVD Info and Meduza. Because they keep terrorizing you anyway, even when you think you're safe."[15]

Russian exiles sometimes become victims of transnational state repression involving online surveillance. These practices have already been studied, especially with exiled Iranian activists targeted by the authorities, both to discredit them internationally and to cut them off from their contacts at home (Michaelsen 2018). A Russian citizen was denied consular services by the Russian Embassy in Canada for participating in the Facebook group For the Beautiful Russia of the Future run by Russian exiles close to Navalny's team. The justification cited for this refusal was the danger that this exile represented for the security of Russia.[16] Other exiles, including digital freedom activists (such as the director of the Internet Protection Society) are wanted by the Russian authorities for "repeatedly violating the law against the discrediting of the Russian army" in broadcasts on YouTube and on their Telegram channels. Such charges can be problematic for people in post-Soviet countries, such as Georgia, Armenia, and Central Asian countries, as they risk being sent back to Russia. But they are also potentially problematic for people living in EU countries when they travel to countries deemed unsafe, such as Turkey.

Until two years ago, trainers advocated cautious use of social media, with limited publication of personal data and information (Bronnikova and Zaytseva, 2022). Today they recommend maximum anonymity for anyone fearing persecution in Russia, even in exile.

This recommendation is not welcomed by journalists, in particular, as being anonymous means putting an end to their career. This has become especially true after many independent Russian media were shut down in Russia (such as Echo of Moscow, Dozhd, before it reorganized in Riga and then in Amsterdam), and many journalists were forced to use YouTube to launch their own projects, whose success relies entirely on their prewar reputation. This tactic is often referred to as "security through publicity" and can

be effective, especially in the event of a lawsuit, as fame can play some role in the success of a support campaign and in raising funds for legal fees.

On the other hand, activists, especially those who remain in Russia, are overwhelmingly following this advice and seeking maximum anonymity because of the dangers that anyone opposed to the war in Russia now faces. This involves, among other things, moving to encrypted messaging systems that allow accounts to be created without providing a phone number: "I see more and more anti-war activists using (the messaging system) Element now. They've decided on their own that this is going to be their way of communicating internally. It's very promising, I hope it will become common practice after this is over."[17] Trainers are pleased to note that activists and NGOs in Russia have finally become serious about verifying participants' identity and controlling material security conditions (access to their premises, presence of surveillance cameras). There is every reason to believe that the war was a tipping point that forced activists, who had been skeptical about implementing repeated recommendations on digital security, to adopt self-defense tools and practices against the Russian state. We had already observed this "crisis-induced safety culture" effect during our investigation of journalists exiled from Crimea after its annexation by Russia in 2014. In interviews, these journalists described the annexation as a turning point after which they finally "took trainers' advice seriously" (Ermoshina 2024).

Certain habits nevertheless remain prevalent in exile. For example, Russian volunteers from associations helping Ukrainian refugees continue to use Yandex's messaging services, sometimes to communicate about refugees who have left the territories occupied by Russia. Others are reluctant to use Signal and secure messaging in general to communicate with potential funders, some of whom have been branded "undesirable organizations" in Russia, and thus prefer Telegram or WhatsApp. Many still keep a Russian phone number abroad, which is paired with various communication services and tools, despite security incidents identified as early as 2016 in Aleksei Navalny's team when the authorities accessed Telegram conversations using duplicate sim-cards.[18] Another factor in the loss of digital vigilance is time. Our study of Crimea showed that respondent's relationship to the space and the temporality of exile (especially during long conflicts, such as the

occupation of Crimea) contributed to a certain fatigue and a decrease in vigilance, which eventually led them to return to the tools and practices they used before the crisis (Ermoshina 2024).

Conflicts regularly arise around confidentiality and security in associations' internal rules between those who advocate the need to be wary of even very hypothetical dangers, on the one hand, and on the other, those who emphasize the need for transparency. Trainers see this as an "eternal debate" in which newcomers to associations,[19] who do not have the experience of years of searches and repression, invariably tend to defend the "nothing to hide" position (Bronnikova and Zaytseva 2021, 2022). Until very recently, despite the best efforts of digital rights advocates such as Roskomsvoboda and digital security trainers to publicize these notions,[20] the rights to anonymity and privacy online were not considered values to be defended—except in radical left-wing activist circles, which had been promoting a "culture of security" since at least 2010. The "privacy paradox" that computer science researchers have observed in lay users thus seems to apply to the activists and journalists studied here. Despite various experts and activists constantly warning users about threats to privacy in digital environments (especially on social networks), these risks remain abstract and uncertain in their minds. They are unfamiliar with privacy technologies and use them very little. However, they tend to volunteer a lot of personal information without being forced to do so (Carey and Burkell 2009).

We must also bear in mind that in the very particular context of exile, people forced to leave their country and abandon their previous life often feel the pressing need to keep a certain number of points of reference to continue living their life. Telegram or WhatsApp groups and chats with relatives in Russia or around the world allow them to feel anchored and stable in ever-changing conditions: "You shouldn't put pressure on people. After all, these WhatsApp groups are pretty much the only thing they have left in this new world."[21]

The New Role of Russian Organizations Located Abroad

In this context, Russian NGOs defending digital freedoms and providing technological support to activists, now located abroad, are acquiring a pivotal role as relays between civil society actors remaining in Russia and the

rest of the world. While NGOs such as the Internet Protection Society and Roskomsvoboda have never shied away from dealing with political issues, or at least working with public opinion (the former was close to Navalny's team, and the latter stems from the Russian Pirate Party [see (Daucé 2022]), the Social Technology Greenhouse claimed to be rooted in the fields of social entrepreneurship and civic tech. Yet since the beginning of the full-scale invasion of Ukraine, the discourse of the Greenhouse's members has changed completely; they now claim that it is impossible to maintain political neutrality in the context of the war.[22] The Russian authorities immediately recognized the NGO's politicization by labeling the Greenhouse's content director, Natalia Baranova—who is also an activist of the feminist antiwar movement (FAS)—as a foreign agent. They also blocked the Greenhouse's website (first with a .ru extension and now with a .org extension) following the publication of an article titled 'How to Escape Mobilization."[23] The association did not adopt this political stance immediately after the onset of the all-out war, as employees and other members first had to be exfiltrated to safety. "We hardly did anything in the first few months because we had to organize the Greenhouse's exile, starting with very practical questions such as negotiations for European visas, finding a place to stay and opening bank accounts. It was very hard because the context was not at all favourable and we had to act quickly."[24]

The NGO is now playing a crucial role in maintaining links with civil society actors who have remained in Russia, especially in terms of security. Since February 24, 2022 it has organized many webinars and training sessions on new digital security issues, particularly for teams scattered between Russia and the various places of exile. The NGO has recruited a full-time security trainer, a testimony to the importance this issue has acquired for them. In the Russian context, with hardly any trainers or security experts left in the country, the opportunity to access these distance learning courses allows those associations that have stayed in the country to remain active. However, members of the Greenhouse have noticed that the digital architectures of these associations now tend toward simplification, including in terms of security protocols. In conditions of chronic lack of resources, especially financial, after all the international and Russian foundations and

organizations independent of the State have left, and faced with increased repression, most associations adopt survival rules or quite simply disappear:

> We see several types of behaviour. The first is survival. Total respect of all laws, self-censorship, self-limitation. The waiting game is the least risky position, but it is also the least militant. The second position is collaboration with the regime. . . . The third model is that of clandestine anti-war organizations that operate in absolute anonymity and total autonomy. The fourth outcome is the gradual dissolution of the sector. Over the last ten years, it had become prestigious to be part of civil society NGOs; we saw people leaving big companies and coming into the sector from the business world. Now these people are just leaving again.[25]

The Greenhouse also provides media and logistical support to collectives remaining in Russia, who are trying to act in a context of extreme economic and political precariousness:

> Often we can't even fathom how difficult the situation is inside the country. Foreign funders are leaving, SWIFT[26] has been cut off, donations are decreasing. There are no independent media left inside and NGOs have nowhere to go to tell their stories. Some teams have been split up: for example, the IT departments have left, while lawyers, psychologists, and professions that provide assistance continue to work in the field. The new laws risk criminalizing any cooperation with human rights projects.[27]

Providing this support has been further complicated by the departure of many foreign technology companies from Russia, the blocking of payment systems (such as Google and Apple Pay) by the digital giants, and difficulties registering domain names for Russian websites,[28] It is also becoming impossible to provide technological support to Russian civil society actors, due to the end of the TeploDigital program coordinated by the Greenhouse. This program provided NGOs with almost free access to Google and Microsoft services and software, which people like for the convenience they offer in organizing digital ecosystems (e.g., Google Workspace) or promoting products online (Google Ads) (Bronnikova and Zaytseva 2021).

To the surprise of associations such as the Greenhouse, their audiences have dropped drastically since the massive blocking in Russia of Facebook and X/Twitter and of their own websites.[29] Despite their efforts over the

past few years, they found out that most other Russian associations still did not know how to use blocking bypass tools such as VPNs, which made it impossible for them to access the digital security information published on the Greenhouse's website. To overcome this problem, the Greenhouse, with the support of its partners abroad, joined the organizing committee of the Internet Without Borders conferences, which aim to bring together associations, journalists, and activists with computer development specialists with the necessary knowledge of tools to circumvent blocks.

Yet the efforts of these NGOs and activists in exile to help those left behind in Russia cannot suffice to guarantee the safety of their entire network, especially when dealing with new, horizontal, fairly unstructured initiatives such as FAS,[30] the feminist antiwar movement:

> We have women activists who have been victims of repression, arrest, torture. They are aware of the risks. The coordinators can only help to better prepare the actions, the security protocols, to remind them that certain dangers exist. But there are activists who are not part of the FAS who call us out because of the ongoing criminal cases against us. Yet we're constantly posting tips on our Telegram channel about digital safety, about offline safety. This way of placing the blame on the anti-war movement, when it falls squarely on the repressive state, is not acceptable.[31]

CONCLUSION

The Russian state's security and policing practices have been hardening consistently over the past few years. With the digital sovereignty project involving the gradual construction of the information security doctrine, dissenting members of civil society positioned themselves against the state offensive by deploying a range of digital security tools, practices, and know-how. Turning away from Russian platforms in favor of the tools proposed by GAFAM/MAGMA companies and, more recently, decentralized and self-hosted solutions, has been one of the main characteristics of this security culture.

Over the last decade, security issues have gradually become a major issue for civil society in general and no longer just a marginal concern of a small minority whom others thought were paranoid. This was the result of

a long and laborious process carried out by groups of actors, of whom we have endeavored to broadly sketch a portrait: trainers, technical experts, NGOs, and professionals of the media public space. The role of international organizations has been crucial and remains so today, despite the context of international sanctions.

This movement, which characteristically features international exchanges and circulation of standards, tools, and practices, highlights several important aspects of digital security per se, two of which stand out. The first is its processual, temporal, and dynamic nature: it is not a state of safety that is given once and for all but an ongoing process of learning and readjusting, interspersed with tests, failures, and the search for new paths. The second is its contextual and relational nature: the risks and especially the consequences of security breaches are never individual but depend largely on the networks in which organizations operate.

While the Russian activist and journalistic organizations we studied prior to February 2022 had the organizational capacity to implement security recommendations in a more or less controlled way, exile has impacted the movements' architectures and administrative structure. The international and decentralized state of the antiwar movement introduces new risks and redefines responsibilities. The new activist organizations that have emerged since, such as the FAS, find themselves caught between a duty to protect their activists and the impossibility of managing a coherent implementation of security protocols. This is due to the very architecture and dynamics of these horizontal movements, with members scattered among different countries, and among whom degrees of mastery of digital tools and perception of the "security culture" prove to vary widely.

By exposing them to risk, war and exile have had a strong impact on security trainers. The themes and formats of training courses have also been redefined (although the groundwork for this transition had been laid during the Covid epidemic, with most courses taking place online in 2020–2021). Nevertheless, as we have shown, digital security know-how has been built up, analyzed, and shared not only by specialized NGOs such as the Greenhouse but also by organizations and individuals (opinion leaders) abroad. More

than ever before, this common know-how appears to be of vital importance to communities that are now dispersed and distressed.

NOTES

1. https://www.accessnow.org/letter-us-government-Internet-access-russia-belarus-ukraine/
2. GAFAM is an acronym commonly used to refer to five major US technology companies: Google, Apple, Facebook, Amazon, and Microsoft. The acronym MAGMA (Microsoft, Apple, Google, Meta, Amazon) has also been in use since 2022, following the introduction of the Meta brand to group together Facebook, WhatsApp, and other services.
3. For safety reasons, in view of the current threats facing these associations, we will not name them here.
4. https://ru.wikipedia.org/wiki/Информационная_безопасность. (note that this Wikipedia page exists only as a page automatically translated from the English page for "digital security").
5. https://ru.wikipedia.org/wiki/Информационная_безопасность
6. An alliance of five English-speaking countries (the United Kingdom, the US, Canada, Australia, and New Zealand), with the aim of sharing information.
7. Interview with a digital security trainer, March 2019, Minsk.
8. E.g., Soros Foundation, Norwegian Helsinki Committee, Freedom House, European Commission, British Embassy, Norwegian Embassy, UNHCR (United Nations Refugee Agency).
9. Interview with an international NGO employee, August 2019, Moscow.
10. However, there are some rare cases of sanctions for serious misconduct causing a security breach.
11. Interview with a digital and physical security trainer, March 2020, Paris.
12. "Presledovanie rossijskih advokatov posle načala Rossiej vojny protiv Ukrajny (The Persecution of Russian Lawyers after Russia Started the War against Ukraine), Pravo na zaŝitu, June 16, 2022, https://www.defenders.by/presledovanie_rus_advokatov; Maria Bontsler, "'Ne nadjtes'—â ne uedu' štraf advokaty is Kaliningrada po donosu sud'y" ('Don't count on me leaving.' Kaliningrad Lawyer Fined after Being Reported by Judge), Sever.Realii, August 24, 2022, https://www.severreal.org/a/ne-nadeytes-ya-ne-uedu-shtraf-advokatu-po-donosu-sudi/31990844.html.
13. Interview with a Russian online trainer, October 2021.
14. Interview with a Russian online trainer, October 2021.
15. Interview with antiwar activist, September 2022, Tbilisi.
16. "Posol'stvo RF v Kanade otkazalo rossiânke v prieme iz-za 'ugrozy bezopasnosti'. Povodom dlâ otkaza stala podpiska na gruppu 'Za prekrasnuû Rossiû buguŝego.'" (The Embassy of the Russian Federation in Canada has Refused to Accept a Russian Citizen for "Threatening

security." At Issue Was Her Subscription to the Group "For the Beautiful Russia of the Future"), Meduza, January 27, 2023, https://meduza.io/news/2023/01/27/posolstvo-rf-v-kanade-otkazalo-rossiyanke-v-prieme-iz-za-ugrozy-bezopasnosti-povodom-dlya-otkaza-stala-podpiska-na-gruppu-za-prekrasnuyu-rossiyu-buduschego.

17. Interview with Russian trainer, November 2022, online.
18. https://medialeaks.ru/2904yut_durov/. (The website has been taken down. However, this publication can be accessed via the Wayback Machine of Internet Archive at https://web.archive.org/web/20230603081346/http://medialeaks.ru/2904yut_durov/. Please refer to our Note on the Availability of Sources.)
19. In the association where we carried out the participant observation, founded in April 2022 in one of the countries of Russian exile and arrival of Ukrainian refugees, the majority of the volunteers had no previous experience of working or volunteering in the field of human rights advocacy.
20. https://roskomsvoboda.org/en/about/
21. Interview with a Russian online trainer, October 2021.
22. Interview with Aleksei Sidorenko, June 2022, Warsaw.
23. "Kak izbezhat' mobilizatsii na voynu. Pamyatka aktivistam" (How to Avoid Mobilization for War. A Memo for Activists), https://te-st.org/2022/09/21/mobilization/
24. Interview with Aleksei Sidorenko, June 2022, Warsaw.
25. Aleksei Sidorenko, "Počinit' Rossiû po čut'-čut' uže ne polučit'sâ: kak vojna povliâla na graždanskie iniciativy" (We Won't Be Able to Fix Russia: How the War Has Impacted Civil Society Initiatives), January 19, 2023, https://reforum.io/blog/2023/01/19/pochinit-rossiyu-po-chut-chut-uzhe-ne-poluchitsya-kak-vojna-povliyala-na-grazhdanskie-inicziativy/.
26. The Society for Worldwide Interbank Financial Telecommunication, the network through which messages to initiate international payments are exchanged.
27. Natalia Baranova, "Graždanskie iniciativy v god vojny" (Civil Society Initiatives during the War Year), https://www.youtube.com/watch?v=TMa24gu_IlEandt=2836s.
28. According to one of the trainers interviewed, the website of his client (a human rights NGO) was disconnected by its foreign host because the NGO was Russian. Interview, online, November 2022.
29. Discussion with members of the Greenhouse, November 2022, Paris.
30. FAS stands for Feministskoie Antivoennoe Soprotivlenie.
31. Discussion with one of the FAS activists, September 2022, Tbilisi.

REFERENCES

Bronnikova, Olga, Bella Ostromooukhova, Perrine Poupin, and Anna Zaytseva, eds. 2022. "Militants face à la 'souverainisation' numérique. Réactions et nouvelles mobilisations dans l'ex-bloc

socialiste (Russie, Ukraine, Cuba)." *Terminal* (134–135). https://journals.openedition.org/terminal/8484.

Bronnikova, Olga, and Anna Zaytseva. 2021. "'In Google we trust'? The Internet Giant as a Subject of Contention and Appropriation for the Russian State and Civil Society." *First Monday*, 26 (5).

Bronnikova, Olga, and Anna Zaytseva. 2022. "'Se protéger ou périr'. Transformations des savoir-faire en sécurité numérique des militants et journalistes russes indépendants (2017–2022)." *Terminal* (134–135). https://journals.openedition.org/terminal/8587.

Carey, Robert F., and Jacquelyn Ann Burkell. 2009. "A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments." In *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock. Oxford University Press.

Daucé, Françoise. 2022. "Pirater l'autoritarisme. Trajectoires de lutte pour les libertés numériques dans la Russie de V. Poutine (2009–2022)." *Terminal* (134–135). https://journals.openedition.org/terminal/8549.

Doktrina informacionnoj bezopasnosti Rossiiskoj Federacii. 2000. "Doctrine of Information Security of the Russian Federation, adopted by the President of the Russian Federation on 9 September 2000." http://base.garant.ru/182535/.

Doktrina informacionnoj bezopasnosti Rossiiskoj Federacii. 2016. "Doctrine of Information Security of the Russian Federation, adopted by the President of the Russian Federation on 5 December 2016." http://static.kremlin.ru/media/acts/files/0001201612060002.pdf.

Ermoshina, Ksenia. 2024. "Voices from the Island: Informational Annexation of Crimea and Transformations of Journalistic Practices." *Journalism* 25 (3): 528–546.

Ermoshina, Ksenia, and Francesca Musiani. 2018. "Hiding from Whom? Threat Models and In-the-Making Encryption Technologies." *Intermédialités/Intermediality* (32).

Ermoshina, Ksenia, and Francesca Musiani. 2022. *Concealing for Freedom: The Making of Encryption, Secure Messaging, and Digital Liberties*. Mattering Press.

FIDH. 2018. "Russie: 50 nouvelles lois antidémocratiques lors du dernier mandat Poutine." March. https://www.fidh.org/fr/regions/europe-asie-centrale/russie/russie-50-nouvelles-lois-antidemocratiques-lors-du-dernier-mandat.

Hankey, Stephanie, and Daniel O'Clunaigh. 2013. "Rethinking Risk and Security of Human Rights Defenders in the Digital Age." *Journal of Human Rights Practice* 5 (3).

Kang, Ruogu, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "'My Data Just Goes Everywhere': User Mental Models of the Internet and Implications for Privacy and Security." Paper presented at the Symposium on Usable Privacy and Security, (SOUPS) Ottawa, Canada, July 22–24.

Lokot, Tetyana. 2020. Articulating Networked Citizenship on the Russian Internet: A Case for Competing Affordances. *Social Media + Society*, 6 (4).

Limonier, Kevin. 2016. "Le cyberespace, nouveau lieu d'affirmation de la puissance russe." In *La Russie: vers une nouvelle guerre froide?*, edited by Jean-Robert Raviot. La Documentation Française.

Michaelsen, Marcus. 2018. "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State." *Globalizations* 15 (2): 248–264.

Ristolainen, Mari. 2017. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West." *Journal of Information Warfare* 16 (4): 113–131.

5 DATA JOURNALISM: INVESTIGATING IN A CENSORED PUBLIC SPACE

Françoise Daucé

In a December 2022 article titled "War in Numbers," journalists from the media outlet *Important Stories* (*Vazhnye istorii*) endeavored to assess the Russian army's losses in Ukraine. Working from open sources with volunteers, they had collected and verified information on the number of military casualties. They counted 9,023 names. As the editors explained, "This figure does not reflect the real losses of the Russian army in Ukraine (which the Ukrainian forces estimate to be over 100,000), it covers only publicly known cases. But this already far exceeds the Ministry of Defence's official estimates."[1] Like many other articles in the Russian press, the text collates digital data to expose the Russian regime's murderous campaign in Ukraine. This digital coverage of the war is part of a shift that has been underway since the 2010s in the Russian media. As the political departments of the main Russian newspapers were taken over (Koltsova 2006; Roudakova 2017; Chupin and Daucé 2016; Daucé 2019), the use of digital data came to represent hope for the revival of investigative journalism. According to a definition proposed by Russian media themselves, data journalists are those who, in addition to traditional journalistic skills, also know how to work with digital sources: they have basic skills in statistics, data analysis, and programming, which they use in their work.[2]

In a time of deep concern about the information circulating on the internet and doubt about its veracity, data journalism, as a new form of investigative journalism, is on the rise around the globe (Giry 2017). The term itself is polysemous and encompasses diverse media practices ranging from the statistical use of digital data to open-source intelligence (OSINT) (*Hérodote* 2022). Given the suspicion around "fake news," data journalism feeds into

a "new rhetoric of objectivity" (Vauchez 2019), which is sometimes based on a "fetishization of the data" itself (Lapoix 2014). Data-driven inquiry is part of a long-standing movement to digitize knowledge (Anderson 2018) in journalism, social sciences (Boullier 2015), or expertise more generally. Journalists rely on data to mitigate their dependence on informants, rein in their biases, and ensure that their work is accurate. These journalists represent a model of sober and factual journalism based on exhaustivity and accuracy, as opposed to the inspired and corrosive presumptuousness of political journalism (a reflection of the opposition between the two historical models identified by C. Lemieux [1992). The use of data is the subject of infographic and technical (code) training in which data are equated with facts. Diverse sources are used here, whether the data are open, purchased, or leaked (Loveluck 2016). Many media outlets have thus revealed scandalous realities using the specific socio-technical forms that are databases. These new sources empower journalists "surveilling the surveillers," in a logic of "sousveillance," an "inverse panopticon," as Steve Mann (2002) put it (see also Alloing 2016). It allows citizens to use digital devices to "look from below" at state and industry powers. Although data journalism is developing in Western newsrooms, its future is still debated. Several scenarios are emerging: the broad development of data journalism, this type of journalism remaining a niche, and data journalism being outsourced to companies outside newsrooms (Stalph and Borges-Rey 2018). Critics have even argued that this brand of "journalism on screens" can be considered an outcome of "digital liberalism" (Boyer in Bounegru and Gray 2021).

While an abundant literature on data journalism in English-speaking contexts is now available (Gray et al. 2012; Anderson 2018; Young et al. 2018; Ausserhofer et al. 2020), it does not cover Russia in any depth. Yet the Russian case raises interesting issues. In a context of strong political and infrastructural control (Oates 2013; Daucé and Musiani 2021), Russian journalists are showing a growing interest in data, as evidenced in the 2010s by the emergence of several pure-player online media outlets claiming to be specialized in this new field. Some of the academic works currently available document these dynamics (Begtin 2013; Valeeva 2017; Shilina and Shilina 2020; Dovbysh 2021). Constraints on citizens and journalists increased with the outbreak of the war

against Ukraine in February 2022, and especially with the adoption of the law on "fake military news" in March 2022. In this context, access to digital data became a key resource for investigations into the frontline and troop movements. Journalists who have fled abroad to escape criminal prosecution in Russia are away from their field of investigation and continue to work from a distance through sources available online. Some run statistical processing on accessible data; others carry out online investigations following the example of the citizen organization Conflict Intelligence Team (founded by Russian citizens after the start of the war in Donbass in 2014), which demonstrates the interest in open-source investigations in the context of armed conflicts. Data processing in turn gives rise to struggles between governments and journalists around access to public data, the quality of sources, private data purchases, and control over leaked data. Data are therefore "enrolled"—in the sense used by Madeleine Akrich, Michel Callon and Bruno Latour (2006)—in conflicts of appropriation and interpretation that shed light on the political stakes in their production and use.

This chapter presents a socio-history of data journalism in Russia from a perspective that includes the innovations, resistances, and trials it encounters. It describes the practices and reflections of its actors, in large part based on interviews conducted from 2018 to February 2022 in Moscow, online, or outside Russia with investigative data journalists working for the editorial offices of the media outlets Proekt, *RBK*, BBC Russian service, *Novaia Gazeta*, Important Stories, and The Insider—all of which have been placed under "foreign agent" or "undesirable organisation" status by the Russian authorities—as well as interviews with Russian open data activists from the InfoKultura foundation and collaborators of A. Navalny's Anti-Corruption Foundation. It also draws on the observations of online sources in Russian (ethnography of social networks and study of Telegram channels, including the Open Data RU channel).

DATA JOURNALISM AS A TRANSNATIONAL MOVEMENT

The development of data journalism in Russia is a part of an international movement that, since the early 2010s, has converged with the concerns

of data activism (Milan and Van der Velden 2016). New ways to objectify investigation have emerged, aimed at exposing abuses of power in society (Carson 2019). By taking advantage of the massive digital traces that are now available, data-driven journalistic inquiry has renewed the practice of journalism, departing from traditional methods that have become obsolete.[3] Digital sources are a response to the many challenges faced by journalists: lack of legitimacy, suspicion of fake news, the acceleration of media time, and so on. Since the mid-2010s, promoters of data journalism have perceived its "quantitative turn" (Coddington 2015) as a source of new opportunities enabling them to offer interpretations that are independent of official data, to act as a reasoned filter faced with the deluge of data, and to reveal unseen realities (Gray et al. 2012). In the sociology of journalism literature, data-driven inquiry is seen to profoundly transform the relationship between journalists and their sources, as it affords them an opportunity to distance themselves from relationships that are considered asymmetrical (Parasie and Dagiral 2013a). In Russia, more than anywhere else, the use of data in journalism is associated with these perspectives and carries hopes of fighting censorship, disinformation, secrecy, and corruption (Yablokov 2018). The Russian case thus supports the findings of studies of a "political economy of data" in other contexts (Loveluck 2016)."

THE MEDIA NETWORKS OF INVESTIGATIVE CONSORTIA

The practices of data journalism vary widely, from big data processing to open data analysis and observation of the many digital traces left by online browsing. A common purpose of all these practices is to shed light on "moral violations" (Parasie and Dagiral 2013b). Participation in the development of data journalism is a transnational practice (Bigot 2017) through which journalists of different nationalities may become part of international investigation collectives and have a role in their investigations. Processing work on large data sets is generally carried out by international collectives that developed during the 2010s, such as the Florida-based International Fact Checking Network (IFCN), the Maryland-based Global Investigative Journalism Network, the International Consortium of Investigative Journalists

(ICIJ), and the Danish SCOOP network. In the Western world, bridges have been built between the worlds of IT and journalism. In the US first, and later in the United Kingdom, programmers have joined the editorial staff of major newspapers or independent organizations producing information (Gray et al. 2012). Russian journalists are joining these collectives, in which they contribute to international investigations involving Russian protagonists, for which data in their language need to be processed. In spring 2016, the independent newspaper *Novaia Gazeta* took part in the Panama Papers investigation. The ICIJ processed the 11 million documents collected through optical character recognition (OCR) and turned them into a huge database. *Novaia Gazeta* participated in the publication of documents related to the Russian side of it.

Digital investigative journalism inspired by open-source investigation (OSINT) methods searches for scandals and revelations. During the Skripal case in Britain, the Russian media outlet The Insider investigated with Bellingcat's team to reveal the names of Russian intelligence personnel involved in the assassination attempt. The website, founded in 2013 by freelance journalist Roman Dobrokhotov, investigates public and leaked data with the help of independent, volunteer contributors. Journalists rely on open-source software, images, and databases, including Google Earth and YouTube. Bellingcat (from the expression "to bell the cat") relies on the work of citizen journalists, most of them self-taught, whose work, beyond informing the public, also unearths evidence for criminal proceedings.[4] Thanks to this cooperation, Russian investigative websites have gained international recognition and have been awarded prizes. The Insider website was awarded the Council of Europe's Innovation prize (2018), the European Press Prize (2019) for its investigation of the perpetrators of the Sergei Skripal poisoning in Salisbury,[5] and the Free Media Award (2019).

RUSSIAN INVESTIGATIVE JOURNALISM'S PASSION FOR DIGITAL TECHNOLOGY

The enthusiasm for data journalism in Russia is commensurate with the closure of the Russian public space, which makes access to physical informants

and sources increasingly difficult. As early as 2013, Sheila Coronel of the Global Investigative Journalism Network asked, In the digital age, "can the worst of times for media and political freedoms in post-Soviet Russia also be the best of times for watchdog reporting?"[6] Elizaveta Osetinskaia, journalist and founder of the online media outlet The Bell, also believes that investigative reporting is more dynamic and of better quality than ever before.[7] New media projects are emerging in the Russian context (Rostova 2019); they consider data as a factor of "mechanical objectivity," which allows for any suspicions of investigators being subjective to be lifted. Many Russian journalists in the "independent" media have been training in data-driven investigation since the mid-2010s.

Journalists at RBK, Meduza, *Novaia Gazeta*, and the BBC Russian Service, as well as investigative websites such as The Insider, Mediazona, Proekt, and Important Stories all use online data. According to a data journalist we interviewed, "New media outlets are mostly the ones adopting data journalism and developing new formats. Big newsrooms like *Vedomosti* or *Kommersant'* don't do that much of it."[8] In 2019, the website *Novaia Gazeta* created a dedicated data journalism section within its editorial office.[9] Journalists write code, collect data, and visualize it. They are part of the broader major investigations department. As one journalist explained, "We often deal with data in our inquiries, it makes for better quality investigations." On the reason for opening this section, Alesia Marokhovskaia (who would later join the investigative media outlet Important Stories, founded in 2020) explains: "Western media have long known that data have many stories to tell . . . but for that you need specialized people, data-journalists."

The website Proekt, which Roman Badanin launched in 2018 after being successively dismissed as editor-in-chief of several news media outlets for political reasons, is also part of this movement. It defines itself as "an independent media outlet, bringing together investigative journalists and reporters. We do what we know we can do: find what is hidden and important, and tell you about it. We believe that this is essential because there are hardly any media that deal with complicated and dangerous issues in Russia."[10] The editorial staff consists of about ten journalists who publish an investigative article every week. As Roman Badanin explained in 2018,

Proekt is based on "big data" (*bolshie dannye*) investigations.[11] The methodology in such cases facilitates a quantified and objective rendering of the truth. Thus, many of their articles present aggregated data that are compiled and made visible through infographic processes.

In the Russian case, data-driven investigations are not conducted only by journalists; they also afford an opportunity for opposition activists to contribute. The best known of them, A. Navalny, became known by exposing the corruption of the country's elite through online investigations. His is a uniquely Russian example, with his movement taking the novel form of a hybrid between a partisan political movement, an anticorruption activist association, and an investigative media outlet. As such, it constitutes an original form of resistance in the context of digital authoritarianism. This multifaceted composition allowed Navalny's Anti-Corruption Foundation (FBK) to conduct its own high-profile investigations in Russia and then to continue working remotely after its main activists went into exile. From abroad, they have carried on working on transnational issues, most notably investigations into money laundering from East to West, mobilizing registers and databases in several countries, including France. The FBK characteristically controls its entire chain of disclosure, from data research to publication. By compiling digital sources, it leads virulent investigations targeting the country's leaders in a populist vein (Glazunova 2020). They focused, for instance, on Prime Minister D. Medvedev in 2017,[12] and on the security services who were tasked with poisoning Navalny in 2020.

In terms of audience, online investigation media are achieving significant success, if we are to believe the metrics of the company Medialogia, which show the various editorial offices' relative renown. Between January and June 2021, the websites Navalny.com, Theins.com, Zona.media, Novaya Gazeta, and Proekt were regularly among the most quoted sources on Russian social media. The Important Stories website is gaining popularity not only for its investigations into corruption in power circles but also for its data on social and environmental inequalities. In July 2021, Roman Dobrokhotov (The Insider) and Roman Badanin (Proekt) were among the top 10 most quoted journalists in Russia.[13]

IS DATA JOURNALISM A TECHNICAL UTOPIA?

In the Russian context, where the media field is politically manipulated and control over the media is tightening, this interest in digital journalism relies on the teaching of statistics, coding, computer graphics and quantitative source analysis. According to a journalist from Znak.com, "working with data almost turns journalism into an exact science."[14] Such technical support allows journalists to revive the hopes that the internet bore in its early days (Flichy 2012; Loveluck 2015), when confidence in the virtues of digital technologies was strong. However, they also raise the question of reflexivity regarding the data they manipulate, which is often taken at face value (Lowrey et al. 2019).

THE DEVELOPMENT OF TRAINING IN DATA JOURNALISM

Data journalism was gradually institutionalized over the 2010s, with the development of teaching programs, training courses, awards, and online communities (Bounegru and Gray 2021). In Russia, it was supported by the creation of a university course (a master's degree in data journalism was set up at the National Research University Higher School of Economics in 2016),[15] as well as the development of online investigation methods training at the interface of programming and journalism and the introduction of specialized journalists in editorial offices. In March 2016, the first data journalism hackathon was held in Moscow on the initiative of A. Kudrin's Civic Initiative committee and the Higher School of Economics. Additionally, the Telegram channel *Data Zhurnalistika* (DDJ Russian) has been a space to share knowledge and reflection around data since August 2019. It is administered by Anastasia Valeeva, who invites its members "to discuss current issues in Russian language data journalism, share material and tips, and create teams."[16] In January 2020, journalist Yulia Apukhtina asked this community, "What is quality in data journalism? The requirement for statistical reliability, the ways in which links and datasets are made and published. Should scientific requirements be applied to investigative journalism, and to what degree? Where does statistical illustration end and research begin?"[17]

The survey method sometimes becomes an integral part of the article. This is evidenced in the methodological boxes featured with surveys on the websites of The Insider, Proekt, and *FBK*. The Important Stories website even offers a "Workshop" section for its readers to learn about data analysis in Excel, visualization and mapping in Datawrapper, and programming in Python.[18] Reading these technical boxes and talking to the journalists at these outlets, one sees how diverse the data they use are. This is not peculiar to the Russian context; research in North America has yielded similar findings (Parasie 2013). The work on data itself is based essentially on learning code—that is, how to harvest and clean data, build databases or design visualizations. As Alesia Marokhovskaia explained, "Data journalism is journalism, except you don't talk with people but with data . . . and for that you need to know its language. Usually, it's the programming language Python." Egor Skovoroda, a journalist for *Mediazona*, attended a training course titled "Python for Data Analysis" in February 2020. While he remembered scoffing at Excel spreadsheet training a few years earlier, he then said that *Code for Dummies* had become his bedside book.[19] As he explained, "For investigative journalists, Python is the new English, not knowing it is plain shameful." One of the journalists who published articles for Proekt had a background as a computer developer and could code in Java and Python. She explained that her dual background in business journalism and programming allowed her to work with large amounts of data.[20]

In addition to statistical data, Russian journalists are broadening their sources and are interested in all digital traces available online: "OSINT activity is used by investigators but also by journalists, IT and global security professionals, and by the banking sector to detect potential fraud, scams, phishing or money laundering."[21] Russian journalists now benefit from the availability of digital analysis tools for these practices. In April 2020, then-BBC correspondent Andrei Zakharov conducted a webinar titled "How to Investigate Covid19 without Leaving Home: The OSINT (Open Source Intelligence) Method." Zakharov is known for his investigation into the FSB Fund's crypto-currency exchanges (which lost $450 million on the WEX exchange platform) and his publications about E. Prigozhin's troll factories. As he explains, "Investigations are necessary for serious media outlets because

they create a reputation in Russia and in the world. . . . It takes time to do good investigations. You have to generate hypotheses, try to verify them, accept failures, look elsewhere. . . . It's true that it's hard on the morale . . . in addition, you constantly have to improve your use of instruments."[22]

Finally, there is an aesthetic dimension to this data work: "We strive to make our content beautiful . . . and understandable."[23] Use of data comes with the need to visualize the statistics obtained through computer graphics (Théviot 2020). Through investments in forms and the invention of visualization tools, journalists are able to show that which was previously invisible.

THE OPPORTUNITIES AFFORDED BY OPEN, PURCHASED, OR LEAKED SOURCES

Data-driven inquiry investigates available sources. The most directly accessible are open data, made available by administrations in the wake of the recommendations issued at the Sebastopol, California, meeting in 2007, when digital activists called for the "liberation" of public data as soon as they were produced and in their entirety. The term "open government data" emerged, and portals for publishing public data were opened. Russia was also part of this movement, and in the 2010s it launched an open-data policy aimed at boosting economic development—not at encouraging counterexpertise within civil society. In 2011 the portal open.gov.ru listed its achievements in terms of open data. In 2013 the city of Moscow launched the open-data platform data.mos.ru., and similar projects followed in various parts of the country. In 2014 the data.gov.ru website opened. Massive volumes of data were published, such as the Rosreestr database (the register of property rights).

These open data are prime sources for journalists investigating fields such as public procurement, legal offences, social inequalities, and medical care. Activists and entrepreneurs defend the opening of public data in Russia and set up initiatives to put forward their content. In a French institutional report titled "Russia: From Glasnost to Open Government. Progress in transparency," V. Ma-Dupont stated that Russia was firmly committed to the open-data revolution, going as far as hosting the Open Data Summit in

December 2015.[24] This openness was in line with the action D. Medvedev took as head of the Russian state between 2008 and 2012, and was backed by economic arguments focused on attracting investors and generating new financial flows.

The media took this openness seriously and collected and analyzed the data made available. Elizaveta Osetinskaia, founder of The Bell project, commented, "We now have a lot of databases. We have information on public tenders. We can find a lot of information about the structures of private companies."[25] One of the journalists we interviewed explained, "From 2014 onwards, the organs of power started to actively publish a lot of data. In what form? The decisive factor was the opening of the public procurement system, where almost all the data on public budget spending could be found. . . . Naturally, we started working with this data on public contracts."[26] Not all surveys based on open data are meant to fight the authorities, but analyzing them helps to document social issues. We see this in the RIA-Novosti data development studio's project Who Pays for Pensions?, Merkator's project on the age of housing in Moscow, the Demoscope project on road accidents, the Yandex statistics from its search engine,[27] and the many articles published by the new online media.

While public data are respectable journalistic sources, stolen, purchased, or leaked data inform the most explosive of investigations. Leaked data circulating in the Russian digital space shed light on the work of hackers who manage to publish hidden sources. Some journalists speak of using data leaks or purchasing data on the darknet. In a country where the grip of the security services is so strong and where it is mandatory to keep personal data on Russian soil, the information harvested by surveillance companies is highly coveted. Poor protection of personal data, which has been denounced by defenders of digital freedoms, means that there are considerable quantities and varieties of available data. Paradoxically, this shortcoming, which is due to a lack of regulations on data management, affords opportunities for investigative journalists to collect a variety of information on their subjects. As journalist A. Zakharov explained in December 2020, "In Moscow, we realize that the population is under a massive surveillance system. One example of this is video surveillance data with facial recognition. . . . It is

very easy to find out where a person lives."[28] He cited the example of the wifi services in the underground, which make it possible to trace a traveler's route throughout the city, and the prices of these data: 1,000 roubles for passport data, 15,000 roubles for the list of passengers on a plane.[29] A. Navalny made a political case out of it. In December 2020, he stated, "Thank the Yarovaya law that allowed corrupt members of law enforcement units to freely sell data from our mobile phones or from airlines"[30]—data that he used for his own foundation's investigations.

POLITICAL STRUGGLES OVER DATA INTERPRETATION AND OWNERSHIP

Data inform investigations that bring to light corruption among the government authorities, malpractice among business owners, or the negligence of administrations. In response to these disclosures, which sometimes turn to scandals (as in the case of the revelations about A. Navalny's poisoners or about V. Putin's palace and the opulence of his relatives in early 2021), countermeasures generally rely less on denial or counterexpertise than on finding justifications or diverting attention and preventing criticism. When scandals break out at the federal level, the authorities' response borrows from the ontologies of international conspiracy. Their counterattack to the most high-profile investigations is to claim that the data "were provided by Western special services."[31] V. Putin himself stated that they were "the legalization of the American special services' sources."[32] Casting aspersions on the origin of the data used by journalists serves to justify their registration on the list of foreign agents, which in turn is a way to discredit their work and point accusations back at them. Beyond these conspiratorial arguments, the political struggle for data appropriation is also present in the socio-technical apparatus built around the data itself to prevent, restrict, or falsify access to it. Accusations leveled at journalists and their data became stronger after the start of the war in Ukraine, and in the context of military mobilization, they took on a strategic value.

THE FIGHT AGAINST DATA JOURNALISTS

In 2020 and 2021, in Russia, digital investigation reactivated political conflicts rooted in episodes of the Cold War and its enduring suspicion regarding foreign influences. While the Russian state is suspected of being the main purveyor of false information published in Western media in the 2010s, it in turn denounced journalists investigating it in the digital sphere as a conspiracy. State media attack Russian data journalists and published articles aimed at discrediting them.[33] Their international cooperation is seen as foreign interference. Attempts to create scandals around misappropriation of state funds are claimed to be the work of foreign agents (under the 2012 Russian law, amended in 2017) with political and financial support from hostile states.

Under Russian law, since 2017 and 2021, respectively, media outlets and individuals that disseminate information to the general public and receive foreign funding (regardless of the amount) can be declared to be foreign agents. Data-driven investigative media very soon fell under this law. The Insider was categorized as a foreign agent by a decision of the Russian Ministry of Justice on December 5, 2017. The progovernment newspaper *Ekspress Gazeta* claimed that it was controlled by "special services of the West."[34] In the autumn of 2019, journalists at Proekt were stalked and faced threats and an attempt to break into their accounts after launching an investigation into Russian mercenaries in Africa and the Middle East. They first received threats of physical retaliation by email. Attempts to break into their Facebook, Telegram, and Google email accounts were noted.[35] In the spring and summer of 2021, the websites Meduza, Dozhd, and Important Stories were put on the list of foreign agents. Several dozen individual journalists are also on this list, including Roman Badanin and several members of the Proekt[36] media team. In July 2021, when Proekt's website was declared "'undesirable media in the country," its editorial team announced it was putting an end to its activities. R. Badanin and several of his colleagues left the country out of concern for their safety. With the start of the war in Ukraine, the list of media outlets and journalists prevented from working grew considerably. The risks they are facing have convinced most of them to go into exile, from where they have continued their online investigations (see chapter 8).

THE FIGHT FOR DIGITAL DATA

In addition to individuals, data are being enlisted in political struggles. In the face of increased repression, the reliability of public sources is brought into question, as state statistics in Russia have long been suspected of being biased. Journalists note that not all public data are published and that some of them are of poor quality.[37] This is not peculiar to Russia but is common to areas where administrations, such as police sources, for example, "have the freedom to manipulate them as they see fit" (Parasie and Dagiral 2013b). In 2021, observers believed that the quantity of open data in Russia was increasing, while their quality was declining. O. Kuzmicheva noted that there were many examples of "bad data," such as data presented in obsolete versions, data in graphical form without access to the original sources, and so on. Under the guise of open data, some administrations post unreadable data online,[38] and the publication of data creates tensions within the Russian administration itself. As one expert on open data explained in 2017, "In the administration, there are two trends: those who want to go digital and the revanchists who want to close the data. The balance of power is 50/50."[39]

Media controversies related to data journalism in turn lead to retaliation against the data. One shining example of this is the case of the Rosreestr database. In 2015, after Aleksei Navalny published his documentary *Chaika*, in which he accused the sons of Prosecutor General Yuri Chaika of corruption, their names were replaced with the codes "LSDU3" and "YFYAU9" in Rosreestr. According to A. Navalny, this was a direct consequence of his investigation. Since this first controversy, suspicions of open-data manipulation have multiplied. In December 2020, the Meduza website reported that the authorities had stopped publishing many companies' tax data. The journalists noted that some data, which had made investigations into corruption possible in the past, were missing. In January 2021 Meduza alleged that Rosreestr hid data on suspected embezzler Mazaraki's real estate in the Unified State Register of Real Estate (USRN). Rosreestr had classified information on the Mazaraki family's real estate.

A December 2020 law prohibits the publication of data on security forces, judges, and senior officials, even if their lives are not in danger—ironically, it was called the Law on LSDU3.. On December 15, 2021, the

Federation Council made plans to limit access to Rosreestr. The state newspaper *Rossijskaia Gazeta* claimed that the closure of access to Rosreestr was justified by the need to protect "personal data" and to fight criminals seeking to steal property. Independent newspapers see this as a new form of censorship. One journalist we spoke to expressed pessimism about the future of open data in Russia:

> There are many examples where the administration used to publish data and then stopped transmitting it. Sometimes a minister will give the order to publish data and then his successor gives the opposite order. . . . Unfortunately, this is sometimes linked to the work of journalists, especially in sensitive areas such as healthcare or the execution of sentences. It happened to me. I published an article about the lack of doctors where I compared oncology care in different regions. After that, access to the section on the Ministry of Health website that published this data required a password.[40]

She cited the case of a colleague working on prison issues, whose access to data was blocked after one of his articles was published. Many regions are closing their open-data portals and stop publishing them altogether. Data on living standards are the most difficult to obtain. As Ivan Begtin of Infokultura explained: "In our country, the state is responsible for everything, and indicators on the quality of education or healthcare, or on crime, are highly politicized. Those who produce these data are afraid that they will reveal what a poor job they are doing and the state is obviously afraid to publish them.[41]

DATA IN THE WAR AND THE DATA WAR

Following the launch of Russia's military offensive against Ukraine, data scientists grew concerned about the impact of the war on their access to digital sources. Amid rumors about the actual figures of mobilization, military casualties, and the effects of sanctions on the Russian economy, official data have gradually become inaccessible. This can be seen on the Telegram channel Open Data RU (*Otkrytye dannye RU*, which had about 2,700 members in November 2022).[42] Ivan Begtin, one of its moderators, published a "guide for rapidly archiving digital material" on February 26, two days after the offensive. He wrote, "Currently, as catastrophic events occur, as

military actions take place, large volumes of text, images or video are published, which may be inaccurate and disappear within hours of publication. Digital archiving is more important than ever." On March 3, he published advice on archiving, explaining, "It seems that it will be a major challenge in the coming months to archive what could very soon be destroyed, deleted, deactivated, blocked. The biggest risks concern all that is shut down when an organization is liquidated. For example, the liquidation of (the association) Memorial or now the liquidation of Ekho Moskvy (the radio Echoes of Moscow)."

Various testimonies support the idea that public data have disappeared. On March 4, Max noted that the results of Duma votes had not been published since February 22. Maksim replied, "In war as in war. The data is open by order." In March, Maria noted, "Amidst the hell of it all, I've noticed that many services with open data are no longer working, many datasets are simply missing from government websites. Even http://data.gov.ru has been down for a month." She spoke of the risk that the institution of open data would disappear from Russia in the future and that data would be issued "on demand," on the whims of bureaucrats. In April, Ivan Begtin confirmed that "the level of openness is decreasing year by year. Many regional open data portals are closed, half of them have not been updated for at least two years." Miroff retorted, "You write as if the level of openness used to be high. For the regions, data openness has always been a senseless duty imposed by federal fashion." In the trials of war, journalists and citizens are experiencing the degradation and disappearance of open data. This movement shows the fragility of sources in a Russian digital world that has fallen under authoritarian control.

CONCLUSION

In the 2010s, data journalism in Russia developed by relying on public, purchased, leaked, or stolen data to conduct investigations on topics as diverse as corruption, social inequalities, healthcare, and environmental issues. The enthusiastic momentum it gathered reflected a will to produce quantitative and objective investigations, in line with the methods used in transnational investigative journalism consortia. As data became more open and more

abundant, it fed into this movement toward the objectification of investigations. These investigations, which sometimes caused scandals, provoked a response from security institutions that in turn repressed journalists and placed data at the heart of conflicts of appropriation between investigators and public administrations. Following embarrassing revelations, data disappeared or were misrepresented. They have been involved in struggles over use and interpretation, as many journalists experienced when they were denied access to previously open data and had to call into question the quality of whatever data were published. This shook their confidence in these figures, calling into question the idea that data yield an objective and positive truth and introducing reflection on its construction. In Russia, like elsewhere, open data are caught up in the political, cultural, or economic arrangements that construct it. As O. Dovbysh (2021) reminds her readers, data journalism is based on data, the production of which is framed by power relations. With war, the strategic aspect of access to digital data becomes even more evident, giving rise to conflicts of appropriation and interpretation for military use. These tensions show the political stakes that are associated with data and inform reflection on the conditions of knowledge production in the current world. They lead investigators to de-naturalize the use of data and to break with the "cybernetic imaginary" (Supiot, 2015) in order to develop new digital and political reflexivity in a time of military confrontation.

NOTES

1. "Vojna v cifrah," *Important Stories*, May 16, 2022 (updated November 10, 2022), https://Important Stories.media/reportages/2022/05/16/voina-v-tsifrakh/.
2. https://istories.media/workshops/2021/11/05/zhurnalistika-dannikh-chast-1-istoriya/
3. Debates about the renewal of journalism through data resemble those around the renewal of social sciences through digital technology (Venturini and Latour 2009; Boullier 2015).
4. Hans Pool, *Bellingcat, Freedom Fighters* (2018, 90 min), www.bellingcatfilm.com.
5. "L'European Press Prize pour 'The Guardian', 'Bellingcat' et le projet 'Forbidden Stories,'" *Le Monde*, May 23, 2019. https://www.lemonde.fr/actualite-medias/article/2019/05/23/l-european-press-prize-pour-the-guardian-bellingcat-et-le-projet-forbidden-stories_5466208_3236.html.
6. Sheila Coronel, "Muckraking in Putin's Russia," April 18, 2013, https://gijn.org/2013/04/18/muckraking-in-putins-russia/.

7. Coronel, "Muckraking in Putin's Russia."
8. Interview by the author with a journalist, online, December 8, 2020.
9. The section is composed of three journalists (Irina Dolinina, Artem Chennikov, and Alesya Marokhovskaya) under the direction of Andrei Zayaakin.
10. https://www.proekt.media/about/
11. https://vc.ru/media/42523-eks-glavred-dozhdya-roman-badanin-zapustit-izdanie-proekt-s-rassledovaniyami-na-osnove-bolshih-dannyh
12. https://dimon.navalny.com/. For an overview of the FBK's online survey methods, see https://www.bellingcat.com/resources/case-studies/2015/08/19/yachtspotting/.
13. See https://www.mlg.ru/ratings/.
14. Dmitrij Kolezev, "Mozhno kupit' labuteny dlia vsekh zhitelej Nishnego Tagila" Znak.com, March 2, 2016. (This website was blocked and deleted in Russia. However, this publication can be accessed at https://web.archive.org/web/20210124174032/https://www.znak.com/2016-03-02/v_moskve_proshel_pervyy_hakaton_po_data_zhurnalistike. Please refer to our Note on the Availability of Sources.")
15. https://www.hse.ru/ma/datajourn/
16. Anastasia (administrator), data journalist based in Kyrgyzstan, posted on August 14, 2019. The channel had 375 members as of January 2021.
17. Iûlâ Apuhtina, post on the Telegram channel DDJ Russian, 9 January 2020.
18. https://istories.media/workshops/
19. https://zeh.media/praktika/obrazovaniye/9648173-ne-znayu-kak-eto-prigoditsya-mne-v-zhurnalistike-no-moy-mozg-popytka-pouchit-python-uzhe-rasshevelil.
20. Interview by the author with a journalist, online, December 8, 2020.
21. https://www.psbedu.paris/fr/actus/open-source-intelligence-technique-renseignement-service-intelligence-economique; see also https://nothing2hide.org/fr/2019-09-18-guide-osint-2019/
22. Andrej Zaharov, webinar hosted on December 2, 2020 by Spektr.
23. https://radioportal.ru/news/chto-takoe-data-zhurnalistika-i-chem-ona-mozhet-pomoch-lyuboy-redakcii
24. https://www.economie.gouv.fr/files/files/directions_services/igpde-editions-publications/revuesGestionPublique/IGPDE_Reactive_Russie_decembre_2015_janvier_2016.pdf
25. Coronel, "Muckraking in Putin's Russia."
26. Author's interview with journalist, online, December 8, 2020.
27. https://data.gov.ru/sites/default/files/presentation/prezentaciya_kuzmicheva.pdf. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")

28. Andrej Zaharov, webinar.
29. https://www.youtube.com/watch?v=v6slhNgKCOI
30. https://www.youtube.com/watch?v=smhi6jts97Iandt=2208s
31. Andrej Zaharov, "Kak rassledovanie ob otravlenii Naval'nogo izmenilo žurnalistiku," IJnet, January 4, 2021, https://ijnet.org/en/node/9468.
32. "Putin nazval dannye po Naval'nomu 'legalizaciej materialov' specslužb SŠA," RBK, December 17, 2020, https://www.rbc.ru/politics/17/12/2020/5fdb30b19a79477f9d320cff.
33. https://russian.rt.com/world/article/593261-hodorkovskii-tsar-rassledovanie.
34. https://www.eg.ru/society/655731-smi-nezavisimyy-the-insider-kontroliruyut-specslujby-zapada-078698/
35. https://zona.media/news/2019/10/15/proekt
36. See the official register of media serving as foreign agents of the Ministry of Justice at https://minjust.gov.ru/ru/documents/7755/. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
37. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Valeeva_Open%20data%20and%20investigative%20journalism%20in%20Russia.pdf
38. https://data.gov.ru/sites/default/files/presentation/prezentaciya_kuzmicheva.pdf. (This URL is not accessible from outside Russia unless a VPN is used. Please refer to our "Note on the Availability of Sources.")
39. Interview with an expert, Moscow, September 14, 2017.
40. Interview with a journalist, online, December 8, 2020.
41. "Količestvo otkrytyh dannyh v Rossii rastet, a ih kačestvo—net," CNews, July 14, 2021, https://www.cnews.ru/news/top/2021-07-14_kolichestvo_otkrytyh_dannyh.
42. https://t.me/opendatarussiachat

REFERENCES

Akrich, Madeleine, Michel Callon, and Bruno Latour. 2006. *Sociologie de la traduction: textes fondateurs*. Presses des Mines.

Alloing, Camille. 2016. "La sousveillance. Vers un renseignement ordinaire." *Hermès* (76): 68–73.

Anderson, Christopher William. 2018. *Apostles of Certainty. Data Journalism and the Politics of Doubt*. Oxford University Press.

Ausserhofer, Julian, Robert Gutounig, and Eva Goldgruber. 2020. "The Datafication of Data Journalism Scholarship: Focal Points, Methods, and Research Propositions for the Investigation of Data-Intensive Newswork." *Journalism* 21 (7): 950–973.

Begtin, Ivan. 2013. "Gotovy li my k žurnalistike dannyh?" (Sommes-nous prêts pour le journalisme de données?). *Polit.ru*.

Bigot, Laurent. 2017. "Le fact-checking ou la réinvention d'une pratique de vérification." *Communication et Langages* (192): 131–156.

Boullier, Dominique. 2015. "Les sciences sociales face aux traces du big data." *Revue Française de Science Politique* 65 (5): 805–828.

Bounegru, Liliana, and Jonathan Gray (ed.). 2021. *The Data Journalism Handbook: Towards a Critical Data Practice*. Amsterdam University Press.

Carson, Andrea. 2019. *Investigative Journalism, Democracy and the Digital Age*. Routledge.

Chupin, Ivan, and Françoise Daucé. 2016. "Par-delà la contrainte politique? La banalité des bifurcations dans les carrières journalistiques en Russie contemporaine." *Réseaux* (199): 131–154.

Coddington, Mark. 2015. "Clarifying Journalism's Quantitative Turn: A Typology for Evaluating Data Journalism, Computational Journalism, and Computer-Assisted Reporting." *Digital Journalism* 3 (3): 331–348.

Daucé, Françoise. 2019. "Épreuves professionnelles et engagement collectif dans la presse en ligne à Moscou (2012–2019)." *Mouvement Social* (269): 101–116.

Daucé, Françoise, and Francesca Musiani. 2021. "Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet: An Introduction." *First Monday* 26 (5). https://firstmonday.org/ojs/index.php/fm/article/view/11685/11225.

Dovbysh, Olga. 2021. "Trust and Reliability of Data in Authoritarian Regime: Practices of Data Journalism in Russian Newsrooms." Automation and Data-Driven Journalism beyond the Western World conference, Helsinki, May 5–6.

Flichy, Patrice. 2012. *L'Imaginaire d'Internet*. La Découverte.

Giry, Julien (ed.). 2017. "Les théories du complot à l'heure du numérique." *Quaderni* (94): 5–11.

Glazunova, Sofia. 2020. "'Four Populisms' of Alexey Navalny: An Analysis of Russian Non-Systemic Opposition Discourse on YouTube." *Media and Communication* 8 (4): 121–132.

Gray, Jonathan, Lucy Chambers, and Liliana Bounegru. 2012. *The Data Journalism Handbook: How Journalists Can Use Data to Improve the News*. O'Reilly Media.

Hérodote. 2022. "OSINT. Enquêtes et terrains numériques." *Hérodote* 186 (3). Special Issue.

Theviot, Anaïs. 2020. "Entre data journalisme et pratique infographique." *Interfaces Numériques* 9 (3). https://www.unilim.fr/interfaces-numeriques/4469.

Lapoix, Sylvain. 2014. "Le data journalisme: entre retour du journalisme d'investigation et fétichisation de la donnée. Entretien avec Sylvain Lapoix." *Mouvements* 79 (3): 74–80.

Koltsova, Olessia. 2006. *News Media and Power in Russia*. Routledge.

Lemieux, Cyril. 1992. "Les journalistes, une morale d'exception?" *Politix* 5 (19): 7–30.

Loveluck, Benjamin. 2015. *Réseaux, libertés et contrôle: Une généalogie politique d'Internet*. Armand Colin.

Loveluck, Benjamin. 2016. "Vers une économie politique des données: le pouvoir à l'aune des *data*." In *Open Data and Big Data. Nouveaux défis pour la vie privée*, edited by Danièle Bourcier and Primavera De Filippi. Mare and Martin.

Lowrey, Wilson, Ryan Broussard, and Lindsey A. Sherrill. 2019. "Data Journalism and Black-Boxed Data Sets." *Newspaper Research Journal* 40 (1): 69–82.

Mann, Steven, Jason Nolan, and Barry Wellman. 2002. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance and Society* 1 (3): 331–355.

Milan, Stefania, and Lonneke Van der Velden. 2016. "The Alternative Epistemologies of Data Activism," *Digital Culture and Society* 2 (2): 57–74.

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

Parasie, Sylvain. 2013. "Des machines à scandale: Éléments pour une sociologie morale des bases de données." *Réseaux* (178–179): 127–161.

Parasie, Sylvain, and Éric Dagiral. 2013a. "Des journalistes enfin libérés de leurs sources? Promesse et réalité du 'journalisme de données.'" *Sur le Journalisme, About Journalism, Sobre Jornalismo* 2 (1): 52–63.

Parasie, Sylvain, and Éric Dagiral. 2013b. "Data-driven Journalism and the Public Good: 'Computer-assisted Reporters' and 'Programmer-Journalists' in Chicago." *New Media and Society* 15 (6): 853–871.

Rostova, Natalia. 2019. "Saving Their Profession: Russian Journalists and Their New Media" *The Russia File*, a blog of the Kennan Institute, Wilson Center. https://www.wilsoncenter.org/blog-post/saving-their-profession-russian-journalists-and-their-new-media

Roudakova, Natalia. 2017. *Losing Pravda: Ethics and the Press in Post-truth Russia*, Cambridge University Press.

Shilina, Alexandra, and Marina Shilina. 2019. "Towards Data Journalism in Russia?" In *Data Journalism in the Global South*, edited by B. Mutsvairo, S. Bebawi, and E. Borges-Rey. Palgrave Macmillan.

Stalph, Florian, and Eddy Borges-Rey. 2018. "Data Journalism Sustainability: An Outlook on the Future of Data-Driven Reporting." *Digital Journalism* 6 (8): 1078–1089.

Supiot, Alain. 2015. *La Gouvernance par les nombres. Cours au Collège de France (2012–2014)*. Fayard.

Valeeva, Anastasia. 2017. *Open Data in a Closed Political System: Open Data Investigative Journalism in Russia.* Thomson Reuters Foundation.

Vauchez, Ysé. 2019. "Les mythes professionnels des fact-checkeurs." *Politiques de Communication* 1: 21–44.

Venturini, Tommaso, and Bruno Latour. 2009. "The Social Fabric: Digital Footprints and Quali-quantitative Methods." *Proceedings of Futur en Seine*: 87–103.

Yablokov, Ilya. 2018. *Fortress Russia: Conspiracy Theories in the Post-Soviet World*. John Wiley and Sons.

Young, Mary Lynn, Alfred Hermida, and Johanna Fulda. 2018. "What Makes for Great Data Journalism? A Content Analysis of Data Journalism Awards Finalists 2012–2015." *Journalism Practice* 12 (1): 115–135.

6 COPYRIGHT AND ONLINE BOOKS: CONTROL OVER CONTENTS, TRANSGRESSIONS, AND SPACES OF FREEDOM

Bella Ostromooukhova

On October 9, 2015, the Moscow City Court ordered that Russia's most popular content-sharing platform, rutracker.org, be permanently blocked following a copyright infringement complaint filed by the Eksmo publishing house, one of the Russian book industry's major companies. The court justified its decision based on an amended version of law 364-FZ, known as the "anti-piracy law," which had come into force the same year, allowing platforms that did not respect copyrights to be definitively blocked. The Roskomsvoboda NGO, an offshoot of the Russian Pirate Party (Daucé 2022), then launched a campaign it called "the battle for the Runet," in which it declared this block (as well as the dozen or so others that had preceded it) to be unconstitutional and in violation of certain fundamental rights such as freedom of the press and opinion.[1]

Questions of freedom—including digital freedom—are thus connected to issues pertaining to the definition and protection of copyrights online. In principle, access to copyrighted content is in the hands of the rightful owner (author, producer, or publisher), who has the power to charge for, or even restrict, access to their cultural product. The online space is thus behind two levels of walls: individuals or private companies can set up barriers to access for content whose rights they own, and states define national standards for the protection of these rights and are responsible for enforcing them. Digital rights advocates contest restrictive measures—such as blocking sites that do not comply with the limitations imposed—in the same way as they oppose other types of online censorship, because copyright can become an

instrument or issue of political or ideological struggle. And some online protest content is indeed censored under the pretext of copyright infringement.[2] Since the Russian full-scale invasion of Ukraine, however, there have been upheavals around the issue of copyright enforcement. International sales of rights for cultural products have been hampered by sanctions. With major cultural industries withdrawing from the Russian market, authorities have been incentivized to infringe on copyright,[3] and circumvention practices, which had officially been on the decline for a decade, made a comeback.[4]

Copyright standards are traditionally defined and amended at national level, based on international agreements that set a common framework[5] but leave countries some room to maneuver (Martin-Prat 2014; Zasurskij 2016, 16–48). Each country composes its own framework with elements of two models that tended to converge over the course of the twentieth century (Baudel 1998, 52–57): the French copyright model, focused on the moral rights of the work's creator, and the Anglosphere model, focused on the economic rights of those who assume financial responsibility for its production and distribution (Benamou and Farchy 2009).

The advent of the internet has shaken up these norms and required them to be redefined. Cyberspace, which some see as a platform for the free circulation of content and others see as a space for new economic possibilities, has become the focus of struggles between businesses, governments, and civil society. "The battle around intellectual property is fought over new forms of private appropriation of knowledge and the shifting boundaries of the domain that is freely available to the public" (Benamou and Farchy 2009, 114). While GAFAM (Google, Apple, Facebook, Amazon, Microsoft) companies and cultural industries tend to prevail in the market for online cultural content production and distribution (Waldfogel 2018), their actions are contested and circumvented in a variety of ways. In addition to actors who mobilize against fraud crackdowns or seek to expand the public domain, there are many who disseminate and consume cultural content despite commercial prohibitions. These individuals belong to a broader set of actors generally referred to as "hackers," which originated in the US computer science world of the 1960s and has subsequently diversified to encompass a vast array of practices, spheres of action, and cultural domains, involving various

political languages (Turner 2006), including anarchism, autonomism, libertarianism, and sometimes combinations of these (Coleman 2012). What hackers have in common is their repertoire of online action (Van Laer and Van Aelst 2010): whatever they are hacking, they are breaking a technical or symbolic barrier to access content hidden from the layperson's sight, often as a "reaction to a certain mode of commercial exchange, and to the practices of control that result from it" (Bacot and Canonne 2019, 10).

This chapter[6] shows how the state, cultural industries, and hackers are all seeking to appropriate the Runet around a specific class of objects: books.[7] While they are nowhere near as lucrative or as massively consumed as cinema or music, books are nevertheless very well integrated into the global market, and Russian authorities lend them considerable symbolic value, as they wish to revive the Soviet cliché of "the nation of great readers" (Ostromooukhova 2019). In the first part of this chapter we outline the development of copyright legislation in Russia since the 1990s and the formation of a legal market for texts in digital format as the cultural goods market was first liberalized and opened up and then subjected to increasingly strict state control. We then look at one type of actor that avoids this control: "shadow libraries"[8] specializing in fiction, which strive to distribute books despite restrictions. We show the evolution of survival techniques through some emblematic case studies: lib.ru, also known as the "Moshkow library," created before the fall of the USSR and whose popularity peaked in the late 1990s; Librusec,[9] which appeared in 2007 and reached its golden age in the mid-2010s; Flibusta,[10] created by a few disillusioned members of the Librusec community in 2009; and Maxima library,[11] which took over the foundations of Librusec and Flibusta in 2013 and spent two years trying to develop as a "legal" platform before being relegated to the "shadows."

THE IMPLEMENTATION OF CONSTRAINTS IN TERMS OF ONLINE COPYRIGHT: RATIONALES, ACTORS, AND CONFLICTS

In Russia, the book industry—in the Western sense of the term—emerged after the fall of the Soviet Union and the introduction of the market economy, just as Russian copyright was redefined so that this new branch, like

other cultural industries, could be integrated into the global economic context. Massive access to the internet opened new perspectives as the free circulation of texts became possible, along with the formation of the digital book market.

The Soviet Legacy

Before 1917, the Russian publishing system was mostly in line with international standards, apart from the legal doctrine of "freedom of translation," which allowed foreign works to be published in Russian without paying royalties. The Bolshevik revolution brought about a radical change, leading the USSR to develop its own book production apparatus and a unique copyright system. In Marxist-Leninist doctrine, all cultural works had to be accessible to the whole population in order to contribute to the education of the working masses. While moral rights, which existed from the moment a work was created, remained inalienable and belonged to the author, they were limited to a much shorter period of time than in countries that had signed the Berne Convention for the Protection of Literary and Artistic Works (1886): twenty-five years from publication or fifteen years after the author's death for posthumous works. Economic rights, however, could be assigned for a short period of time to state-owned enterprises involved in the production and distribution of cultural goods. In addition, the law included a very long list of free uses of a work that allowed them to be distributed as widely as possible. The Soviet Union had also kept Tsarist Russia's freedom of translation laws regarding foreign works. Although the USSR joined the Universal Copyright Convention in 1973, it would retain a certain degree of freedom toward foreign rights holders, which lasted into the early post-Soviet years (Elst 2005, 65–90).

The state's severely censored cultural production was rivalled in the post-Stalinist period by the artisanal production and distribution of works, referred to as *samizdat*. It brought together people who clandestinely copied and circulated typed texts (monographs, anthologies, tracts, periodicals) that were banned by Soviet censorship or rejected by publishing houses, thus circumventing both copyright and censorship issues (Zaslavskaya 2015). Strictly speaking, this practice was not illegal, provided that the works produced

and distributed outside official channels were not sold (Elst 2005, 34). In practice, however, the informal production and distribution of uncensored texts were considered criminal activities, contributing to the dissemination of politically harmful content, and those involved were severely punished. A black market in cultural goods (including *samizdat* and *tamizdat*,[12] or official cultural production diverted from its usual distribution channels) nevertheless proliferated in the 1970s and 1980s. While it was prohibited by law, the Soviet state tolerated this type of commercial activity as a way to mitigate the planned economy's shortcomings (Thiesse and Chmatko 1999, 77).

Post-1991: Bringing Russian Copyright Law into Line with International Standards to Integrate the Global Market

After the fall of the Soviet Union, increasingly privatized and polarized Russian cultural production sought to integrate global production by entering into partnerships with large foreign companies. Foreign films, music, and books that were previously difficult to access were imported en masse, often through parallel channels, regardless of copyright (Kiria and Sherstoboeva 2015; Thiesse and Chmatko 1999). They came both on physical media and over the internet, access to which gradually became commonplace in Russia during the 1990s and 2000s.

However, to appease foreign partners and make the Russian market attractive, Russian copyright legislation was gradually brought in line with world standards. Law 5351–1 on intellectual property and related rights, enacted in 1993, extended the term of protection to fifty years after the death of the author, as recommended by the Berne Convention, to which Russia acceded in 1995. The law also excluded the cases of free use provided for in Soviet legislation, recognized related rights that until then had not been provided for in the law, and allowed for the emergence of organizations taking charge of collectively managing intellectual property rights (IPR).

In the 1990s the Russian government began negotiations to join the World Trade Organization (WTO), which were not concluded until 2012. In the run-up to its accession, US companies such as Microsoft, the Motion Picture Association of America (MPAA), and the Recording Industry Association of America (RIAA) demanded a stronger commitment from Russia on

IPR protection. In 2004, to meet these expectations and provide guarantees to these foreign partners, the copyright term was extended to seventy years, to match the US Copyright Term Extension Act of 1998 (Alekseeva et al. 2013, 69). At the same time, the Law on Intellectual Property and Related Rights was amended to include digital uses of works (Rassolov 2016), in line with the US Digital Millennium Copyright Act (DMCA) of 1998. However, this law has been applied only sporadically, partly due to the lack of an enforcement mechanism.

Part IV of the Civil Code of the Russian Federation, which is dedicated to copyright, had been in preparation since the 1990s and was adopted in 2006. Immediately after its entry into force on January 1, 2008, President Medvedev ordered that it be revised. The aim was to find a compromise between several requirements: to include the standards set by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (Alekseeva et al. 2013, 62); to respond to the demands of internet professionals such as the Russian Association of Electronic Communications (RAEK), founded in 2006, and internet freedom associations such as Wikimedia.ru and the Association of Cyber Publishers to create a simplified mechanism for interactions between rights holders and information intermediaries; and to legalize open licensing in Russia (Alekseeva et al. 2013, 72). President Medvedev sided with these experts' aspirations to more flexibility in legislation. In 2008, he called for "limiting the liability of information intermediaries for content uploaded by users" (Zasurskij 2016, 54).

"Fighting Piracy": An Aspect of Efforts to Control the Runet in the 2010s

State policy would, however, take a sharp turn in 2012, with the return of V. Putin to the presidency of the Russian Federation. From the beginning of his new term, he approved a series of legislative initiatives aimed at intensifying state control over the national internet (Soldatov and Borogan 2016). Federal Law 139 of 2012, known as the Blacklist Law, providing for the creation of a register of websites sharing "illegal" content (i.e., publishing information on drugs, child pornography and suicide, or else falling under the vague category of "extremism"), was among the first. It created a tool for online

content censorship. A year later, in 2013, members of the Duma submitted a bill to apply the same mechanism to websites that did not respect copyright. The aim was to introduce tools for the repression of online copyright infringements, which had been lacking until then. V. Putin then clearly sided with copyright holders, and the Duma approved Federal Law 187, which its detractors have referred to as the anti-piracy law, the anti-internet law or the Russian SOPA—and it did indeed echo the US 2011 Stop Online Piracy Act (SOPA) and Protect Intellectual Property Act (PIPA) bills, which also aimed to invest the state with the power to "mobilize the managers of online platforms to enforce the interests of copyright industries" (Nowak 2016, 178). But while the outcry against SOPA and PIPA in American society caused US lawmakers to back down (Herman 2012, 215–216), the Russian government was impervious to the widespread opposition against the anti-piracy law (Zasursky 2016, 62–63). Critics drew a parallel between the blacklist law and the anti-piracy law, as there were strong similarities between the repressive mechanisms they put in place and the actors they involved (the Moscow City Court, the Roskomnadzor agency). This led to a convergence of struggles around these two distinct issues (blocking sites due to undesirable content or due to copyright infringement). Russian internet actors such as Wikimedia.ru and Yandex led numerous protest actions, not unlike those of US platforms against the SOPA (Alekseeva et al. 2013, 81–85). In addition, the petition published by the digital rights organization Roskomsvoboda, created in 2012 (Daucé 2022), garnered 100,000 signatures according to the organization, and the RAEK issued reports on the damage that this law would cause to the internet industry and to rights holders themselves.

Despite the various actors' mobilization, the law was passed and then, over the years, strengthened and extended to cover more content and new actors. The first version of the law, which applied only to audiovisual content, set out the legal process and designated "information intermediaries" (site administrators, hosts, and internet service providers [ISPs]) as the ones in charge of ensuring that content was legal. Amendments that came into force on May 1, 2015 extended copyright protection to all cultural products in digital format, apart from photography. Informal agreements between right holders and "information intermediaries," which were once common

practice, were made more difficult. Sanctions were also strengthened. The Moscow City Court, in particular, was granted the authority to permanently and irrevocably block sites in cases of repeated infringements.

The resulting blocks, including the one on Rutracker, gave rise to numerous circumvention tactics, which subsequent amendments to the legislation sought to counter. For example, amendments that came into force on October 1, 2017 allowed Roskomnadzor to block "mirrors" created by shadow sites. The next step was to ban platforms that failed to respect copyright from search engine results and social media. Gazprom Media–owned TV channels sued the search engine Yandex in 2018 over links to illegal content on the Yandex.video service. This lawsuit resulted in a memorandum signed on November 1, 2018 by the Russian internet industry major actors (Yandex, Mail.ru, and Rambler) that undertook to remove links to illegal audiovisual content from their search engines. A new version of this memorandum, signed in January 2022, included more players—most notably VKontakte—and covered books (unlike its first version, which focused mainly on audiovisual content), pending a new version of the anti-piracy law.

In the late 2010s, messenger applications (especially Telegram) and other mobile applications became a convenient way to distribute content while circumventing copyright. A new law,[13] which came into force in October 2020, made these applications and their aggregators, App Store, Google Play, and Huawei AppGallery, liable for the distribution of illegal content. While they were not obliged to comply with Russian laws, these foreign companies were nonetheless quite willing to respond to complaints. In the case of the messaging service Telegram, after being unblocked in 2020, the company started collaborating actively with the Russian book industry major actors, especially by deleting the channels that drew complaints, even though no specific legal provision obliged it to do so.[14]

The war against copyright infringement is therefore being waged by two types of players: foreign cultural industries (mostly American ones) wishing to curb IPR infringement on Russian platforms and Russian companies that are anxious to protect their products in the national cyber space. The largest among the latter also created an organization tasked with this protection, AZAPI,[15] when the first version of the anti-piracy law was passed. The anti-piracy

legislation, criticized for its flaws by some and for its liberticidal intention by others, was an attempt to provide guarantees for these different actors.

ONLINE LIBRARIES: THE ART OF SURVIVAL, BOTH WITHIN THE LAW AND OUTSIDE IT

In this shrinking environment, which private players and state actors alike are making increasingly restrictive, books are distributed in digital format both via a legal market, which is monopolized by large companies, and through multiple informal channels, some of which remain in the legal domain while others survive illegally. These different channels, however, have a common origin, which dates back to the Soviet parallel economy.

The Formation of the Legal Market for Digital Books

Obtaining texts outside official channels was part of Soviet citizens' habitus in the late socialist era. As books played an essential role in the Soviet value system, and given the chronic shortage of fashionable literature, 68 percent of households in large cities bought books on the black market (Stemakh 2001, 146). Thus, Maksim Moshkow, the administrator of lib.ru, one of the first Russian online libraries, described the first exchanges of digitized texts between collaborators at research institutes in the 1980s and early 1990s, as a way of quenching a "thirst for reading" that the book shortage of the late socialist period had given him:

> We were used to the fact that if a book was good, you couldn't buy it in a bookshop, it would always be sold out. And at the library you had to queue up and even then you never knew if you could borrow it. That's why we all used to go book hunting. You would challenge yourself to find a specific text, queue up, ask around. . . . And then one day you get to work and you see that the book you were looking for is right there (on the computer hard drive). And you're not in a library where you have to return it, or in a shop where it's never available, or with a scalper who will sell it to you at four times the normal rate. . . . This is the file—you can just take it, copy it to your computer, and that's it.[16]

Manually digitizing texts and exchanging them between peers was thus an established practice among the technical intelligentsia even before the fall of

the USSR, market liberalization, and the advent of the internet. It became even more commonplace in the 1990s, and the development of the internet gave it new impetus. Russian-speaking online libraries proliferated and diversified in the 1990s, without any concern for copyright. Only in the late 1990s did an awareness of the need to pay attention to the law begin to emerge in online chatrooms and in media outlets that dealt with the internet (Bodó 2018).

In the 2000s, as books in digital format gradually became attractive to mainstream publishers, an online library market emerged, which created a need to draw the boundaries between legal and illegal players. The latter were identified through a series of piracy lawsuits. In 2004, KM online, an online company specializing in multimedia educational products, attempted to become a legal online bookstore and signed a contract with major Russian publishers. It then filed a piracy lawsuit against the major libraries adelbaran.ru and lit.ru, which resulted in minor fines only for the managers of the offending platforms but defined these platforms as illegal. Ironically, the plaintiff would eventually meet the same fate: in July 2006, a translator filed a lawsuit against KM online for the unauthorized use of his translations, thus expelling it, in turn, from the legal sphere.

This is the context in which the company Litres, founded in 2005, became the first major online bookstore specializing in e-book sales. Its founders—administrators of large shadow libraries—had studied the reasons for the commercial failure of KM online and set out to create a more functional and efficient system. They also made good use of their technical know-how: one of the company's founders, Dmitry Gribov, led the team that developed the e-book format FictionBook (FB2 and its new version FB3, released in 2017[17]), which with some promotional backing from Litres, would become the most popular format on the Russian market (Haritonov 2016, 24). The founders also set up a system of interconnection between the illegal libraries they managed and Litres. The latter signed a contract with the writers, who gave it exclusive rights to sell e-books, after which the illegal versions of their works were removed from the shadow libraries, which would instead redirect their readers to Litres. The legal library was thus largely fed by illegal resources, which continued to exist in parallel. In 2009, majority

shares of Litres were bought by the Russian publishing major actors AST and Eksmo, which made it their agent in the e-book market.

Bookmate, another platform dedicated to online reading but oriented more toward international development, was created around the same time and developed in parallel. It was founded by a British businessman living in Russia and his Russian partner and since 2017 has belonged to the company Bookmate Limited, officially registered in Ireland, which had developed its services in many other countries in Europe, Asia, and Latin America. However, because of Russia's invasion of Ukraine, the Irish company withdrew from the Russian market in July 2022, and was declared a "foreign agent media" in October of the same year. The Bookmate platform has been acquired by Yandex, which will continue to expand it within Russia.[18]

Other foreign platforms, such as the Swedish audiobook streaming service Storytel, which has been the largest player to occupy this niche in Russia since 2017, withdrew from the Russian market in 2022. This left room for Russian players and, in particular, allowed Litres and Bookmate (as a property of Yandex) to continue growing.

The e-book market in Russia was thus monopolized by large companies early on and remains very much so in the current context, even though it has refocused on a smaller set of national major players since February 2022.

Staying within the Law

Contrary to this market focused on the output of the major Russian publishing houses, platforms enabling their users to freely share texts have continued to develop. They seek to make up for this system's shortcomings by providing access to texts that are inaccessible because they are too old, too rare, or published outside the major channels.

Some of these platforms manage to stay within the bounds of legality, as does lib.ru, for instance. This library, which began as a private collection that its administrator, Maksim Moshkow, shared in the early days of the internet in Russia, rose to prominence in the 1990s. Its collection's exponential growth relied on a collaborative mode of operation. Enthusiasts would digitize books using scanners, transform them into text files using the FineReader software—which was broadly distributed in Russia from

1994—and send them to Moshkow, who would add them to his collection after a brief editing process. However, this centralization hampered the collection's growth, as the influx of messages eventually became greater than the administrator could handle; when he ran out of time to process applications, he had to slow down the rate of updates.

When lib.ru was sued for piracy in 2004,[19] Moshkow had to choose between some form of legality or survival outside the legal framework. He opted for the first solution by splitting his library in two. He created a new section he called "Samizdat," dedicated to texts sent by their authors for a first publication online. Moshkow, who did not see these texts as "real" literature because their value had not been validated by a publisher, agreed that they could be uploaded in a decentralized way. The Samizdat section was therefore fitted with a program allowing authors to upload texts themselves, so that it could grow without the administrator's intervention. Since its creation, this part of the website has been actively developing, to the extent that publishers now use it to seek out new talent. Once their text has been spotted and published, it is up to authors to negotiate with their publishing house whether or not their work will be featured in Moshkow's library.

The "library" part, which contains books that had already been published in 2004, has been frozen since the late 2000s and purged of works whose owners have demanded to be removed. In addition to the drawback of his centralized operation, Moshkow argues that there has been a paradigm shift in the way files are made. The community that fed the lib.ru collection valued the manual work of scanning books and converting them to text format. This process was seen as a hacking practice that created new value. Since it has become commonplace for publishing houses to produce e-books, digitizing texts has become an obsolete practice, the community dedicated to it has gradually disintegrated, and the influx of scanned books has dwindled.

Thus, lib.ru is now a sort of a museum for royalty-free classics, on the one hand and, on the other, a self-publishing website, with its community of authors in search of an audience and a publisher, its internal operating rules, and its code of conduct regarding publishing houses, elaborated over the course of past collaborations.

Other libraries, created more recently but often built upon the archives of their predecessors, and which continued to enrich their collections, held onto hopes of remaining in the legal domain until the mid-2010s.

One of those was Maxima Library, which initially tried to look as legitimate as possible, a tactic that had proved effective for lib.ru. The website's homepage stated, "We are a free library for free people. . . . We strive to ensure free access to works without infringing on anyone's rights."[20] Later, the administrators would announce on the library's forum that they had been forced to remove some books to provide free access to the rest. Nevertheless, despite these efforts, in December 2016, http://maxima-library.org was blocked in Russia. The library's representative on the librusec.ucoz forum bitterly announced,

> Because of two lousy books by some guy called Pereliaguin, which had been on our site for ages, we are "blocked at the request of the rights holders." But none of these book murderers have read these books, it is not the business of the rights holders to read, their business is to prevent people from reading. . . . The Library continues to function, of course, everyone knows the means and methods for circumvention (well, except maybe for the members of *Roskompozor*).[21]

This exit from the legal sphere was welcomed by other forum users who, in their comments, reversed the stigma of being blocked: "Welcome!" "At last you are considered a serious library."[22]

The same applied to the other libraries we mentioned at the beginning of this chapter, Librusec and Flibusta. While these platforms were able to maintain close links with the official market until the early 2010s, the implementation of the anti-piracy law definitively shut down these grey areas and radicalized the legal versus illegal dichotomy. Most shadow libraries were blocked by Roskomnadzor before the end of 2016. They thus consolidated around the image of a cultural underground and had to appropriate, or even produce, tools of digital resistance.

The Tactics of Illegal Survival

The survival strategies Russian shadow libraries are now developing have three main objectives. The first is to ensure the sustainability and growth of their

collection, which in turn depends on the vitality of the community their website brings together. The second is to ensure the personal safety of the administrators who bear the legal responsibility for the alleged fraud. Finally, these websites must guarantee access to their collections on the territory of the Russian Federation, where they are generally blocked under the anti-piracy law.

Shadow libraries are communities that bring together readers and administrators (Bodó 2018). Unlike lib.ru, Librusec, Flibusta, and Maxima Library operate on a Wiki model, where texts and records about works and authors are uploaded by the users themselves. The range of actions available to each user depends on seniority, skills (especially when it comes to coding), and merit earned within the community (such as having solved technical problems or having uploaded or commented on a large number of books). However, every logged-in member can download and edit the library's content. For some time, this allowed the tiny teams of administrators to avoid liability in the event of criminal prosecution, as they could disclaim responsibility for content posted by users.[23] The argument is, however, is no longer valid, since the anti-piracy legislation introduced the notion of "information intermediaries."

This collaborative way of building collections also allows them to grow exponentially. Ilya Larin, a developer by trade and an administrator of Librusec, has made the source code of his library freely available on his website.[24] The practice of sharing code in this way is deeply embedded in hacker culture, in which freedom of expression and code sharing are intrinsically linked (Coleman 2012, 9). The author's interview with Larin shows that he sees this sharing of code and texts as ways to ensure the ecosystem's survival: "They [Flibusta] borrowed the source code of my site, copied my archives. Many libraries have used Librusec's source code. Since then, they have evolved in different directions. Cross-pollination is happening all the time: some users are on several libraries at the same time, and when a new book comes out, they download it from several sites at the same time. It's now a fairly dense community, which makes it more sustainable. If Flibusta disappears tomorrow, well, nothing will change."[25]

This cross-pollination process is these collections' sustainability guarantee, as the members of these communities give them access to ever-increasing numbers of media and means of dissemination by sharing their skills or access

to specific resources. For example, any user can download the entire library along with a program that transforms the archive into a database, making it more convenient to browse. Once the complete database is installed on their computer, the user can download its updates on a monthly or yearly basis. In this way, the library's collection is replicated many times and maintained not only online, but also offline. If the virtual library were to be deleted from the server, it could be restored at any time from the copies kept by the users, which makes it impossible for it to disappear completely. The most convenient way to download large amounts of data, such as the library or its updates, is using "torrents." Comments on the main torrent aggregators show that library updates are distributed by a small number of volunteers. Other users then take over and distribute the downloaded databases on their own. Some shadow libraries have their own torrents, created by community members.

The server hosting the collection is also of great importance for the library's security. The laws of the country where it is physically located must be tolerant enough of copyright infringement. On the forums, administrators exchange comments on "good" and "bad" locations. Larin says there is a balance to be struck between the different types of censorship provided for by national laws. Although it is located in the Netherlands, a country that Larin perceives as tolerant of pirate sites, Librusec was accused of offering child pornography because it had a Soviet sex education manual depicting naked children in its collection. As a result, its administrator had to have it hosted in another country.[26] This is how differences in national legislation can be used to evade constraints.

The right choice of hosting services can provide further security. Some of the more expensive ones claim to be impervious to external requests. They thus offer protection against possible complaints from right holders that an ordinary hosting service would comply with, no questions asked.

Another task for library administrators is to ensure their own personal safety. The anti-piracy law makes them criminally responsible for the illegal content of the sites they maintain. There are two tactics in this respect: geographical distance is an immunity guarantee, and observing the strictest anonymity keeps any link from being drawn between the physical person and their virtual avatar.

Larin, who has lived in Ecuador since the early 2000s, is an example of the first tactic. Living far away allows him to reveal his identity, which he uses freely on social media (Livejournal, Facebook) and in public interviews. In our interview, he emphasized the ineffectiveness of court decisions in his country of residence:

- Larin: Litres took me to court here in Ecuador. I think they even won, but it had no impact on me. The thing about Latin America is that when one gringo sues another, nobody really cares.
- Author: Can they demand that you pay a fine?
- Larin: They can demand it, yes. But they can't force me to pay it. Also, the court ruled that the Librusec domain be taken away from me, which was supposed to kill the library. It's been two years now. Yet the domain still works, I renew the license every year. So there you have it, that's Ecuador.[27]

The term "gringo," which refers to foreigners in Latin America, underlines Larin's status as someone who perceives himself—and is perceived—as foreign to the local concerns of his country of residence. However, he also feels distant from the Russian context: "[The people at Litres,] I've never seen them in real life; they live somewhere in the distant city of Moscow, on another continent, they're doing their little business there. Well, good for them."[28]

His position as a person free of geographical constraints makes him impervious to possible prosecution. This contrasts with WikiLeaks founder Julian Assange, who also saw Ecuador—or at least its London embassy—as a safe haven from extradition to the US, where he was facing trial on charges of disclosing US government classified documents. His political stature as a symbol of opposition to the US government made him dependent on a diplomatic game between powers. In 2012, he was granted asylum for seven years as the result of president of Ecuador Rafael Correa's anti-imperialist stance. Correa's successor, Lenin Moreno, was anxious to distinguish himself from Correa and therefore handed Assange over to the British police. Larin, on the other hand, is not a public figure at all. He emphasizes the totally apolitical reasons that pushed him to choose his place of residence in 2000,

well before the creation of Librusec ("because of its pleasant climate") and takes care not to be associated with any local or international cause.

The administrators of other libraries cite his example to explain why they cannot afford to reveal their identities, as they do not enjoy the same geographical immunity as he does. For example, in November 2014, one of Flibusta's main administrators, who goes by Stiver and supposedly lives in Germany, wrote of his confrontation with local law enforcement on the library's forum, without naming the country where this took place:

> As some of you know, I've been under investigation for about two years. The same well-known publishing house in Russia has filed a complaint against me, accusing me of all sorts of sins, ranging from illegal distribution of texts to running an international crime syndicate and enriching myself in the process, of course.
>
> The police collected information about me, searched my home and office and seized my laptop. Then they started to examine what they . . . had collected. The outcome at this point: case closed. The investigation has not found and does not expect to find any irregularities beyond a few insignificant details. . . .
>
> The attempt to incriminate—with absolutely hilarious arguments—not only myself, but also the whole library, also failed. The investigation specifically stated that the project is non-profit and does not generate income.[29]

This seemingly positive news was met with mixed reactions from forum members. Most of them expressed joy, hoping that this would set a precedent that would allow shadow libraries to come out of illegality. Some users teased that Stiver should reveal their identity, since the police already knew it. However, users eventually agreed that it was best for everyone to remain anonymous to avoid trouble, especially in light of the precedents of arrested shadow library managers, such as the founders of Pirate Bay in 2010, who had been discussed on the forum before.

The Stiver investigation did not set a precedent in Russia. The ruling of a German court changed neither the Russian authorities' relation to the library nor the Russian industry major players' perception of it. However, it has reinforced the need for community members to remain anonymous. The "Rules" section of the website emphasizes the crucial importance of anonymity, stating that "actions that may compromise the security or personal rights

of users are prohibited. In particular, revealing someone's identity is prohibited."[30] When I requested an interview with another Flibusta administrator, they categorically refused any means of communication that might reveal their identity or whereabouts and mentioned the Stiver trial as a justification.

Finally, the third way to ensure the sustainability of libraries is to make sure that all users can access them. Attempts were undertaken to prevent blocks on their websites, most notably by Roskomsvoboda during the "Battle for Runet" in November 2015. After the court ruled that Rutracker should permanently be blocked, Roskomsvoboda's lawyers launched a campaign to lift these restrictive measures. They argued that restricting access to the entire website to protect a few titles from Eksmo's catalog violated the rights of millions of users to access the website's content, as well as the rights of the thousands of authors who distributed their own works there.[31] A website was created to collect funds and signatures,[32] and a complaint signed by seven thousand people was filed in court. This attempt to put an end to the blocks by setting a legal precedent was, however, unsuccessful. The appeal was dismissed twice and had no impact on further proceedings.

Blocks became commonplace from 2015 onward. It is now vital for shadow libraries to find ways to remain visible to the general public living in Russia. The first way is to look for an adequate domain and acquire safer mirrors. For example, Roskomsvoboda's experts recommend the .lib domain, run by EmerCoin, which is structured in such a way that it is considered invulnerable: "EmerCoin's DNS network is entirely decentralized and does not contain any websites that could be blocked at the request of the authorities or that could allow for pressure to be put on its owners,"[33] as can happen with domains managed by ICANN[34].

As networks that guarantee anonymity, such as Tor and the Invisible Internet Project (i2p), also allow their users to evade national constraints, shadow libraries set up mirrors there.[35]

Another way to increase visibility is to teach users tips on how to circumvent blocks. Shadow libraries' websites and forums all post lists of technical ways to get around the constraints created by Russian ISPs at the request of Roskomsvoboda. This dissemination of know-how seems to be ubiquitous and circulates through many other channels, including mailing lists, social

media posts, and YouTube tutorials. Proposed solutions include changing DNS servers, using browsers' turbo mode (Opera, Chrome, and Yandex), special browser plug-ins, VPN services, Tor browser, and anonymizers. Community members familiar with these skills explain to less experienced users how each method works and their advantages and disadvantages (which often come down to the balance between speed and ease of use). They test VPNs and anonymizers and then share their observations with other users. This mastery of circumvention tools is now a skill shared by people in shadow libraries and brings them closer to users who wish to access other types of blocked content. These have proliferated since the introduction of war censorship in March 2022, as they now range from independent media websites to social media owned by Meta.

In addition to the torrent files mentioned above, library users and administrators are finding impressively creative ways to organize the distribution of collection updates. Here too, the name of the game is the proliferation of means and media. For example, Librusec.ucoz, a forum shared by several parallel libraries, which serves as a refuge when their internal forums are inaccessible, has a section called "Our Tortuga."[36] On it, one of the forum administrators places links to updates of the Librusec and Flibusta databases via free file-sharing websites.

Alongside this platform, communities also use social media and messaging. An example of this is a bot installed on the Russian social media platform VKontakte that, for a time, allowed users to quickly search shadow libraries and facilitated access to them in the event of a breakdown or blockage. This ended in June 2019, when VKontakte and the publishing house Eksmo signed an agreement obliging the social media company to check the legal status of all books uploaded by its users. This did not lead to the bot's demise, however. By September, it had been moved to a safer location.[37]

After VKontakte adopted a harsher stance on illegal content, some shadow libraries started to use Telegram, which despite having been blocked from 2018 to 2020—and even because of this—has become very popular in Russia. It is said to be tolerant of illegal content thanks to the libertarian views of its owner, Pavel Durov. Many Telegram channels distributed digital and audio books,[38] and bots were coded for this purpose. However,

in August 2020 these bots reportedly ceased to operate, supposedly following an agreement between Telegram and the Russian authorities. When the news was announced on the Flibusta forum, users immediately proposed a technical solution to circumvent this new barrier:

> The Flibusta bot has been blocked not only on iOS, but also on Android.
> How to get the bot working again? It's simple—just follow these steps:
> 1. Create a group;
> 2. Add a bot by clicking on the following link[39]

When added to a group, the bot is no longer considered as such by the system and can continue to be used. Users thus take advantage of internal loopholes in the messaging system to circumvent blocks.

The survival of libraries and the communities that sustain them is therefore dependent on the proliferation of media and places where they are held, through the responsiveness of community members to obstacles and their ability to find creative solutions and distribute them as widely as possible. Communities rely on their members' technical know-how to keep these libraries going. Sustaining communication channels appears to be essential in this process, which explains their proliferation and even their redundancy in some cases.

This is in no way peculiar to Russia; it is part of a broader movement. According to Keucheyan and Tessier, in today's digital world, hackers or pirates are not revolutionaries; the idea of a revolution bears little promise because it would be "systematically followed by a counter-revolution that would result in similar—or worse—conditions of existence than those that preceded said revolution." Thus, hackers do not seek confrontation. On the contrary, they take advantage of "interstices, areas unoccupied by the state," and when they have been spotted, "they disappear, disperse to reform in another place" (Keucheyan and Tessier 2008, 457). Yet, while Keucheyan and Tessier argue that these symbolic moves can take place only in a democratic country, we have shown that they can also exist in an authoritarian context. Russian NGOs fighting for open access, such as the Association of Internet Editors, Wikimedia.ru, and Roskomsvoboda, are part of international networks and endorse globalized political struggles. Shadow libraries, on the other hand, stay away from these causes and promote a conception of

freedom rooted in mastering technical tools and cultural practices that are not censored by any authority outside their community.

CONCLUSION

After the fall of the USSR, the Russian state and cultural industries engaged in long-term endeavors to enforce international copyright standards on the Runet, to reassure foreign trading partners, and to allow domestic players to develop. Joint efforts to combat piracy have been one of the direct consequences of this. However, since the invasion of Ukraine, collaboration with major Western companies has been broken off, while the Russian public is used to consuming cultural products that are distributed worldwide. The state has therefore sought ways to legalize forms of copyright circumvention while at the same time protecting national industries. A bill allowing the use of cultural products from "unfriendly countries" without the consent of foreign rights holders was introduced in August 2022 but has been strongly criticized by industry representatives, who fear losing credibility on the global market.[40] They are looking for their own ways to provide the Russian public with the content it is seeking. Eksmo, for example, has announced that it would publish global bestsellers in the form of "summaries" of the books, avoiding any direct quotes. Many, including digital rights advocates who had previously fought back against the anti-piracy law, have criticized this practice, pointing out that it is a form of legalized piracy.[41]

This reversal of roles does not, however, change anything for shadow libraries, which are still seen as a potential danger to the national cultural industries, or even as an uncontrolled cultural underground.

The struggles for a censorship-free internet and for free and fair access to printed material overlap in many ways. Digital rights advocates are mobilizing for both causes, encompassing them under the same term, the "free internet." Outside Russia, repression has led shadow library administrators to gradually become more politicized. While they had started out as "nice guys happily sharing what was sold" by others, they found themselves in the same struggle as "victims of persecution and political censorship," which gave them a reason to rebel (Bodó 2015, 7). Meanwhile, the communities that have formed around Russian shadow libraries generally stay away from the

public protests that digital freedom organizations lead on their behalf and focus more on the technical aspects of constraint circumvention and user training. This is illustrated by the lack of reaction on their forum to the few explicitly political posts about anticopyright mobilization around the world, especially compared to the interest generated by posts on technical issues.

These platforms have nevertheless become a space of freedom in an increasingly restrictive context, as their outlaw status frees them from the need to respect the restrictions imposed by Russian legislation. Some communities use them to express a clear political position, which would be subject to repression if it appeared on an unblocked website. Thus, for example, after February 2022 the Maxima Library highlighted the slogan "Freedom to Ukraine! No to war! Death to the Putin fascists" in Ukrainian, Russian, and English on the homepage of its website.

Others assert their independence from the repressive Russian context. For example, when a user of the Flibusta forum asked whether sex in certain science fiction works could be considered "propaganda for LGBT relationships,"[42] another community member replied, "You're on a blocked site here, whose administrator doesn't care about the laws of the Russian Federation. Don't worry about it, this is only of concern to those unfortunate authors who try to sell their writings for roubles."[43]

Others yet, like Flibusta, remain focused on purely literary and technical discussions. However, regardless of the extent to which they publicly claim to be politicized or not, these communities promote an ideal of "absolute freedom," which is inseparable from the pirate imaginary. By merely existing, they challenge efforts to construct a Sovereign Runet on which only works produced and distributed by the Russian book industry, over which the state is trying to assert its control, could circulate.

NOTES

1. https://roskomsvoboda.org/13913.
2. For example, on July 23, 2022, *St. Marienburg*, a cartoon by famous animator Oleg Kuvaev that aimed to raise awareness of the horror experienced by the Ukrainian civilian population among the Russian population, by depicting the lives of Petersburgians during an imaginary invasion of Russia by China, was blocked by YouTube due to an alleged copyright

infringement in the use of a photograph. This was clearly a pretext to remove a cartoon condemning the war in Ukraine.

3. On January 31, 2023, Dmitry Medvedev called for legalizing the use of Western intellectual property without paying royalties, as a response to the new round of Western sanctions. https://www.vedomosti.ru/politics/news/2023/01/31/961116-medvedev-predlozhil-polzovatsya.

4. Roskomnadzor notes that the number of complaints about fraudulent use of intellectual property increased by 20 percent in 2022. https://www.vedomosti.ru/technology/news/2023/01/23/960100-rkn-otmetil-rost.

5. The Berne Convention for the Protection of Literary and Artistic Works was adopted in 1886 and signed by ten countries. The number of signatories grew but remained limited, as the US and USSR, for example, did not sign it. The Geneva Convention, also known as the Universal Copyright Convention, was drawn up under the auspices of UNESCO and ratified in 1952.

6. This chapter is an updated version of an article on the same subject (Ostromooukhova 2021).

7. The study is based on a qualitative investigation that includes semistructured interviews conducted in Moscow in February–March and June 2019 with various actors: lawyers who participated in drafting the anti-piracy legislation and others who defend shadow libraries; members of NGOs involved in negotiating the limits of legality (Roskomsvoboda, Wikimedia.ru, and the Association of Cyber-Publishers); and a representative of the AZAPI. We draw on interviews with administrators at lib.ru (June 2019) and Librusec (July 2020), along with a study of discussions on library forums and personal blogs, conducted from 2019 to 2023, to highlight circumvention strategies and their significance for these actors.

8. The term "pirate," which is frequently used in everyday language, has multiple connotations that actors often use to their advantage. While pirates are stigmatized by certain rights holders or defenders, who highlight the illegal or even "terrorist" aspect of their actions, they often willingly refer to themselves as such to invoke the idea of freedom and power attached to this notion (Keucheyan 2008). To step away from these connotations, we follow Joe Karaganis (2018) in referring to our object of study as "shadow libraries" and using the words "pirate" or "hacking" only where they have been used by actors themselves.

9. https://librusec.pro/

10. http://flibusta.is/

11. https://maxima-library.com

12. Manuscripts that were clandestinely exported, published in the West, and reintroduced in the USSR.

13. Law 177-FZ of June 8, 2020; http://publication.pravo.gov.ru/Document/View/0001202006080030?index=1andrangeSize=1.

14. https://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/. (The website has been taken down; however, this publication can be accessed via the Wayback Machine of Internet Archive at https://web.archive.org/web/20230603073504

/https://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/. Please refer to our Note on the Availability of Sources.")

15. Associaciâ po zaŝite avtorskih prav v internete (Association for the Defence of Copyright on the Internet), https://azapi.ru/.
16. Interview with Maksim Moshkow, July 4, 2019.
17. https://gorky.media/context/strannovatyj-fb3-otchet-federatsii-izdatelej-i-portret-pirata/
18. https://www.vedomosti.ru/media/articles/2022/06/30/929253-yandeks-pokupaet-bookmate
19. https://www.ng.ru/telecom/2004-11-02/13_lib.html
20. http://maxima-library.com/
21. http://librusec.ucoz.de/forum/27-2818-103197-16-1482497381. The term *Roskompozor* is formed by combining *Roskomnadzor* with the word *pozor*, which means "shame."
22. http://librusec.ucoz.de/forum/27-2818-103197-16-1482497381
23. See, for example, the interview with the Librusec administrator published in Livejournal: https://ya-parazit.livejournal.com/227533.html.
24. https://github.com/larin/librusec
25. Interview with Ilya Larin, 14 July 2020.
26. Interview with Ilya Larin.
27. Interview with Ilya Larin.
28. Interview with Ilya Larin.
29. https://flibusta.is/node/261839
30. http://flibusta.is/node/4023
31. https://roskomsvoboda.org/13690/
32. https://zarunet.org/
33. https://roskomsvoboda.org/12118/
34. Internet Corporation for Assigned Names and Numbers, a nonprofit organization based in Los Angeles.
35. https://roskomsvoboda.org/28612/
36. http://flibusta.is/node/474924
37. https://github.com/FlyInk13/FlibustaBot
38. https://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/. (The website has been taken down. However, this publication can be accessed via the Wayback Machine of Internet Archive at https://web.archive.org/web/20230603071739/http://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/. Please refer to our "Note on the Availability of Sources.")

39. http://flibusta.is/node/474924

40. https://www.vedomosti.ru/business/articles/2022/10/14/945479-kinoseti-i-prodyuseri-poprosili-mishustina

41. https://roskomsvoboda.org/post/prinuditelnoe-licenzirovanie/

42. A law banning "LGBT propaganda" in public space came into force in December 2022 to toughen the laws adopted since the early 2010s, in the context of a "war of values" waged by Russia against Western countries.

43. http://flibusta.is/node/588957

REFERENCES

Alekseeva, Anastasija, ed. 2013. *Transformaciâ Avtorskogo Prava v Internete. Zarubežnye tendencii, biznes-modeli, rekomendacii dlâ Rossii* [Transformation of Copyright in the Face of the Internet. Foreign Trends, Models of Business, Recommendations for Russia]. Associaciâ internet-izdatelej.

Bacot, Baptiste, and Clément Canonne. 2019. "Musique et hacking: de l'éthique aux pratiques." *Volume!* 16 (1): 7–14.

Baudel, Jules-Marc. 1998. "Le droit d'auteur français et le copyright américain: les enjeux." *Revue Française d'Études Américaines* (78): 48–59.

Benhamou, Françoise, and Joëlle Farchy. 2009. *Droit d'auteur et copyright*. La Découverte.

Bodó, Balázs. 2015. "The Common Paths of Piracy and Samizdat." In *Samizdat*, edited by Valentins Parisi. CEU Institute for Advanced Study.

Bodó, Balázs. 2018. "The Genesis of the Library Genesis: The Birth of a Global Scholarly Shadow Library." In *Shadow Libraries*, edited by Joe Karaganis. MIT Press.

Coleman, Gabriella. 2012. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.

Daucé, Françoise. 2022. "Pirater l'autoritarisme." *Terminal* (134–135).

Elst, Michiel. 2005. *Copyright, Freedom of Speech, and Cultural Policy in the Russian Federation*. Brill.

Haritonov, Vladimir. 2016. *Elektronnoe knigoizdanie v Rossii. Problema dostupa i gosudarstvennoe regulirovanie* [Electronic Publishing in Russia. Access Problems and State Regulation]. Associacija internet-izdatelej.

Herman, Bill. 2012. "A Political History of DRM and Related Copyright Debates, 1987–2012." *Yale Journal of Law and Technology* 14 (1): 162–225.

Karaganis, Joe. 2018. "Introduction: Access from above, access from below," in *Shadow Libraries,* edited by Joe Karaganis, MIT Press, pp. 1–24.

Keucheyan, Razmig. 2008. "Philosophie politique du pirate" *Critique*, (733–734): 458–469.

Keucheyan, Razmig, and Laurent Tessier. 2008. "Présentation. De la piraterie au piratage." *Critique* 64 (733–734): 451–457.

Kiriya, Ilya, and Elena Sherstoboeva. 2015. "Russian Media Piracy in the Context of Censoring Practices." *International Journal of Communication* 9: 839–851.

Martin-Prat, Maria. 2014. "The Future of Copyright in Europe." *Columbia Journal of Law and The Arts* 38 (1): 29–47.

Nowak, Jakub. 2016. "The Good, the Bad, and the Commons: A Critical Review of Popular Discourse on Piracy and Power, during Anti-ACTA Protests." *Journal of Computer-Mediated Communication* 21 (2): 177–194.

Ostromooukhova, Bella. 2019. "Négocier le contrôle, promouvoir la lecture. Éditeurs indépendants face à l'État dans la Russie des années 2010." *Bibliodiversité* June. https://www.alliance-editeurs.org/les-politiques-publiques-du-livre,1607#

Ostromooukhova, Bella. 2021. "Free Libraries for the Free People: How Mass-Literature 'Shadow' Libraries Circumvent Digital Barriers and Redefine Legality in Contemporary Russia." *First Monday* 26 (5). https://firstmonday.org/ojs/index.php/fm/article/view/11715/10136.

Rassolov, Il'ja. 2016. *Pravo i kibernetičeskoe prostranstvo* [Law and Cyberspace]. Moskovskoe bjuro po pravam čeloveka.

Roskomsvoboda. 2017. "Antipiratskij zakon, pravoprimenenie, tendencii i sistemnye problemy za period 08.2013-06.2017" [Anti-Piracy Laws: Application, Tendencies and Systemic Problems, 08.2013-06.2017]. Archived at https://web.archive.org/web/20230926033712/https://antipiracy.changecopyright.ru.

Soldatov, Andrej, and Irina Borogan. 2016. *Bitva za Runet. Kak vlast' manipuliruet informaciej i sledit za každym iz nas* [Battle for the Runet. How Authorities Manipulate Information and Surveil Each of Us]. Al'pina.

Stelmakh, Valeria. 2001. "Reading in the Context of Censorship in the Soviet Union." *Libraries and Culture* 36 (1): 143–51.

Thiesse, Anne-Marie, and Natalia Chmatko. 1999. "Les nouveaux éditeurs russes." *Actes de la Recherche en Sciences Sociales* 126–127: 75–89.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

Van Laer, Jeroen, and Peter Van Aelst. 2010. "Internet and Social Movement ACTION Repertoires: Opportunities and Limitations." *Information, Communication and Society* 13 (8): 1146–1171.

Waldfogel, Joel. 2018. *Digital Renaissance: What Data and Economics Tell Us about the Future of Popular Culture.* Princeton University Press.

Zaslavskaya, Olga. 2015. "Samizdat. Between Practices and Representations." Lecture series at Open Society Archives, Budapest, February–June 2013. IAS Publications no. 1. Budapest, Central European University, Institute of Advanced Study, p. 87–99.

Zasurskij, Ivan. 2016. *Novaâ Model' Regulirovaniâ Avtorskih Prav. Obŝestvennoe Dostojanie i Koncepcija Obŝego Blaga* [A New Copyright Regulation Model. Public Domain and the Idea of Common Good]. Associaciâ internet-izdatelej.

7 MOBILIZATION AND DISSENT ON BLOGS AND SOCIAL MEDIA

Perrine Poupin

In Russia, digital technologies have impacted the world of activism and ways of protesting. The extent of this transformation is of such global magnitude that reflection on the internet and digital social networks is now essential to any research on these activities (Desroches 2011). Like other aspects of the social world, collective mobilization has increasingly been mediated by computerized technological media, especially on handheld devices, even in the most remote parts of the country. Most protesters have moved from emails, mailing lists, and blogs (LiveJournal) to Web 2.0 systems (social networking sites and social media such as YouTube). Users and types of use differ: Facebook, Instagram, Telegram, and X (formerly Twitter) are the main means of communication for political activists and urban and educated populations, while the Russian networks VKontakte and Odnoklassniki remain the main medium for laypeople and ordinary citizens.

In addition to being used for coordinating protest actions, since the 1990s digital technologies have enabled collectives to inform their members on a daily basis, to share counterexpertise, to put pressure on leaders, and to conduct and discuss investigations. Some initiatives are dedicated to informational activity on general or specific topics (corruption of elites, the environment, online freedoms, etc.), and some of them are now based in Europe as their founders have gone into exile. Legal assistance nonprofit organizations also provide support for victims of internet-related repression. The context of the pandemic and lockdown presented opportunities for online solidarity initiatives or, for example, virtual demonstrations that employ user-generated text inclusions on the maps of large cities offered by

GPS applications. After a historical contextualization, this chapter focuses on the interrelatedness of collective action and new technologies in the collective mobilizations in the last decades in Russia, notably before the start of the full-scale Russian invasion of Ukraine in February 2022. It shows how collective action has evolved in the Russian context, where the internet has gradually ceased to be the space of freedom it had seemed to be until the early 2010s. In conclusion, it briefly shows what these spaces have become in the context of the ongoing war, where social networks (VKontakte, as well as Telegram and YouTube) are also vectors of pro-Kremlin propaganda in Russia, in Europe, and in the Russian-occupied territories in Ukraine.

LATE 1990s AND EARLY 2000s: THE DEVELOPMENT OF A DISSENT-FOCUSED INTERNET AND THE APPEAL OF MEDIA ACTIVISM

Political marketing emerged in Russia during the 1996 presidential campaign, at a time when the Russian media had come under the control of oligarchic groups that used them as tools of media warfare. This political marketing is now part of the Russian political landscape (Rakhmanova 2012). New communication devices fascinated activists and politically engaged artists in large urban centers, who felt that political PR (public relations) and *polittekhnologia* (political technology) were essential instruments of political action and, as such, were tools to be studied (Kireev 2006: 17). Activists therefore initiated a form of "mediactivism" (a term that appeared in the late 1990s and early 2000s in Russia), with the intention of horizontally producing news that was underpinned by activism and thus proposing an alternative framing of political and social realities.[1]

During the December 1999 parliamentary election campaign, the Radek group, a collective of Moscow artists and activists, organized a spectacular performance focused on the theme of media success. This followed a series of urban artistic events that would subsequently be grouped under the name "Moscow actionism." They were strongly political and had until then been aimed mostly at their authors' community of peers. When they turned toward a broader audience, they used a model of what they saw as

an "anonymous spectator," who was meant to embody the common condition of individuals in Russia at the time. According to these artists, the chaos, depression, and violence of the 1990s had destroyed the democratic and active public of perestroika; the audience that was to be addressed had become that of the mass media. On December 7, 1999, the Radek group held up a banner on Lenin's mausoleum at the foot of the Kremlin walls with the words "Against all!"[2] The artists had invited journalists from several television stations that still enjoyed a degree of freedom of tone at the time, and they broadcasted the performance.

Participants in this type of action hoped that, by preparing a clear, unexpected, dazzling action and showing it on television, they could change mentalities. The initiators of spectacular actions saw them as the only way to attract a public discouraged by ordinary politics (Cossart and Taïeb 2011, 146). While the campaign was a success, there were no follow-ups to it (except the FSB's years-long surveillance of artists). These street performances paved the way for a series of strongly spectacular yet short-lived protest actions that required no long-term commitment. This type of action was carried out in the 1990s by the environment and freedoms activists of Khraniteli Radugui (Rainbow Guardians) and Eduard Limonov's Russian National-Bolshevik Party (NBP), and in the 2000s and 2010s by the groups Voina (2007–), Pussy Riot (2011–), and antifascist activists. Starting in the late 2010s, and even more so after 2012, these last groups were prosecuted, and their members incarcerated and forced into exile. Limonov did not have this kind of destiny: he supported Russia's annexation of Crimea in 2014 and subsequently expressed nationalist and imperialist (expansionist) positions on the issue of Ukraine. Despite this repression and the insignificant results these spectacular media-friendly protest actions yielded, they have remained very popular and are still something of a yardstick among activists and politically engaged artists and intellectuals to this day.

Mediactivism in Russia then diversified and embraced technological innovations that would subsequently shape the production and dissemination of activist-informed news. It took a turn toward video in the early 2000s and embraced digital communication devices as tools for emancipation and catalysts for social change. The development of affordable, lightweight video

cameras and mobile devices such as smartphones and tablets allowed many activists to photograph and film street rallies and protest activities. Activists began to post images online to present a different perspective on protest events than that of the official media, which provided poor coverage of these actions, if any. These images served various purposes (Poupin 2013). Among an audience of peers, stories and images allowed viewers to relive past experiences, some of which were very vivid. With the wider public, the internet allowed activists and committed artists to transmit and display visual evidence that protest and courage were possible. Activists believed that they could convince and recruit new people and encourage the public to take action. In this perspective, emotionally charged images were seen as both the medium and the message, and they were deliberately performative. They were perceived as a direct catalyst for the public's evolution (Bloomfield and Doolin 2012) from passivity to action. This view is still prevalent in the activist world.

In addition to showing street rallies, activist groups have also seized the internet and digital communication tools as opportunities to disseminate information, criticize government action, conduct public campaigns, debate, network, recruit, socialize, and organize rallies. These groups used email from the mid-1990s, (O'Lear 1999), then blogs in the early 2000s (LiveJournal, launched in 2000 in Cyrillic) (Poberezhskaya 2018), and then websites and digital platforms (in order of popularity, YouTube launched in Russia in 2007, VKontakte in 2006, Facebook in 2008, and Twitter in 2007—later than their launch in the US, Europe, and most of the Western world). Instagram was launched in Russia in 2011. Telegram was launched later, in 2013, by VKontakte's founding brothers Nikolai and Pavel Durov, after the Russian government took control of VKontakte. LiveJournal, Facebook, Telegram, and X/Twitter are mostly used in the inner circles of the political opposition and among urban, educated populations. VKontakte has always been the most popular social network in Russia in terms of number of users. Instagram and TikTok are also widely used, especially by younger users. These differences in usage reflect a political and social divide in the country, although there are mixed and complementary uses of different digital tools, depending on content and contacts. In the following,

we distinguish two main categories of users: the political opposition and nonactivist citizens.

2000s AND 2010s: PROMISES OF INTERNET AS A PUBLIC SPACE AMONG THE POLITICAL OPPOSITION

With the development of the internet in the 2000s, political activists became partial to digital media, which they saw as powerful information, communication, and organization tools. At the same time, Putin's regime was regaining control over the mainstream media. For the urban, educated population, which distrusted those media, the internet came as an information revolution after the Soviet period and the 1990s (Trakhtenberg 2004; Nenachev 2010). Internet users kept considerable freedom of tone up until the 2011–2012 election-tampering protests, which brought several hundred thousand people to the streets and marked a turning point in Russian authorities' relationship to the internet. While control mechanisms were already in place, they had until then remained targeted and subtle. For activists and some analysts, the internet was a haven for free speech and debate in Russia, and even a truly autonomous public space (Nocetti 2012). It was the locus of new forms of expression and protest that agitated the online space in Russia, largely unconcerned until then with traditional activism. The internet allowed users to engage in politics in a playful and remote way and was a factor of emancipation for the urban middle classes. Some analysts saw this freedom to inform and debate on the internet as a decoy, the "virtual emigration" of a part of the intellectuals (Tchernyshev 2008) or, to use a Russian expression, a "social safety valve." They believed the authorities tolerated it because they saw it as a way of monitoring criticism and protest, of containing it online and, if need be, of repressing the authors. Criticism of the internet as a place of alternative expression appeared in the early 2000s, when Putin came to power. At the time, most of the population still used television as their main source of information, including in Moscow.

After the 2003 parliamentary elections and Putin's continuous amendments to the electoral law that allowed for candidate screening, liberal-democratic opposition parties (e.g., Yabloko and Pravoye Delo) were expelled

from the parliamentary arena. The opposition recomposed itself and returned to the streets, which became a new space of representation for them.[3] Under these conditions, street protest was seen as the only possible means of expression for political outsiders in the public sphere (Lipsky 1968). The opposition's use of the internet shifted in accordance with these changes in the balance of power between political actors. Some of them developed information-sharing activities on the internet, broadly dealing with social issues or focusing on a particular cause (fighting high-level corruption, human rights movements, legal associations for the defense of online freedoms, etc.). They created blogs and then personal pages and websites. Some of these groups are now based in Europe, as their founders have had to flee persecution, especially after the sharp turn of 2011–2012 (see chapter 8). Other opposition political actors organized a series of street rallies for a change in the political system (the Dissenters March, 2005–2008) and the right to freedom of assembly (Strategy-31, 2009–2015), which were brutally dispersed by the authorities. LiveJournal bloggers, who played a pioneering role in Russia's internet of protest in the 2000s (Etling et al. 2010), were able to report on these events on their personal pages, as first-hand witnesses. In 2017, several tens of thousands of people took to the streets, chanting Aleksei Navalny's slogan: "Don't call him Dimon" (a slang diminutive of Dmitry), after Navalny had broadcasted a documentary on YouTube, dealing with corruption cases related to president of the government of the Russian Federation, Dmitry Medvedev, which was viewed 33 million times in just a few days. In August 2019, after some sixty independent candidates were barred from running in local elections, around fifty thousand protesters gathered in Moscow and demanded free elections.

In the 2010s, with the development of digital social networks in urban centers and the digitization of part of social life, the boundaries between the public and private spheres shifted. Sociality around political demands evolved. Activist groups thus occupied physical and open geographical spaces (street rallies), closed places (for meetings and talks), and digital public spaces alike (Baker 2011). These developments in the digitization of protest activities were seen as major improvements by activists in Russia. They explicitly called for the convergence of the street and cyberspace and sometimes even

the replacement of the former (which was increasingly targeted by repressive measures) by the latter.

Internet and digital tools offered new media opportunities for political struggles (Gamson 1998, 63): activists could compose alternative narratives to counteract both the official ones and common opinions. The narratives and images that circulated on the internet constructed imagined communities and public identities defined by opposition to the regime. Every street rally was an opportunity to produce films and photographs, which were published and broadcast online. These visual forms are powerful triggers of private and public conversations (Gunthert 2013, 2014). According to activists, without these images, there would be no action. Activists had high hopes for the internet, including for recruiting new members. They counted on media outreach more than on physical meetings at rallies and would measure the success of their actions by the reactions they generated online (Gromov 2008, 27), especially in the digital media. This media strategy and belief were typical of the 2000s and 2010s.

The development of digital media has not challenged activists' dependence on professional media—and not only in Russia (Neveu 2010; Lysenko and Desouza 2010). Many activists in Russian cities have embraced careers in journalism and have made media work central to their advocacy. Their discourses have been informed by strategies to capture media attention. Activist collectives have organized rallies and public campaigns in "media-friendly" forms—ones that conform to the Russian liberal-democratic canons of protest action—in a legalistic approach that uses accepted channels of protest such as meetings, petitions and letters, and criticism of more radical practices (unauthorized protests, strikes, site occupations, and sabotage, even in times of war like the current one). This media-centered strategy created exhausting tensions and pressures on individuals and on the pooling of resources within groups. It had an impact on advocacy and narratives about action, for activists adapted to the needs of the media more than they developed their own strategy (Rucht 2004). Instead of problematizing the activist's claims as collective issues, the media framed them as individual cases (Neveu 1999), tending to focus on certain activists within the crowd and to make heroes out of them (Gitlin 1980, 146–179). The "media certification of leaders" (Neveu

1999, 249) strengthened leaders within their organizations. It validated the traditional organizational form of Russian political opposition circles, which excludes laypersons from decision-making processes. The primary goal of this strategy was to occupy the stages of rallies and media space as much as possible in order to—as activists keep repeating—"impose (their) agenda (*povestka*) on society."[4] This strategy caused organizations to pull away from activist fieldwork (Neveu 2010, 250) for lack of time and interest and due to the risk it involves. It discouraged activist collectives from opening up spaces for discussion and politicization in rallies or meetings, even though such spaces could serve to shape a political imaginary and activist behaviors, as well as promoting tactical innovation (Sobieraj 2011).

The dematerialization of discussions has had another impact on advocacy. It has given rise to a new form of specifically online socialization that has not helped activists in Russia establish the kind of public language necessary to draw communication situations out of the two formats prevailing in the USSR: "kitchen talk" among family, friends, and close acquaintances and the rigid and formal language of official politics. The art of public speaking and listening is not a recognized exercise in political or advocacy activities. Sociologist Boris Gladarev (2013) uses the metaphor of "public deafness" to describe the lack of public speaking skills in public discussions. In Russia, as in other authoritarian countries, the internet constitutes a space for complex interactions between a variety of users, journalists, and authorities (Arsène 2011). Moreover, the different activist platforms are aggregated, and the views expressed on them tend to be homogeneous. Contributors are ideologically close, and some of them belong to the same offline networks. While they excel in narrowcasting within small circles of people who know where to find information, these platforms generally play a minor role in broadcasting and transforming opinions (Sobieraj 2011, 175). According to analysts, the Russian dissenting public space's media are clustered in a kind of "information ghetto" that is both isolated and isolating (Kiriya 2012)—an aspect that may be exacerbated by algorithms (Pariser 2011). It is difficult to concretely assess the effectiveness of online participation and mobilization, as well as the effects of the internet on explicit offline engagement, because the nature of the relevant audiences is not easily identifiable (Arsène 2011, 896).

In Russia, in the 2000s and 2010s, protest activities faced a hostile and unpredictable environment. Most of the time, they were carried out in a state of emergency. Activists were few in number and felt isolated and marginalized. Rallies averaged a few hundred participants, even in Moscow and St. Petersburg, which had populations of 12.7 and 5.4 million, respectively. Protest practices were dangerous and seldom successful, and rallies were often dispersed by the police. In this context, the internet offered the possibility to communicate without the risks involved in real-life relationships. The belief in an ability to change society through the internet has redefined the protest scene's priorities of the 2000s and 2010s. The media strategy informed as many beliefs as it fueled uncertainties among activists. As a certain circular logic of causality would have it, the absence of activists and of a social base prompted activists to choose the media strategy. This process widened the gap between political activists and the rest of the population, and between experienced activists and less invested ones who are quick to leave the collectives. The media strategy was both a cause for and a consequence of the erosion of activism.

Moreover, making activist practices visible on the internet carried risks: it could attract the authorities' attention and lead to close surveillance and police and judicial repression. Russian activists found this out in the 2010s. The information and digital traces left on web platforms by opposition and progressive activists (antiracist, LGBT, antifascist, etc.) have also been used by their political enemies, members of far-right or pro-Kremlin movements. Far-right movements started using the internet and digital tools in the late 1990s, like other activist groups, to organize and to disseminate propaganda (Kuzmin 2008). Since the 2000s, they have been using manipulation and disinformation techniques to disseminate hate speech and stigmatization on websites, online libraries, blogs, and digital social networks. The internet was also a resource for these groups to prepare their street actions: by using LiveJournal they were able to coordinate the Russian March, an annual demonstration of nationalist movements, which has been taking place since 2005 in major Russian cities. In 2006, the Movement Against Illegal Immigration—which played a key role as an intermediary between political parties, MPs, and far-right movements in the 2000s—even used LiveJournal to organize

riots against people from the Caucasus, especially Chechens, in the small industrial town of Kondopoga, in Karelia. In the 2000s and 2010s, far-right bloggers identified activists (especially antifascist ones) in street protests with the help of online material, reported them to the authorities (through ultranationalist politicians close to the government), and published lists online of "enemies of the people" with names, photographs, addresses, and phone numbers. While it is not entirely certain that this was a direct result of online identifications and denunciations, a dozen of the antifascist activists whose names were circulated online were murdered in the 2000s.

Pro-Kremlin youth movements have also been very active on the internet since the 2000s. The government has reportedly spent considerable sums of money paying progovernment bloggers to delegitimize opponents by flooding their blogs and video sites with photomontages and defamatory comments or by organizing cyber-attacks (Stukal et al. 2022). With the advent of blogs, online media, and social media, practices such as "trolling" have emerged, a form of provocation aimed at diverting a conversation from its original topic and dragging it to unstable ground by using unproductive and hateful arguments. These practices provoke anger and destabilize other internet users. Another one is "flooding," where a few users generate a large number of messages in order to drown out their opponents' voices. With progovernment actors massively producing disparaging images of the government's opponents online, the internet cannot be properly used as a tool for discussion and political advocacy, and its predominant uses thus turn toward entertainment and private communication.[5] At the same time, the government media and their allies have never stopped flooding the Internet with patriotic, nationalist, and imperialist content, particularly since the annexation of Crimea in 2014, to justify it and galvanize popular support.

The opposition internet peaked during the major protests of 2011–2012. The blogging platform LiveJournal and the social media platforms Facebook and Twitter played a key role in disseminating content offering visual evidence of election fraud (Radchenko et al. 2012; Reuter and Szakonyi 2015; White and McAllister 2014). The government simply replied that this evidence was fake. At the same time, progovernment youth movements organized rallies in Moscow's central squares to prevent opposition protests

from taking place. Denial of service attacks were also carried out on opposition websites and digital platforms (LiveJournal, Twitter, Facebook). Many rumors were spread on these networks about the dangers of demonstrating. Internet users reacted to these online attacks and threats with derision and calls to demonstrate. Social media, including VKontakte, facilitated communication and the organization and coordination of rallies and thus played a part in increasing participation (Enikolopov et al., 2020), especially through the use of hashtags. After the major protests of 2011–2012, the authorities increasingly placed the internet under a regime of surveillance and repression.

LATE 2000s–2010s: LOCAL MOBILIZATION, CONTROVERSIES, AND SOCIAL MEDIA

Domestic access to the internet has increased steeply in Russia over the last twenty years.[6] No longer a technological privilege of a few expert activists or of the educated population in large cities, the internet is now used by large numbers of people. Social media have gradually become one of the main sources of information in Russia (Toepfl 2013)[7] and have been effective vehicles for whistle-blowers to reveal information to a wide audience.

During the 2000s, local and more or less interconnected collective mobilizations, led by NGOs or residents' collectives, used the internet in various fields in Russia, including safeguarding heritage[8] and defending housing and access rights in cities (Clément et al. 2010), environmental and planning conflicts,[9] transport,[10] criticism of the state's arbitrary use of power,[11] the fight against pension reform (2018), trade unionism, the defense of the public sectors of research, education, culture, social welfare and health, election watching, and documenting frauds such as ballot box stuffing (2011–2012), and so on.

Some groups used only one platform (their website or LiveJournal); others used several. New digital tools emerged in the 2000s: dedicated websites were created for petitions linked to a particular mobilization, and then online petition websites appeared (such as Change.org and Avaaz.org). Uses also varied according to the types of activities groups led. In the late 2010s, in

mass mobilizations such as the struggle against a national mega-landfill project in Shies, in the Arkhangelsk region (2018–2020), activists used VKontakte for community-building and communication. They also used public Telegram channels to distribute information to a smaller audience than on VKontakte (Poupin, 2021a, 2021b), which was also widely used during Russia's "garbage revolt" (Wu and Martus 2020). When it comes to the practical aspect of coordinating actions, activists preferred to use encrypted messengers, such as WhatsApp, Viber, and Telegram, rather than VKontakte chats, as they are perceived to be safer from Russian law enforcement. These messengers thus constituted "backstage spaces" in mobilization (Treré 2019).

From the early 2000s, the internet (LiveJournal and then VKontakte) offered a source of instant information and an alternative to the official media in emergency situations, especially when terrorist attacks, natural disasters (Asmolov 2020), or industrial catastrophes struck (Golbraich 2011). By the late 2000s, the internet had spread outside the large urban centers and capital cities to small and medium-sized towns and rural areas and then to the country's most peripheral regions. It gave visibility to little-known regions and territories and to the struggles of their inhabitants to defend the environment or better their daily life, which the media had until then marginalized and erased. The greatest increases in the number of web users in the 2010s and early 2020s have been in the country's small towns and rural areas. As in many countries, the spread of the internet in some areas has been greatly facilitated by the reduced cost of access and the rapid development of mobile communication technologies.

Virtual online communities were created around common local problems or emergencies. They brought together individuals who seek to provide practical responses to immediate problems (Zvereva 2012). Faced with the government's slow and weak response to pressing issues, volunteer associations developed digital social networks. Examples include efforts led to fight forest fires and provide support for their victims in 2010, to rescue people from flash floods in Krymsk in the Krasnodar region in 2012 (Roesen and Zvereva 2014), and to solve everyday roadwork and residential common space management issues. Activists have created applications to document these types of problems in different spheres (elections, education, ecology,

transport, public health, etc.) and report them to the authorities (Ermoshina 2014). In this way, the internet has encouraged and organized offline action, which is part of an ad hoc emergency response system. Some groups have become permanent and have been reactivated during other similar disasters. This was the case of many of the citizen forest fire–fighting groups. Many Indigenous groups living in Russia (Saami, Tatars, Komis, Buryats, Evenks, Nenets, Yakuts, Karelians, etc.) have also used the internet to voice their political demands and defend their rights. They have been particularly active on environmental issues. They have also been able to connect with other Indigenous groups elsewhere in the world, notably in northern Europe and the US. However, these claims were never relayed by Russian-ethnic activists in both urban and rural areas.

Societal issues entail complex politicization and depoliticization dynamics, which vary according to the context, issue, and time. Mobilization and controversies are revealing events in terms of publicizing problems and politicizing social issues (Chateauraynaud 2010). However, they also come as time-limited sequences. An issue such as pension reform, garbage disposal, or an industrial disaster becomes problematic and controversial only under certain conditions and for a given period of time. It is then redefined and returned to a kind of oblivion when the administrative and social routine settle down again (Hird et al. 2014). When they are at the center of public and media attention, these matters are "public issues" (Gusfield 2013). Mobilized citizens then expect the authorities to be accountable, to inform them, and to describe these problems in a transparent way.[12] In these light-shedding processes, the internet has profoundly altered the regimes under which actions, events, individuals, and experts and counterexperts are visible. It has disrupted the worlds of information and knowledge. The internet in Russia also provided many critical supports for those seeking information. It has profoundly modified the modes of existence of issues in the public eye and the scope and circulation of arguments (Bureau et al. 2003). It has created new publics and transformed the modalities of public appearance and the way in which collective actors take up causes, make themselves heard, and fight for visibility. It has offered mediation of a different kind to the traditional institutional, television, and journalistic ones. The internet was

used to inform and to be informed, day-to-day, to take stock of controversial issues, to conduct and disseminate counterexpertise and citizen inquiries, to challenge power, and to discuss, compare, and put into perspective the results of mobilizations. These processes could be seen in the many groups dedicated to the struggles and issues mentioned above, on VKontakte and Facebook.

Environmental struggles in the 2000s and 2010s presented some interesting features in terms of connections between mobilizations and digital tools. They were the first large-scale protest actions tolerated by the Soviet authorities during perestroika, and they gave rise to a large-scale environmental movement from 1986 to 1991 (Coumel and Elie 2014; Raviot 2001). After the fall of the Soviet regime, these movements lost steam (Coumel and Elie 2014; Henry 2010), and some of their activists were co-opted by the organs of power under Yeltsin (Yanitskii, 1999). Others ran nongovernmental organizations that often subsisted on Western funding; they chose the path of moderation and technical expertise and did not establish or rely on a social base (Ziegler and Lyon 2002). During perestroika, the mass media would cover environmental issues, sometimes even critically. From the 2000s onward, such topics were erased from the media agenda as the mainstream media became loyal to the government. In response, environmental activists were the first to turn to digital social media. In the 2000s, environmental organizations such as Greenpeace, WWF, Bellona, the North Caucasus Environmental Watch, and Save the Utrish (Nature Reserve)! were pioneers in the use of digital tools such as websites, VKontakte, LiveJournal, Facebook, and Twitter (Golbraich 2012).

Since the early 2010s, environmental and health issues have gained momentum in the media, digital social networks, and public concerns.[13] This was happening worldwide. Tanguy Lepesant (2018), for instance, has described similar dynamics in Taiwan. Environmental concerns took center stage in the democratic context of the late 1980s, were overlooked in the 1990s and 2000s, and made a strong comeback in the 2010s. This development coincided with the rise of the internet and digital social networks. In parallel, an increasing number of environmental conflicts have cropped up in the Russian regions, right before the 2022 war started. At the time, ecology was one of the topics with the strongest potential to mobilize the Russian

population; the destruction of the immediate environment and health conditions drew more attention than political or human rights issues. The most discussed environmental issues on local digital networks such as VKontakte were the destruction of parks in cities, the felling of forests, and development projects threatening natural environments and local life (Golbraich 2019). The largest groups organizing around these issues had tens of thousands of members.

There were different types of environmental groups, with some covering ecology in general and others focusing on a specific conflict. The latter mostly used VKontakte and YouTube. Active users of pages on local conflicts went outside the digital space and engaged in offline rallies and actions. Their various groups were quite diverse and loosely interconnected. As Vladimir Golbraich (2018) has shown, the VKontakte pages of local single-issue groups in St. Petersburg were very poorly connected to each other and to generalist groups. Yet, for some massive and unprecedented mobilizations, such as the struggle against the mega-landfill project in Shies, in the Arkhangelsk region, information was circulated outside single-issue groups (Golbraich 2021; Poupin 2021).

Until recent years, the political opposition has shown little interest in these initiatives and mobilizations, as it focused on demands for systemic change and on denouncing corruption and political repression, to the detriment of social and environmental issues (Wood 2018). Local social and environmental mobilizations, on the other hand, tend to steer clear of political parties, including liberal opposition movements. Mobilized residents felt that politics was a separate, dangerous, corrupt, and vile realm, which should not be approached. Opposition movements and parties had traditionally built more of a presence on Western social media (Facebook, Telegram). From 2013 and until his death, the famous nationalist and liberal opponent Aleksei Navalny was an exception to the rule: his professional communication team at the Anti-Corruption Foundation (FBK) implemented a transmedia strategy to mobilize public opinion on websites, emails, LiveJournal, Twitter, Odnoklassniki, Instagram, VKontakte, Facebook, YouTube, Telegram, and so on (Gambarato and Medvedev 2015). While they systematically fail to credit them, his reports often drew on material published by local activists,

officials, and journalists who lived near the sites in question in the provinces. Examples of this included coverage of the Shies struggle and the Norilsk oil spill (in May 2020).

2020–2021: THE COVID-19 PANDEMIC, HEALTH MEASURES, AND ADVOCACY

The Covid-19 pandemic was a health disaster in Russia. For fear of having to deal with mass discontent directed at President Putin, the government chose to delegate binding measures to regional authorities after the September 2020 parliamentary elections. The result was a chaotic epidemic response, with regions in which the health situation was comparable adopting very different measures and health passes sometimes being valid only at local level. Uncoordinated yet very strict health measures stoked discontent and distrust of the government, which until then had not paid much attention to people's health (the health system has deteriorated significantly, especially in the provinces). During the pandemic, masses of people switched to remote work or learning and had to adapt to the digitization of many state services. The pandemic led to a more massive use of the internet and digital social networks. As in other countries, these networks have contributed to the circulation of misleading information and polarizing, hateful, and stigmatizing speech.

The health and social crisis that came with the Covid-19 pandemic also triggered a wave of volunteerism, which was carried out through or with social media. Various aid movements were initiated to provide vulnerable people with basic necessities, support health facilities and staff, and provide legal assistance to patients and their families. For example, Yandex.Maps users used hashtags to connect volunteers with people in need in their neighborhoods.

In 2020, after restrictive measures had been put in place, virtual rallies were led in several Russian cities, including Rostov-on-Don, Krasnoyarsk, Nizhny Novgorod, and Moscow. Internet users would drop a pin close to a local or federal government building on a map on the Yandex.Map application and attach comments to these pins (to the effect of "Down with

the passes!" for instance). Yandex "dispersed" these rallies by deleting messages that were deemed inappropriate. Another online rally was organized in February 2020, against the sweeping constitutional revision that allowed Vladimir Putin to remain in power until 2036.

At the same time, and despite the context of the pandemic, massive street demonstrations, bringing together tens of thousands of protestors, took place. For example, Khabarovsk, the largest city in the Russian Far East, saw demonstrations from July 2020 to September 2021 against the political arrest of the region's governor, Sergei Furgal. The social media VKontakte, Odnoklassniki, and Twitter provided platforms to organize these events and to show them (Brodovskaya et al. 2021). Navalny was arrested in January 2021 upon returning from Berlin, where he had spent several months recovering after he was poisoned. His team retaliated with numerous calls for protests on social media. On the popular video-sharing platform TikTok, which is widely used by high school students, the hashtag #svobodunaval'nomu (#FreeNavalny) was shared over ninety million times in just a few days. They also posted a documentary on YouTube about Putin's massive compound on the shores of the Black Sea, which was viewed more than sixty million times. In the context of the pandemic, like in other countries, the government banned demonstrations. Despite this, about fifteen thousand people gathered in Moscow, along with several thousand others in about a hundred cities across the country. These rallies were violently dispersed.

2022—RUSSIA'S WAR IN UKRAINE: A CONCLUSION

As mentioned above, most Russian citizens have Internet access. While unofficial, critical, and relevant sources of information are available on many topics (on Telegram and YouTube, for example), relatively little use is made of them. Internet users have to choose who to believe: these alternative sources or the official ones. This is a difficult task, as people generally do not consciously consider these choices and therefore accept the official, dominant news as accurate and reliable, without verifying its sources. The majority of people in Russia seems to have internalized and assimilated the official

interpretation of the events that took place in Ukraine in the winter and spring of 2014 (Maidan, the annexation of Crimea, and then the Russian occupation of the Donbass territories) and since February 24, 2022 (the current war) and even more so to be indifferent to the fate of the people of Ukraine under the bombs. The silence or general passivity toward this fate is the result of indifference, of not knowing or not wanting to know, or alternatively, of a repression of such knowledge. Social media is full of content that shows ordinary life as it used to be, as if nothing has happened. Along with these events came a flood of Russian nationalist online discourse and activity. Anti-Maidan groups on VKontakte, which the government funded, instrumentalized nostalgia for the Soviet past—which Putin's regime cultivates—to describe Ukrainian protesters and the provisional government that emerged from the Maidan revolution as "fascists" and "Nazis" (Kozachenko 2019). Warmongering has made its way onto the political and media agenda and managed to remain at the center of public attention since February 2022. Television remains the main media in Russia, and its contents are prevalent in shaping most citizens' worldview.[14] The official mainstream media are also available online. Their websites draw considerable traffic, and as internet users quote them extensively, social media platforms find themselves relaying state propaganda. In Russia—as elsewhere, of course—only a minor part of the population knows the rules of the disinformation game.

A small part of the population spoke out against the war in late February 2022, for one month. In March the Russian State Duma quickly adopted a law on "discrediting the army" (Article 20.3.3), which also covers online discourse such as posts, comments, and even "likes." Amendments were made to the Code of Administrative Offences as well as to the Russian Criminal Code. Between late February and late November 2022, 19,428 people were arrested at antiwar rallies—the vast majority of them in the first month of the war—just over 5,000 fines (averaging 400 euros) were issued, and about 350 court cases were filed on grounds of false information and discrediting the army.[15] However, in practice, judges often side with the citizens accused under this article, and funds have been raised to help pay these fines. In this context of war and media censorship, the messaging application Telegram has grown in popularity. It is now a major source of information

for some and a propaganda vehicle for others. Internet thus allows for fake news and propaganda to be disseminated on colossal scales while also offering stronger platforms for broadcasting knowledge and debunking content than before. As a result, due to the strength of this propaganda and the absence of long-term reflexive work on the imperial nature of the Russian regime, the critique of imperialism and the formulation of a decolonizing agenda both outside and inside the country have never been a highly visible priority for the Russian digital social media, including those of the various types of activists mentioned above.

In this chapter, we have observed how the internet can serve to exchange information, encourage political discussion, and organize protest activities, as well as being a tool for surveillance, communication, and repression in the hands of state or progovernment nationalist organizations. The Russian case shows interesting perspectives on the effects of online activism on offline protest activities. While the internet shines a light on mobilizations and public problems that emerge over a huge territory and might therefore have been hidden from the general public, activism in Russia remains a very high-risk activity. It requires preparation for face-to-face situations, which the internet does not provide. We have also seen that disinformation covers all political and social issues in Russia, and especially protests, the Covid, and the war in Ukraine. The internet is used to build not democratic publics, but reactionary groups, ignorance, and hatred. Disinformation creates conflicts and divisions between people and increases social polarization. It is difficult to say what will emerge from this. Times are uncertain and the sands of Russian society are shifting, to say the least.

NOTES

1. On the concept of mediactivism, see (Cardon and Granjon, 2013).
2. According to the Russian Constitution, it was legally possible until 2006 to vote "against all candidates." If this statement garnered a majority of votes, new elections would have to be held, with new candidates. This never happened.
3. Democratic leader Ilya Yashin explains this in his 2005 book *Ulitchny protest* (Street Protest) (https://www.yabloko.ru/Publ/Book/Yashin/protest_004.html, accessed February 17, 2023).
4. The notion of "agenda-setting" was imported from the US and entered massively into the ordinary language of journalists, tens of thousands of whom have attended courses in the US

and NGO seminars in Russia since 1991. The NGO Interviews, for instance, provided them with free professional training until Vladimir Putin had it shut down in 2007 (Matvejchev 2010, 10).

5. Arsène noted a similar turn of events in China (2011, 897).

6. From 2 percent in 2000 to 50 percent in 2011 and 80 percent in 2019 for the population over 16 years old (https://www.tadviser.ru/index.php/Статья:Интернет-доступ_%28рынок_России%29).

7. According to a survey conducted in August 2020 by the Levada Centre, over a third of Russians get their news from social media (https://www.levada.ru/2020/09/28/ggh/).

8. Against the construction of the Gazprom Tower, which would have been the new tallest building in Europe, in St. Petersburg in 2009, using a website, LiveJournal, and VKontakte.

9. Defending urban parks slated to be replaced by parking lots or real estate projects; protecting Lake Baikal against chemical pollution; defending the Khimki forest, on the outskirts of Moscow, against a motorway project in 2007–2011 (according to the media outlet Public.ru's observation, this was the blogging topic the media took up the most in 2010 and 2011: http://www.public.ru/blogsmi and http://www.public.ru/blogsmi2011); opposing the Sochi Olympics project, which led to many illegal expropriations in 2014; and mobilizing against a national mega-landfill project in Shies in the Arkhangelsk region in 2018–2020.

10. There was mobilization against customs taxes on imported cars in Vladivostok in 2018 and against transport taxes in Kaliningrad in 2009–2010.

11. As does the Society of Blue Buckets, which fights against traffic violations by official vehicles.

12. These actions are summarized in Harold Garfinkel's notion of "accountability" (see Koschmann 2019).

13. A poll conducted in January 2020 by the Levada independent research center found that 48 percent of Russians saw environmental pollution as one of the main threats to humanity, ahead of terrorism (42 percent) or wars (37 percent) (https://www.levada.ru/ 2020/01/23 /problemy-okruzhayushhej-sredy/).

14. In a study published by the independent Levada Centre, in June 2022 an average of 63 percent of respondents mentioned television as a source of news in Russia overall, while only 52 percent of respondents in Moscow did. Internet media was mentioned by 32 percent of respondents in Russia and by 50 percent of Muscovites; 16 percent of respondents in Russia and 30 percent of Muscovites also mentioned Telegram as a source of information: https://www.levada.ru/2022/07/15/istochniki-informatsii-moskva-i-rossiya/.

15. As of late November 2022. These data were compiled by the OVD-Info movement, founded in 2011, which records political arrests throughout Russia and provides legal assistance to their victims: https://data.ovdinfo.org/svodka-antivoennyy-repressiy-devyat-mesyacev-voyny.

REFERENCES

Asmolov, Gregory. 2020. "Runet in Crisis Situations." In *Internet in Russia. A Study of the Runet and Its Impact on Social Life*, edited by Sergey Davidov. Springer.

Arsène, Séverine. 2011. "De l'autocensure aux mobilisations. Prendre la parole en ligne en contexte autoritaire." *Revue Française de Science Politique* 61 (5): 893–915.

Baker, Stéphanie-Alice. 2011. "The Mediated Crowd: New Social Media and New Forms of Rioting." *Sociological Research Online* 16 (4).

Bloomfield, Brian, and Bill Doolin. 2012. "Symbolic Communication in Public Protest over Genetic Modification: Visual Rhetoric, Symbolic Excess, and Social Mores." *Science Communication* 20 (10): 1–26.

Brodovskaia, Elena, Maria Davydova, Aleksandr Doncov, and Anna Hardikova. 2021. "Bazovye tendencii transformacii massovyh političeskih protestov v RF (2020–2021 gg.)" [Basic trends in the transformation of mass political protests in the Russian Federation (2020–2021)]. In *Proceedings of Tula State University* 2.

Bureau, Marie-Christine, Francis Chateauraynaud, Christophe Lejeune, Didier Torny, and Patrick Trabal. 2003. "Internet à l'épreuve de la critique." Report for the CNRS program "Société de l'information."

Cardon, Dominique, and Fabien Granjon. 2013. *Médiactivistes*. Presses de Sciences Po.

Chateauraynaud, Francis. 2010. "Des disputes ordinaires à la violence politique: l'analyse des controverses et la sociologie des conflits." In *La Politisation: conflits et construction du politique depuis le Moyen Âge*, edited by Laurent Bourquin and Philippe Hamon. Presses Universitaires de Rennes.

Clément, Karine, Olga Miriasova, and Andrey Demidov. 2010. *Ot obyvatelej k aktivistam. Zarožd*aûiecâ *social'nye dviženâ v sovremennoj Rossii* [From Ordinary Men to Activists: Emerging Social Movements in Contemporary Russia]. Tri kvadrata.

Cossart, Paula, and Emmanuel Taïeb. 2011. "Spectacle politique et participation. Entre médiatisation nécessaire et idéal de la citoyenneté." *Sociétés & Représentations* 31 (1): 137–156.

Coumel, Laurent, and Marc Elie. 2014. "A Belated and Tragic Ecological Revolution: Nature, Disasters, and Green Activists in the Soviet Union and the Post-Soviet States, 1960s–2010s." *Soviet and Post-Soviet Review* 40 (2): 157–165.

Desroches, Dominic. 2011. "La fabrication du climat politique. Analyse de l'espace émotionnel et de la communauté d'émotions." *Implications Philosophiques*, http://www.implications-philosophiques.org/semaines-thematiques/passions-dans-lespace-public/la-fabrication-du-climat-politique/. Accessed September 7, 2024.

Enikolopov, Ruben, Alexey Makarin, and Maria Petrova. 2020. "Social Media and Protest Participation: Evidence from Russia." *Econometrica* 88 (4): 1479–1514.

Ermoshina, Ksenia. 2014. "Democracy as Pothole Repair: Civic Applications and Cyber-Empowerment in Russia." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 8 (3).

Etling, Bruce, Karina Alexanyan, John Kelly, Robert Faris, John G. Palfrey, and Urs Gasser. 2010. "Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization." Berkman Center Research Publication, no. 2010–2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1698344.

Gambarato, Renira Rampazzo, and Sergey Medvedev. 2015. "Grassroots Political Campaign in Russia: Alexey Navalny and Transmedia Strategies for Democratic Development." In *Promoting Social Change and Democracy through Information Technology*. IGI Global.

Gamson, William. 1998. "Social Movements and Cultural Change." In *From Contention to Democracy*, edited by Marco Giugni, Doug McAdam, and Charles Tilly. Rowman and Littlefield.

Gitlin, Todd. 1980. *The Whole World is Watching*. University of California Press.

Gladarev, Boris. 2013. "Opyty preodolenia 'publičnoj nemoty': analiz obŝ estvennyh diskussi v Rossii načala XXI veka" [Experiments in Overcoming "Public Deafness": Analysis of Public Discussions in Russia at the Beginning of the 21st Century]. Conference Report, *La Société Russe à la Recherche d'une Langue Publique: Hier, Aujourd'hui, Demain* (January 15–17, 2013, St. Petersburg). European University of Saint Petersburg Publishing House.

Golbraich, Vladimir. 2011. "Počemou proizošel 'Sibirskij černobyl'"? Avaria na Saâno-šušenskoj GES v rossiskoj blogosfere" [Why Did the "Siberian Chernobyl" Happen? The Sayano-Shushenskaya Hydroelectric Power Plant Accident in the Russian Blogosphere], *Télescope* 6: 39–45.

Golbraich, Vladimir. 2012. "Social'nye seti v Internete kak resours dlâ ekologičeskogo dviženâ v Rossii" [Internet Social Media as a Resource for the Environmental Movement in Russia]. In *La Sociologie Hier, Aujourd'hui, Demain*, edited by Oleg Božkov. Éditions Eidos.

Golbraich, Vladimir. 2018. "Členy ekologičeskih grupp v sotsial'ny'h media: tsifrovoe učastie i interesy" [Environmental Group Members on Social Media: Digital Participation and Interests]. *La Sociologie Pétersbourgeoise Aujourd'hui* 9: 91–119.

Golbraich, Vladimir. 2019. "Ekologičeskie konflikty v Rossii i cifrovoe setevoe učastie" [Environmental Conflicts in Russia and Participation in Digital Networks]. *Sociologičeskie Issledovaniâ* 6: 74–85.

Golbraich, Vladimir. 2021. "Ekologičeski konflikt v povestke dlâ social'noj seti" [Environmental Conflicts on Social Media Agenda]. *Sociologie et Gouvernement* 7 (2): 102–115.

Gromov, Dmitrij. 2008. "Ulitčny teatr molodežnoj politiki: oppozicionnye dviženia" [The Street Theatre of Youth politics: Opposition Movements]. *Etnograficheskoe obozrenie* 1: 19–29.

Gunthert, André. 2013. "La culture du partage ou la revanche des foules." In *Culturenum. Jeunesse, culture et éducation dans la vague numérique*, edited by Hervé Le Crosnier. C & F Editions.

Gunthert, André. 2014. "L'image conversationnelle." *Études Photographiques* (31). https://journals.openedition.org/etudesphotographiques/3387.

Gusfield, Joseph R. (2013). The culture of public problems: Drinking-driving and the symbolic order. In *Morality and health,* edited by Allan M. Brandt and Paul Rozin. Routledge.

Henry, Laura. 2010. *Red to Green. Environmental Activism in Post-Soviet Russia*. Cornell University Press.

Hird, Myra, Scott Lougheed, Kerry Rowe, and Cassandra Kuyvenhoven. 2014. "Making Waste Management Public (or Falling Back to Sleep)." *Social Studies of Science* 44 (3): 441–465.

Kireev, Oleg. 2006. *Povarennaâ kniga media-aktivista* [The Media-Activist's Cookbook]. Ultra Kultura.

Kiriya, Ilia. 2012. "Les réseaux sociaux comme outil d'isolation politique en Russie." *Journal of Communication Studies* 5 (1): 193–207.

Koschmann, Timothy. 2019. "Tracing the seminal notion of accountability across the Garfinkelian œuvre." *Human Studies* 42: 239–252.

Kozachenko, Ivan. 2019. "Fighting for the Soviet Union 2.0: Digital Nostalgia and National Belonging in the Context of the Ukrainian crisis." *Communist and Post-Communist Studies* 52 (1): 1–10.

Kuzmin, Alexander. 2008. "'Pravy' Internet v Rossii: specifika razvitia i problemy protivodejstvâ" ["Right-wing Internet in Russia: Specifics of Development and Problems of Combating This Phenomenon"]. *POLITEX* 4 (3): 74–96.

Lepesant, Tanguy. 2018. "Les questions environnementales, espace de (re) politisation de la jeunesse taïwanaise." *Monde Chinois* 56: 108–119.

Lipsky, Michael. 1968. "Protest as a Political Resource." *American Political Science Review* 62 (4): 1144–1158.

Lysenko, Volodymyr, and Kevin Desouza. 2010. "Cyberprotest in Contemporary Russia: The Cases of Ingushetiya.ru and Bakhmina.ru." *Technological Forecasting and Social Change* 77: 1179–1193.

Matvejchev, Oleg. 2010. *Povelitel'noe naklonenie istorii* [Authoritarian Inclination of History]. Éksmo.

Nenachev, Mikhaïl. 2010. *Illiuzii svobody. Rossijskie SMI v epohu peremen (1985–2009)* [The Illusion of Freedom. Russian Media in an Age of Change (1985–2009)]. Logos.

Neveu, Erik. 1999. "Médias, mouvements sociaux, espaces publics." *Réseaux* 17 (98): 17–85.

Neveu, Erik. 2010. "Médias et protestation collective." In *Penser les mouvements sociaux*, edited by Eric Agrikoliansky, Isabelle Sommier, and Olivier Fillieule. La Découverte.

Nocetti, Julien. 2012. "Le Web en Russie: de la virtualité à la réalité politique?" *Russie.Nei.Reports*, 10. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifrirnr10nocettiwebrussiemars2012.pdf.

O'Lear, Shannon. 1999. "Networks of Engagement: Electronic Communication and Grassroots Environmental Activism in Kaliningrad." *Geografiska Annaler: Series B, Human Geography* 81 (3): 165–178.

Pariser, Eli. 2011. *The Filter Bubble. What the Internet Is Hiding from You*. Penguin Press.

Poberezhskaya, Marianna. 2018. "Blogging about Climate Change in Russia: Activism, Scepticism and Conspiracies." *Environmental Communication* 12 (7): 942–955.

Poupin, Perrine. 2013. "Quand les manifestants s'emparent de la vidéo à Moscou: communiquer ou faire participer?" *Participations* 7: 73–96.

Poupin, Perrine. 2021. "Government Responses to Online Activities of Waste Protest: The Case of VKontakte and the Shies Uprising in Far Northern Russia." *First Monday* 26 (5). https://firstmonday.org/ojs/index.php/fm/article/view/11711/10135.

Radchenko, Darya, Dina Pisarevskaya, and Irina Ksenofontova. 2012. "Logika virtual'nogo protesta: nedelâ posle vyborov-2011" [The Logic of Virtual Protest: The Week After the 2011 Election]. *Forum d'Anthropologie* 16: 108–126.

Rakhmanova, Tania. 2012. *Au cœur du pouvoir russe. Enquête sur l'empire Poutine*. La Découverte.

Raviot, Jean-Robert. 2001. "L'écologie et les forces profondes de la perestroïka." *Diogène* 194 (2): 152–159.

Reuter, Ora John, and David Szakonyi. 2015. "Online Social Media and Political Awareness in Authoritarian Regimes." *British Journal of Political Science* 45 (1): 29–51.

Roesen, Tine, and Vera Zvereva. 2014. "Social Networks Sites on the Runet: Exploring Social Communication." In *Digital Russia. The Language, Culture and Politics of New Media Communication*, edited by Michael Gorham, Ingunn Lunde, and Martin Paulsen. Routledge.

Rucht, Dieter. 2004. "The Quadruple 'A': Media Strategies of Protests Movements Since the 1960s." In *Cyber Protest. New Media, Citizens and Social Movements*, edited by Wim van de Donk, Brian Loader, Paul G. Nixon, and Dieter Rucht. Routledge.

Sobieraj, Sarah. 2011. *Soundbitten. The Perils of Media-Centered Political Activism*. New York University Press.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. 2022. "Why Botter: How Pro-Government Bots Fight Opposition in Russia." *American Political Science Review* 116 (1): 843–857.

Tchernyshev, Yuri. 2008. "O vlânij blogosfery na rossijskuiû publičnuiû politiku" [On the Impact of the Blogosphere on Russian Public Policy]. *Sciences Politiques* 2: 99–118.

Toepfl, Florian. 2013. "Making Sense of the News in a Hybrid Regime: How Young Russians Decode State TV and an Oppositional blog." *Journal of Communication* 63 (2): 244–265.

Trakhtenberg, Anna. 2004. "Informatsionnaâ revoliuciâ i informacionnij raskol: čto proishodit v Rossii?" [The Information Revolution and the Information Divide: What is Happening in Russia?]. Annual Scientific Report of the Institute of Philosophy and Law of the Ural Department of the Russian Academy of Sciences.

Treré, Emiliano. 2019. *Hybrid Media Activism: Ecologies, Imaginaries, Algorithms*. Routledge.

Yanitskii, Oleg. 1999. "Russian Environmental Movements." In *Earth, Air, Fire, Water: Humanistic Studies of the Environment*, edited by Jill Conway, Kenneth Keniston, and Leo Marx. University of Massachusetts Press.

White, Stephen, and Ian McAllister, 2014. "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism." *Politics* 34 (1): 72–84.

Wood, Tony. 2018. *Russia without Putin. Money, Power and the Myths of the New Cold War*. Verso.

Wu, Fengshi, and Ellie Martus. 2020. "Contested Environmentalism: The Politics of Waste in China and Russia." *Environmental Politics* 30 (4): 493–512.

Zvereva, Vera. 2012. *Setevye razgovory: kul'turnye kommunikacii v Runete* [Networked Conversations: Cultural Communication in Runet]. University of Bergen.

Ziegler, Charles, and Henry Lyon. 2002. "The Politics of Nuclear Waste in Russia." *Problems of Post-Communism* 49 (4): 33–42.

8 FROM DIGITAL CONTROL TO PHYSICAL REPRESSION: SEARCHES, PRISON, EXILE, AND WAR

Olga Bronnikova, Françoise Daucé, Ksenia Ermoshina, and Benjamin Loveluck

During the 2010s, the forms of political control over the Russian internet were varied, distributed, and indirect (black boxes, ISPs, algorithms, data management, copyright rules, etc.). They relied essentially on regulating and channeling digital behavior rather than on physical violence. As authoritarian coercion gradually increased, these forms of control turned into direct attacks on the safety of people and digital goods by the state apparatus. Criminal prosecutions for online publications, as well as strong-armed searches with seizure of equipment at the offices of media outlets and NGOs, and at activists' homes, became common. Laws on "foreign agents," "extremist organizations," and "undesirable organizations" were amended to apply to a growing number of activists, journalists, researchers, and campaigners, and criminal charges were laid against those who were the most committed and publicly visible. Repression was ramped up when political opponent A. Navalny was poisoned and subsequently jailed (he died in a penitentiary in the far north in February 2024), and his entire movement was banned in 2020. This culminated in the large-scale invasion of Ukraine in February 2022 and the adoption of the so-called false military information law prohibiting use of the word "war" (March 4, 2022). Police and judiciary repression were put in place to prevent any protest mobilization.

The shift to a hardline approach articulated offline and online constraints in a broad "digital repression" dynamic that has already been documented elsewhere (Keremoğlu and Weidmann 2020; Feldstein 2021; Earl et al. 2022). Today, the issue is no longer only that of surveillance or control

through digital tools; it also encompasses the question of individuals' physical safety. Earl et al. (2022) broadly define digital repression as including:

- the use of traditional repressive techniques against online protesters (arrests, detentions, fines, searches, etc.),
- the use of digital tools to reinforce traditional repressive measures (surveillance, tapping, profiling, facial recognition, etc.), and
- the development of information strategies to reduce protest.

This has been well documented, for example, in the cases of the arrest of Saudi bloggers (Pan and Siegel 2020) and Azeri activists (Human Rights Watch 2021), as well as activists in Kazakhstan (Anceschi 2015), Egypt, Syria, and Iran (Michaelsen 2020). As activists generally operate both online and offline, retaliation through repression targets both spaces.

In Russia, since 2020 and especially following the military invasion of Ukraine in 2022, stronger digital and traditional threats based on the use of police force, physical arrests of activists, and forfeiture of their property condemned many of them to exile. From abroad, digital infrastructure and equipment are resources to facilitate their remote coordination. "Digital exile" allows for the "mobile belonging here and there" of people connected in both their host and home countries, as in the comparable case of displaced Iranian activists (Bublatzky 2022). However, during wartime these links also introduce vulnerabilities, especially for exiles' contacts back home, as maintaining communications across the frontline can expose individuals to new forms of suspicion. This double-edged dialectic has been highlighted in the case of Syrian and Iraqi activists (Gillespie et al. 2018). Exile does not end threats to the safety of political exiles, who sometimes find themselves exposed to transnational forms of repression, as witnessed during the Arab Spring (Moss 2016) and in the cases of Iranian and Syrian activists (Michaelsen 2020). In this situation, they develop new skills around sousveillance, protection, training, and expertise on digital issues (Porlezza and Arafat 2022) to continue fighting from abroad. As they engage in the struggle against the war in Ukraine, they mobilize their militant and technical knowledge to denounce the authoritarian excesses of the Russian state and the resurgence of genocidal imperialism.

This chapter presents an analysis of the trajectories of actors of the free internet, whom we first met in Russia as part of our fieldwork and were later able to meet with again abroad after their forced exile. We documented the ordeals faced by these activists (especially those from the NGOs Roskomsvoboda, Teplitsa, and the Internet Protection Society [OZI]), by independent journalists (from the main independent online media), and by activists in organizations facing repression by the Russian authorities. Their paths also cross with Belarusian activists, who have likewise faced brutal repression since the summer 2020 protests. While they are scattered abroad, these exiles nevertheless remain connected (Diminescu 2005); some of them describe themselves as *relokanty*, or relocated.[1] They are opposed to the war in Ukraine and to V. Putin's regime but remain part of networks and social circles in their home country and generally continue with critical activities intended for the Russian public or conceive of new associative and media initiatives aimed at the diaspora. While these initiatives benefit from looser constraints in the host countries, they are also caught up in the geopolitical confrontations of war. Exile introduces a situation of significant asymmetry between those who have relocated and those who have remained, in terms of the digital and legal risks incurred (Ermoshina 2024). This means that those who have stayed in Russia may be inclined to call into question the legitimacy of the discourses of those who have relocated, especially when exiles call for protest from the relative safety of the countries where they have settled.

VIOLATION OF PHYSICAL AND DIGITAL INTEGRITY: ARRESTS, SEARCHES, AND FORFEITURE

Throughout the 2010s, the Russian state's repressive repertoire diversified as it created a range of legal, judicial, and technical requirements to restrict digital practices (see chapter 1). These multiple, distributed constraints relied on technical infrastructures (access and service providers, platforms, boxes, networks, algorithms) to discipline the public space. As early as 2012, the law first authorized the authorities to block websites without a court order. In 2016, according to the Google Transparency Report, the Russian state sent the largest number of requests ever to Google to remove content (Bronnikova

and Zaytseva 2021). In the same year, the Yarovaya laws came into force, requiring internet service providers to save users' traffic data and, on request, to provide government services with users' personal data along with the contents of their e-mail boxes, where applicable. From 2017 onward, many digital operators received warnings from Roskomnadzor, threatening them with fines or closure. In 2018, the Russian state unsuccessfully attempted to block the Telegram application.

Gradually, individuals themselves, and not just their data or content, have been caught up in the oppressive web of power, threatened with ever heavier fines and detention. Arrest, searches, and other police threats are some of the dangers faced by internet users. Prosecution targeting users who have employed circumvention tools such as Tor (the "Bogatov case")[2] or published or republished critical content online, as well as the opening of criminal cases for alleged extremism served as warnings to all critical actors on the Russian internet. This government repression was based not only on police and security practices that were well documented in Russia (Le Huérou 2022) but also on forms of intimidation "from below," such as denunciations by "vigilant citizens" (Favarel-Garrigues 2018; Daucé et al. 2020). With the war, the physical and digital integrity of all opponents of Russia's military aggression against Ukraine came under threat, both online and offline. Given the ubiquitous and intimate nature of the internet, this can be considered a human rights violation (Rochel 2021).

ATTACKS ON ORGANIZATIONS AND INDIVIDUALS

Throughout the 2010s, demonstrations and street actions were followed by mass arrests and detentions lasting from a few days to a few weeks. The security services laid charges against the most committed activists, journalists, and opponents, which usually also involved searches at their homes and offices. To stifle any protest, the repertoire of repressive measures relies on traditional methods common to all oppressive regimes: denunciations, arrests, remand in custody, opening of criminal cases, and searches.

Opposition organizations and media fall under the law on "extremist organizations" or "undesirable organizations," which puts their members

in jeopardy. In 2020, the legislation on "foreign agents," initially targeting nonprofit organizations (2012) and the media (2017), was extended to individuals in their personal capacity. Many of the journalists and activists we met during our survey were blacklisted by the Ministry of Justice as foreign agents, such as human rights defender Lev Ponomarëv, feminist activist Daria Apakhonchich, Radio Svoboda journalist Elizaveta Maetnaya, editor-in-chief of Mediazona Sergei Smirnov, director of the Society for the Defence of the Internet Mikhail Klimarev, and Social Technology Greenhouse activist Natalia Baranova. The list is already long and is growing by the month. All the legal entities and individuals concerned are subject to in-depth controls (of their resources and expenses in particular) and must publish a banner online officially announcing their status as foreign agents.

Starting in 2019, activists from Aleksei Navalny's Anti-Corruption Foundation (FBK) became prime targets of prosecutions and searches. An activist who worked on the *Navalny Live* program, which is broadcast online on YouTube, described almost weekly raids on the studio, to the point where all the audio and video equipment were seized to stop the broadcast. The team had to innovate by setting up two parallel studios, so that they could switch the broadcast from one to the other. "Sometimes the cops really didn't understand what was going on. They would block everything during the search and the broadcast would continue. It made them so mad."[3] These searches often involved physical violence and psychological humiliation ("They put us on the floor, buried our heads in the carpet and left us like that for six hours, threatening to beat us up. They didn't even let us go to the toilet."). Rather than a judicial or administrative investigation tool, searches in this context are a proven method of harassment and intimidation. In April 2021, A. Navalny's Foundation was dissolved nationwide after being listed as an "'extremist and terrorist organization."

Searches are also carried out on human rights organizations and the editorial offices of investigative media. In June 2021, the homes of the journalists of the media outlet Proekt were raided. A few days later, Proekt was accused of threatening the country's order and security, and declared "undesirable" in Russia. Users who collaborated with its editorial staff were liable for criminal prosecution. In July 2021, the organization Komanda 29,

which defends political prisoners, was also declared undesirable and forced to cease all its activities. To protect its members, it deleted all its online content and social media accounts. It advised its readers to delete all the content it had produced, thus practically erasing all traces of its activity. In general, the physical and digital repression of recent years calls into question the durability of digital content: the digital security trainers and the media and NGOs at risk recommend deleting data, both at an individual level (clearing the memory of computers and telephones) and at a collective level (regularly deleting chat histories or even deleting entire websites, as Komanda 29 had to do). In response, independent archiving projects have been launched, such as the National Digital Archive,[4] while the Russian state archives content for judicial purposes.[5]

ATTACKS ON DIGITAL DEVICES AND DATA

While repression (arrests and searches)—abundantly documented by human rights organizations since 2012[6]—endangers the physical integrity of individuals, it also threatens their digital equipment and data. These are particularly vulnerable during arrests. Confiscation of computers and mobile phones is officially illegal but possible under threat of force. This deprives activists of all communication tools and compromises both the data related to their activities and the personal information stored on their devices. During house searches, systematic attacks on digital assets have been documented. Computer equipment (computers, telephones, hard drives) is seized, which raises safety issues both for the people searched and for their political and professional contacts.

Since 2018, many testimonies, especially from people belonging to A. Navalny's movement, have described these violations. An activist told us, "When they searched, I just had time to block access to my phone and my Telegram channel. But I couldn't do anything about my Mac, which was seized." Two years later, in 2020, he was arrested again for "disrespecting the organs of power." During his one-week stay in prison, he testified: "They seized my phone. I could only use it for 15 minutes a day. I wasn't ready for this situation because all my data was on my sim card. They took all the data from my Microsoft account, all my contacts on Skype. They took everything,

absolutely everything. When they force you to put your fingerprint to open the phone, there's nothing you can do about it."[7] Another activist from a regional branch of A. Navalny's movement also reported: "There were searches in 2019 when they opened the first criminal cases, accusing us of laundering crime money. . . . The searches took place in the movement's offices and in the homes of activists. There were three waves: first the coordinators of the movement, then the volunteers and finally their parents. They wanted to deprive us of all our equipment.—*'All of it?'*—Yes, phones, computers, USB sticks, cameras, absolutely everything."[8] In the case against Ekaterina Muranova, an anarchist activist from Medvezhiegorsk accused of advocating for terrorism, even her six-year-old son's tablet was seized.

The individuals and organizations facing these risks developed legal and technical know-how to train themselves in new protection tools and learn the principles of "holistic security," which encompasses the physical and legal safety of people and their digital data, as well as their psychological integrity (see chapter 4). Human and digital rights organizations, such as OVD-Info and the Social Technology Greenhouse, published advice for people who were arrested, to enable them to defend themselves. All organizations advised that a virtually blank phone should be used for demonstrations and street actions. During administrative detentions, they suggested blocking the phone before handing it over to the police and requesting its return at the end of custody. Legally, seized property must be returned at the end of the judicial investigation procedure, but activists question the reliability of the returned goods. As one activist explained, "The equipment returned by the police should not be used, as it may contain malicious or surveillance software that is a danger to the user."[9]

THE OUTBREAK OF WAR AND FORCED EXILE

The most committed dissidents generally understood detention, and the accompanying searches especially, as such a serious warning that they considered exile. In some cases, at the end of the search, the police returned the international passport to its holder, which was immediately interpreted as an incentive to leave. Security trainers also advised keeping one's international

passport outside the home. If the passport was not returned, the threat of arrest became clear, prompting people to leave the country illegally by any means possible (even overland, through the forests on the country's western borders). A journalist in exile in Vilnius recalled the story of a colleague who was forced to flee: "He crossed the Ukrainian border on foot, his family stayed in Moscow. His house was searched and both his passports were taken away. This meant he risked prison. When they leave your passport after a search, it's an invitation to flee."[10]

After the invasion of Ukraine in February 2022, the incentive to leave became even more explicit. Despite the risks of repression, many citizens signed online petitions to denounce the war (the petition launched by human rights defender Lev Ponomarëv collected more than a million signatures in a few days), and the most intrepid took to the streets, where the police made mass arrests. The adoption of the law on "fake military news" (March 4, 2022) forbids journalists to use the very term "war" and requires them to publish official sources. As they refused to submit to censorship, many media outlets, which were already registered as foreign agents, were permanently blocked at the request of Roskomnadzor. For having covered the war in Ukraine, the websites of Dozhd television and Echo of Moscow radio, as well as the news websites Meduza, the BBC's Russian service, and Radio Svoboda were all banned in Russia. Major international platforms were also targeted. Facebook and X/Twitter were blocked, while TikTok chose to suspend its activities.[11] In addition, foreign technology companies and service providers voluntarily left the Russian market, and Google and Apple suspended access to online payment systems for Russian users. The entire Russian digital ecosystem, where international operators (GAFAM [Google, Apple, Facebook, Amazon, Microsoft]) coexisted with national competitors (VKontakte, Yandex), has been disrupted by wartime digital restrictions. Only YouTube services remained temporarily accessible, which made it the main open channel for accessing alternative media and cultural content.

In this context, activists, journalists and citizens received direct or indirect threats from security services. Sometimes incredulous at the time of the first alerts, they subsequently realized the severity of the risks they run. According to a freelance journalist from Rostov whom we interviewed in Tbilisi,

> On 24 February, . . . a friend who knows someone at the FSB wrote me to say that . . . well, I have to leave Russia, because if I don't I'll probably be prosecuted for a criminal case soon. I asked her: "Are these criminal proceedings against me or against journalists in general?" She said: "against you personally." I answered something like "Fuck you, I'm not going anywhere, I'm going to stay here until the end" . . . Three days later I more or less came to my senses and told myself that I really should leave Russia, because going to prison now would be totally counterproductive for my family, my work . . . [12]

Once the decision to leave has been made, the experience of "digitally crossing" to another country is transformative. The goal is to take as much as one can of one's digital life and hiding what might be compromising (Latonero 2015). Activists and journalists are careful to delete all data on their devices and disconnect from the main social media they use, to avoid attracting security services' attention. Best practice guides and wiki-like sites are proliferating, which try to synthesize experiences of border crossings and holistic self-defense practices while traveling abroad. As the journalist from Rostov recalls,

> At the airport, I was interrogated by FSB men. They checked my Telegram application. I was expecting them to and I'd deleted all the channels I was following. . . . They asked me about my political preferences. I answered that I don't support any movement because I don't like any of them. You have to encrypt the disk on your notebook when you cross the Russian, Belarusian or Azeri borders. If the authorities seize it for forty minutes and it's not encrypted, they can download everything.[13]

After many years of repression, the protection of their physical and digital integrity has become a vital requirement for all politically persecuted and prosecuted persons in Russia—including when they are forced to leave.

EXILE, DISPERSION, AND THE ROLE OF DIGITAL NETWORKS FROM ABROAD

The number of Russian citizens in exile steadily increased during the year 2022. According to some estimates, it had reached one million people by December. Although it is dwarfed by the eight million Ukrainians who have

had to flee the war in their country, this number of departures is unprecedented for post-Soviet Russia. The political exile began with the repression of the 2011–2012 protest movement and followed a timeline that accelerated as authoritarianism grew. The first political activists and journalists left for the Baltic States, Germany, and Israel, marking out the routes that the following exiles would follow in various ways.

From February 2022 onward, the scale of the exile broadened the range of destinations. A rough map highlights the main places of refuge (Riga, Vilnius, Tbilisi, Berlin, Tel Aviv, Yerevan, Istanbul), in addition to the historical rear bases of the Russian opposition (including, for example, Mikhail Khodorkovsky's teams in London, Radio Free Europe in Prague, the hacker and artistic community in Berlin, etc.). These various trajectories outline some favorite destinations, mostly of course because of simplified entry, residence, and visa regimes for Russians. But the place of exile is not always the result of a programmed trajectory, and an exile's first port of call is not necessarily their intended destination, which may also vary according to their profile (journalists, activists, lawyers, internet specialists called *ITichniki*, etc.). Those professionals who are the most present in the media and the public sphere manage to obtain visas in European Union countries, while the other exiles remain stuck in countries that are not as safe because they are still within the Russian sphere of influence or are not protected by NATO membership. According to some exiles, there is also a difference in treatment between "political" emigration (for which there are administrative categories) and what they call "moral" emigration.[14]

THE BALTIC STATES: OUTPOSTS OF POLITICAL EXILE

A map of media in exile shows journalists' preferred locations for the editorial offices that produce information for Russian-speaking audiences, both in Russia (despite the main websites being blocked) and abroad. While some journalists find refuge in Western Europe, most of them prefer to work in countries bordering Russia, to stay in a Russian-speaking space and be close to their sources and readers. The Baltic States (Latvia and Lithuania) and Georgia have become their go-to host countries. The best-known editorial

offices, those that enjoy a strong international reputation and are well integrated into transnational media networks, have for many years given priority to Riga. Unaffiliated freelance journalists, who often work for the regional media, often find temporary asylum in Georgia. A social and professional distinction is emerging, depending on the reputation and resources of journalists' editorial office of origin.

The exile of Russian journalists began in 2014, following the annexation of Crimea and the adoption of the Lugovoy law on blocked websites. The most exposed journalists, such as the team of the media outlet Grani.ru, for instance, chose to leave and to settle mainly in Western Europe, with help from the NGO Reporters Without Borders. Following the dismantling of the general news media outlet Lenta.ru, the editor-in-chief, Galina Timchenko, transferred her team to Latvia, where she founded the website Meduza.io. The Latvian government facilitated her installation and Meduza became a new reference among online media, thanks to its team of editors in Riga and its correspondents in Russia.

From 2020 and 2021 onward, the number of Russian journalists taking refuge in Riga would gradually increase following many threats targeting editorial offices. Journalists from the investigative media outlets The Insider, Proekt, and *Istories* moved to the Baltic States. The Latvian authorities were prone to issue humanitarian visas (D visas) to create a hub for Russian journalists in exile in their capital. From February 2022, teams from the best-known international media groups, such as Dozhd television, the BBC's Russian service, *Novaya Gazeta*, Radio Svoboda and some regional media (Lyudi Baykala, *Pskovskaya Guberniya*) all moved to Latvia. There, they received material and logistical support from their employers (the BBC chartered a bus to take its journalists from Moscow to Riga in March 2022). According to witnesses, by December 2022 nearly two hundred Russian journalists had settled in Latvia. Latvian institutions have provided them with places to set up their newsrooms.

Also starting in 2020, many Russian activists moved to Vilnius, following the repression of A. Navalny's movement. His supporters found refuge there, with the support of the local authorities. They rub shoulders with activists of the Free Russia Movement, supported by Garry Kasparov, who

has organized an annual opposition forum there since 2014. Some Russian journalists have also chosen to settle in Vilnius since 2014. A journalism school for Russian journalists from the provinces was created by a former journalist in 2018. Her "media school" offers training courses to raise awareness of safety issues among Russian journalists, including a training module on digital security, in partnership with the French nonprofit Nothing to Hide. The aim of the training is also to create information and mutual support networks between journalists. Before the war, she also planned to offer retreats for burned-out journalists in protected areas, with the help of specialized psychologists.[15]

In Lithuania, all these Russian actors meet the thousands of Belarusian exiles who settled in Vilnius, a few dozen kilometers from the Belarusian border, following the violent repression of demonstrations against opponents of A. Lukashenko's regime in the summer of 2020. They form an exile community united by the presence of S. Tsikhanouskaia, the exiled "president" of Belarusian opponents. There are several reasons why the Baltic States are one of these political exiles' preferred destinations. In geographical terms, they allow them to stay close to the Russian and Belarusian borders, and some can even pay short visits to their relatives. As there are large Russian-speaking minorities in these countries, the local linguistic environment facilitates their integration. Moreover, the Baltic States' European Union and NATO membership seems to provide them with security guarantees. At the interface between the former Soviet Union and the European Union, they are an outpost for exiles, who also set up solidarity actions there.

Their increasingly large presence is, however, causing tensions. On December 6, 2022, the Latvian National Council for Electronic Media (NEPLP) withdrew Dozhd's license to broadcast on cable in the country. This sanction followed controversial remarks by a journalist from the channel, Aleksei Korostelev, who spoke live about his organization's desire to "help Russian soldiers sent to the front." Latvian authorities understood this statement as support for the Russian army attacking Ukraine and immediately condemned it. The NEPLP accused Dozhd television of "threatening national security and public order" and stated its recriminations: use of the term "our army" to refer to the Russian army, publication of a map of

Russia that included Crimea, Aleksei Korostelev's ambiguous remarks, and Dozhd's interview with the mayor of Riga, which was deemed too critical. Russian journalists perceived the NEPLP's sanction as a "mirror" of the Russian government's sanctions on the media. They were deeply shaken by it: "We have become enemies here and there," said one journalist, who was registered in Russia as a foreign agent and arrived in Latvia in the spring with her children. This controversy illustrates the contradictory demands that political exiles are faced with, caught as they are between their bond with their community of origin and their integration into the host society. As a result of this conflict, Dozhd television obtained a broadcasting license in the Netherlands and announced its relocation to Amsterdam.

THE DISPERSION OF TRAJECTORIES WITH THE WAR AGAINST UKRAINE

Since the war began, paths of exile have branched out to a range of destinations beyond the Baltic countries. Alternative or autonomous actors, who are not supported by their employer when emigrating and often do not have a preexisting network, adapt to the available opportunities. Some go to Central Asian countries, others to the Caucasus, while others yet go to Turkey or manage to reach the European Union. In the rush, whatever ticket they can buy to get out is often the determining factor, as is the accessibility of any country that does not require a visa.

In Georgia, many journalists arrive in Tbilisi thanks to administrative facilities that allow them to settle in the country for long stays without a visa. Many of them are young journalists from the editorial offices of local Russian media (in Kazan or Rostov, for example) or freelancers working for various independent media. They resume their work remotely from Tbilisi, living in a precarious situation without a salaried contract with an editorial office or any certainty regarding their situation in this country. Although Georgia is more independent from Russia than some post-Soviet states, civil society actors often allege that the ruling party is too tolerant of Russian citizens in Georgia, for fear of straining relations with Russia. Georgia has banned media figures such as Mikhail Fishman, a political journalist from

Dozhd, and Mitia Aleshkovski, an activist and journalist who created OK Russians, a self-help network for Russian exiles (now called NODA), from entering the country.

The liveliness of the projects being developed in Georgia sets it apart from many other destinations for Russian exiles. Some journalists are involved in small alternative media that are being set up in response to the war, such as the feminist online media Verstka and the Kholod project. Others are creating local media, telling the story of the Russian diaspora in Georgia and talking about Georgia to Russian exiles, such as Paper Kartuli, founded by former journalists from the St. Petersburg media outlet Bumaga. Since March 2022, at least five nonprofit organizations aimed at supporting Ukrainian refugees have been established by Russian nationals, either exiled after the start of the large-scale war or having lived in Georgia for a longer period. Long-standing political exiles sometimes offer assistance to newcomers, providing them with accommodation or urgent advice on how to navigate the migration process. In other cases, the new arrivals, especially those who waited until the mobilization began in Russia to go into exile, arouse suspicion and criticism from those who left immediately after the invasion began. The trajectories of exiles are very fluid, and the first host country is often a stepping stone on the way to another destination. Journalists and activists thus pass through Georgia or Kyrgyzstan before reaching Riga, Prague, or even Berlin or Paris. In this vast exodus, there is a high degree of uncertainty regarding people's locations, as a digital presence often compensates for the indeterminacy of physical location.

REGAINING PHYSICAL AND DIGITAL INTEGRITY

Exile is an experience of personal and professional, individual and family, and moral and administrative insecurity. In the face of uncertainty, obtaining a legal status (a residence permit), finding a place to call home (obtaining accommodation), getting children into school, and accessing financial resources (opening a bank account) are priorities for exiled people. There is also the matter of restoring their digital integrity. The wide disparities in exile's trajectories, which started to increase from February 2022 onward, is

accompanied by an intense use of online resources. These resources maintain a link between geographically distant people and a presence in the public space. With the first mass departures, coordination tools immediately emerged to facilitate communication. On Signal and Telegram, channels and chats were created to circulate information and coordinate mutual aid, both at the level of each country of exile and internationally. A key example is the Kovcheg initiative,[16] which set up a per-country system of local chats to exchange know-how and share experiences.

Exile also takes the form of new socio-technical barriers. In the context of the Sovereign Runet law, many important Russian services have become inaccessible from foreign IP addresses (such as Gosuslugi, the Russian public services website, and banking applications). To restore digital links with the home country, exiles have to use VPNs with servers located in Russia that have been set up by volunteers (free of charge) or by start-ups (for a fee). In addition to these digital tools, what are known as "human VPNs" have also been developed, especially to circumvent the ban on international bank transfers (sometimes with very complex schemes involving several human and technological intermediaries), as well as the "opportunities" (*okaziya*) system of mutual assistance for the delivery of documents, medicines, or other valuables between Russia and countries of exile.

Once they are safe abroad, exiles can extricate themselves from the constraints imposed by the oppressive Russian apparatus and regain integrity online. However, this process is neither self-evident nor uniform. Some people registered as foreign agents defy the constraints of this status by ceasing to mention the mandated and degrading warning label on their publications, to declare their income to the Russian Ministry of Justice, or to keep bills for all their daily expenses. The activist Daria Apakhontchitch, in exile abroad, has turned her report to the ministry into an antiwar manifesto, which she posts online to denounce the violence of the war. Others, however, continue to abide by these legal obligations. Their departure is not enough to lift Russian legal obligations. Many activists who are registered as foreign agents continue to comply with the obligations this entails to be able to return to Russia in cases of absolute necessity (to visit an ill relative, for instance). Prosecutions can also be brought against activists who are already

abroad. For example, the director of the Internet Protection Society (OZI), Mikhail Klimarev, who is close to A. Navalny's movement, was put on the Russian Interior Ministry's wanted list in November 2022, even though he had been out of the country for a long time. Abroad, exiles remain concerned about surveillance and provocation by members of the special services sent by Moscow, especially in the countries of the post-Soviet space where Russians can travel without a visa.[17]

NEW DIGITAL MOBILIZATION IN EXILE: HOW TO ACT IN TIMES OF WAR

From abroad, activists, journalists, and exiled citizens access an uncensored digital space with information on military violence and crimes committed by Russia in Ukraine. This extreme brutality produces a vast individual and collective reflex, which raises the question of historical legacies, political responsibilities, and moral reparations toward Ukraine. In this dynamic, the digital network participates in this new reflexivity by raising the question of the dissemination of antiwar content in Russian society, on the one hand, and of the mobilization of exiled citizens, on the other.

Digital freedom activists are at the heart of these two dynamics, as evidenced by the Internet Without Borders initiative led by the main nonprofit organizations promoting the free internet (OZI, Teplitsa, Roskomsvoboda, eQualit.ie). They organized a series of talks and hackathons for ITichniki in the spring of 2022 in the main cities hosting exiles (Tbilisi, Yerevan, Vilnius, Warsaw, Berlin, Paris, Haifa), which were markedly more technical and applied than their other events. During these meetings, they promoted the use of censorship circumvention tools to allow the circulation of content to audiences in Russia. They also mobilize their exiled peers to imagine new initiatives against the war and to build solidarity networks in exile. These technical dynamics raise political questions. While some of them incriminate the policies of the Russian regime and attribute the war to Putin's authoritarianism, others more broadly blame the imperial nature of the Russian state. They put forward decolonial arguments to envisage its defeat, which are coherent with the positions of Ukrainian citizens fighting to defend their state.

INFORMATION AGAINST THE WAR

Access to audiences in Russia is a major concern of exiled activists and journalists who insist on fighting state propaganda inside their country. From the start of the war in February 2022, they have been concerned about Western sanctions that would lead the Russian internet to be disconnected from international digital networks. For activists from digital freedom organizations such as Roskomsvoboda, OZI, and Teplitsa, maintaining the technical infrastructure is essential if they are to reach the critical Russian public. As early as March 2022, Roskomsvoboda issued a statement against sanctions by international companies in the digital sphere, fearing that they would primarily affect ordinary users, who have a vital need for pluralistic information.[18] Feminist activists, such as those from the Feminist Anti-War Resistance (FAS), also criticize the decision:

> I spend 24 hours a day, 7 days a week, coordinating the feminist anti-war movement in Russia and in exile. We provide logistical, technical and organizational help and support. In case of danger, we get activists out of the country. Today, our mission is to get the guys out of Russia: women get the guys out of Russia—can you believe it!—so that they don't go and kill Ukrainians. I don't see why we should be prevented from doing all this by making it more difficult to access the internet, without which we can't do anything.[19]

In the spring of 2022, the Internet Without Borders talks promoted tools to circumvent online censorship in order to keep in touch with audiences in Russia. According to the activists, ten to twenty million Russian users regularly use VPNs to access content that is blocked in Russia. Their goal is to significantly increase this number. The issue of content circulation is crucial for journalists in exile who produce information to raise awareness of the ravages of war, seeking to document the crimes committed in Ukraine and to alert Russian public opinion to the criminal violence of the armed forces. Being abroad allows them to regain their freedom of speech and to use terms that are forbidden in Russia (especially the word "war"). While they are blocked in Russia, these media groups run campaigns promoting tools to circulate their content. They have developed digital guides to circumvent constraints, in collaboration with Russian digital freedom organizations.

Thus, at their own level, they are contributing to empowering their readers and participating in the dissemination of alternative digital information. After being blocked in Russia, the Meduza, Mediazona, OVD-info and Kholod websites invited their readers to follow them on different media platforms (Telegram channel, mirror sites, email list). Some media groups create their own application to download on mobile devices. Above all, they advise their readers to use VPNs to overcome blockages in Russia, directing them to the most reliable solutions available on the market (Bronnikova and Daucé 2022).

While the technical opportunities afforded by digital tools allow them to act remotely, building on the knowledge gained during the pandemic, online safety issues remain in the foreground in communication with those who have stayed in Russia. Journalists in exile are concerned about the safety of the informants that allow them to continue covering Russian news. They use security measures for their digital communications with their sources in Russia (secure social networks, data encryption, etc.). From abroad, this relationship with sources is difficult. As a BBC journalist and video producer relocated to Riga explains, "My work depends a lot on the ability to film in Russia. And this ability has been strongly impacted, it has become very hard to work. . . . People don't want to talk to us remotely by video link, they would like to meet us in person. . . . People are afraid we might be spies, but sometimes they talk when they need us."[20] To overcome the difficulty of accessing sources, the media in exile work with freelance journalists or local acquaintances who take risks in the field but are not under the responsibility of the editorial office that employs them.

MOBILIZING WITHOUT BORDERS

For activists and journalists alike, establishing new links with people dispersed by exile is a major challenge for promoting a political agenda against the Russian regime and the war. From the Baltic States, the Caucasus, or Western Europe, many digital initiatives are being invented to network citizens scattered by the war. Physical meetings are organized in the main cities of exile, along with online conferences to bring together those who have

relocated. The Internet Without Borders meetings, for example, enable exiles to network in their new places of residence and between their different host countries. In their declaration the organizers claimed that: "the 'Internet Without Borders' conference . . . has technical and social ambitions for the local diaspora, most of whom are Russian speakers. We are campaigning for free access to the Internet as a means of combating political propaganda, so that citizens have access to plural information."[21]

The meetings involve hackathons, which are designed to tackle technical challenges collectively. In Paris in November 2022, developers were invited to introduce users not specialized in digital technology to the CENO browser (censorship.no), which uses the BitTorrent protocol to access blocked information. They were also asked to popularize AmneziaVPN, a free service for creating a personal multiprotocol VPN on one's own server. During these workshops, exiled developers are able to form local relationships to foster a new social fabric in which they can exchange know-how and political projects. The meetings, which take place in Russian, bring together about a hundred people in each host city.

The networks of digital freedom activists intersect with those of political activists and human rights defenders who organize demonstrations or publish petitions against Russian state policy. Human rights defender Lev Ponomarëv attended the Internet Without Borders conference in Paris, coorganized by the ResisTIC team, alongside representatives of the Russia Freedom Association, members of the Memorial organization in exile, and a journalist from Dozhd television based in Paris. In the audience, young activists, artists, and students from Russia showed a common interest in militant uses of digital technology and their importance and challenges in the context of the war.

IS THE FIGHT AGAINST POLITICAL AUTHORITARIANISM OR COLONIAL DOMINATION?

Free internet activists have long hoped the internet would bring democracy and called out the Russian political regime's growing authoritarianism. With the war, a controversy is emerging among Russian exiles: is it the

war-mongering Russian state's authoritarianism that should be denounced, or is it, rather, the imperialism of its society as a whole? In light of this controversy, can the defense of a democratic agenda suffice without a fundamental critique of Russian colonialism? The trajectories of exiled opponents diverge considerably, depending on their political vision for Russia's future. Antiwar initiatives come with public statements that can generate tension. Many "forums for a free Russia," wishing to revive the democratic and liberal project, propose projects to restore the country's economy or rehabilitate its reputation (with initiatives such as the white-blue-white flag, which symbolically expunges the color red associated with blood and communism). However, critics point out that their positions fail to bring a decolonial perspective and to challenge the very project of a Russian Federation.

Ukrainian activists, fighting for the survival of their country, argue that "this is a war not between two states but between two systems: authoritarianism and democracy,"[22] but they denounce Moscow's colonial oppression more generally. In her Nobel Peace Prize acceptance speech in December 2022, Ukrainian lawyer and human rights activist Oleksandra Matviichuk said, "The Russian people will be responsible for this abject page in their history and for this attempt to restore their former empire by force. . . . This is why the Ukrainian people's determination to resist Russian imperialism is so important."[23] A perspective that can be described as decolonial, which deconstructs the concept of Russia, is gaining popularity among Ukrainian citizens as well as among some exiles from Russia. It is defended, in particular, by the organizers of the Internet Without Borders initiative who, in a statement, have claimed that they "share the interpretation of this war as imperial and Ukraine's resistance as decolonial. The organizers acknowledge the weight of centuries of difficult relations between Russia and Ukraine, which Soviet and Russian propaganda has tried to pass off as brotherhood or friendship. The words 'fraternal nations', both in this context and in the political context, are interpreted by the organizers as instruments of colonization of Ukraine and are not shared by them."[24]

"Decolonial" and regionalist media projects, such as *Beda Media*,[25] the Free Buryatia Foundation,[26] the Free Yakutia Foundation,[27] and so on are developing to inform Russian-speaking readers about the colonial issue.

Exile allows Russian opponents, newly settled in independent neighboring states, to observe and experience different cultures, thus putting their own political, linguistic, and economic positions into perspective. This experience brings self-criticism and raises questions about what it means to be Russian and the project of the Russian Federation—especially as they learn more and more about Russia's colonial past. This critical perspective changes the individual trajectories of Russian activists in exile. They now focus on local issues, learn the local language, try to join initiatives in host countries, and do extensive work on the vocabulary they use in their daily lives on the internet, including emphasizing Russia's colonial past and deconstructing the narrative of "greater Russia" and its "brother-peoples." Examples of these processes include Russian activists in exile in Armenia getting involved in the campaign to support the city of Artsakh, which is blocked by Azerbaijan, or the House under the Red Roof project in Bishkek (Kyrgyzstan), a cultural center opened by Russian citizens with the active participation of local communities.

The democratic and decolonial positions circulating on the "Runet in exile" are not necessarily consensual and lead to debates, controversies,[28] and sometimes even the end of relationships of cooperation. However, their very existence testifies to the emergence of a pluralist Russian-speaking public space beyond the country's borders, which defies the patriotic and reactionary demands of the Russian regulator. It gives a glimpse of what could be a digital world freed from authoritarian constraints, capable of carrying out projects for Russia other than the deadly war against Ukraine. However, these alternative voices remain weak and dispersed by exile. In Russia itself, criticism has become inaudible. For twenty years, the trajectory of digital authoritarianism has been built up in small oppressive steps, in response to the free inventiveness of Runet users. A multitude of actors, human and nonhuman, have been enlisted in the vast repressive mesh constructed at multiple scales of the internet. While limited spaces of freedom remained online until February 2022, the large-scale military aggression against Ukraine lifted the last authoritarian taboos, justifying censorship, surveillance, and digital controls as a defense of the national interest against hostile foreign forces. This bellicose and imperial authoritarianism embraces

new technical opportunities to hijack the internet's promise and spread state propaganda to connected citizens, mobilize its online society, and destabilize opposing countries. Russia thus offers a disastrous example of augmented authoritarianism whose materiality is quite ordinary, although it carries a tragic political project. It is therefore a heuristic case to study when it comes to framing and preventing the autocratic drifts of contemporary societies that could be bolstered and underpinned by digital technologies.

NOTES

1. The term, coined during the Covid pandemic to refer to the geographical displacement of remote workers, is now used by some of the people forced to leave Russia during the war. It exists in addition to other categories of displacement (migrants, exiles, displaced persons, expatriates).
2. Dmitry Bogatov is a developer, mathematics teacher, open-access software activist, contributor to the Debian and GNU projects, and an Esperantist. He has been accused of making public calls for terrorist acts on the internet, on the forum sysadmins.ru. These messages were identified with the IP address of a server hosted at Bogatov's home, which was an exit node he maintained in the Tor network. The mathematician was initially remanded in custody on April 6, 2017, but a campaign for his release was organized and supported not only by many Russian and international organizations such as the Pirate Party, Roskomsvoboda, Access Now, and the Electronic Frontier Foundation, but also by open-access software projects such as Debian and Torproject itself. The Bogatov case mobilized the open-access software developers and cypherpunk communities, culminating in a series of tweets by Edward Snowden himself in July 2017. Six months after his arrest, Bogatov was placed under house arrest in his Moscow flat and later acquitted. He and his wife Natalia Fedorova, a researcher with a PhD in biology, left Russia and moved to the United States, where Bogatov was granted political asylum.
3. Interview with an activist in exile, Warsaw, June 2022.
4. https://ruarxive.org/
5. https://web-arhive.ru/
6. See the International Federation for Human Rights (FIDH) reports on Russia (https://www.fidh.org/fr/regions/europe-asie-centrale/russie/14548-russie-2012-2013-l-offensive-contre-les-libertes).
7. Interview with an activist in exile, Vilnius, November 2021.
8. Interview with an activist from the Anti-Corruption Foundation, Tbilisi, May 2022.
9. Interview with an activist, Vilnius, November 2021.
10. Interview with a journalist, Vilnius, November 2021.

11. For a chronology of these bans and censorship decisions, see https://timeline.resistic.fr/.
12. Interview with an independent journalist in Tbilisi, May 2022.
13. Interview with a journalist exiled in Vilnius, November 2021.
14. Observation and discussion with Russian volunteers from Ukrainian refugee aid associations in Tbilisi, September 2022.
15. Interview with a Russian journalist in exile, Vilnius, November 2021.
16. https://kovcheg.live/
17. Interview with journalists in exile in Georgia, May 2022.
18. https://roskomsvoboda.org/uploads/documents/statement_of_roskomsvoboda_team.pdf
19. Interview with an activist from the Feminist Anti-War Movement, September 2022, Tbilisi.
20. Interview with a refugee journalist in Riga, 4 December 2022.
21. https://internetborders.net/statement-on-war/
22. Interview with a Ukrainian activist by the chapter authors, November 2022.
23. The French translation of this speech was published by the newspaper *Le Monde*: https://www.lemonde.fr/international/article/2022/12/10/discours-du-prix-nobel-de-la-paix-la-guerre-en-ukraine-n-est-pas-une-guerre-entre-deux-etats-mais-entre-deux-systemes-l-autoritarisme-et-la-democratie_6153845_3210.html.
24. https://internetborders.net/statement-on-war/
25. https://www.beda.media/
26. https://instagram.com/freeburyatiafoundation?igshid=YmMyMTA2M2Y=
27. https://instagram.com/freeyakutiafoundation?igshid=YmMyMTA2M2Y=
28. See the editorial "Russkie, zatknites" (Russians, shut up), *Grani.ru*, 22 July 2022, https://graniru.org/opinion/editorial/m.285545.html.

REFERENCES

Anceschi, Luca. 2015. "The Persistence of Media Control under Consolidated Authoritarianism: Containing Kazakhstan's Digital Media." *Demokratizatsiya* 23: 277–295.

Bronnikova, Olga, and Françoise Daucé. 2022. "Un manuel de survie numérique pour s'informer et éviter la censure en Russie." May 2. The Conversation. https://theconversation.com/un-manuel-de-survie-numerique-pour-sinformer-et-eviter-la-censure-en-russie-181889.

Bublatzky, Cathrine. 2022. "Mobile Belonging in Digital Exile: Methodological Reflection on Doing Ethnography on (social) Media Practices." *Media and Communication* 10 (3): 236–246.

Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. 2020. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia." *Laboratorium: Russian Review of Social Research* 11 (3): 46–70.

Diminescu, Dana. 2005. "Le migrant connecté: pour un manifeste épistémologique." *Migrations/Société* 17 (102): 275–292.

Earl, Jennifer, Thomas V. Maher, and Jennifer Pan. 2022. "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review." *Science Advances* 8 (10. https://www.science.org/doi/full/10.1126/sciadv.abl8198.

Ermoshina, Ksenia. 2024. "Voices from the Island: Informational Annexation of Crimea and Transformations of Journalistic Practices." *Journalism* 25 (3): 528–546.

Favarel-Garrigues, Gilles. 2018. "Justiciers amateurs et croisades morales en Russie contemporaine." *Revue Française de Science Politique* 68 (4): 651–668.

Feldstein, Steven. 2021. *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford University Press.

Gillespie, Marie, Souad Osseiran, and Margie Cheesman. 2018. "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances." *Social Media + Society* 4 (1). https://journals.sagepub.com/doi/full/10.1177/2056305118764440.

Human Rights Watch. 2021. *Azerbaijan*. https://hrw.org/europe/central-asia/azerbaijan.

Michaelsen, Marcus. 2020. "Silencing Across Borders: Transnational repression and Digital Threats against Exiled Dissidents from Egypt, Syria and Iran." Hivos Foundation (Humanist Organisation for Social Change). https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf.

Keremoğlu, Eda, and Nils B. Weidmann. 2020. "How Dictators Control the Internet: A Review Essay." *Comparative Political Studies* 53 (10–11): 1690–1703.

Latonero, Mark. 2015. "For Refugees, a Digital Passage to Europe." Thomson Reuters Foundation News. December 27. https://news.trust.org/item/20151227124555-blem7/.

Le Huérou, Anne. 2022. "Les paradoxes du recours au droit dans les mobilisations contre les violences policières en Russie." *Champ Pénal/Penal Field* 26. https://journals.openedition.org/champpenal/14158.

Moss, Dana M. 2016. "Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring." *Social Problems* 63 (4): 480–498.

Pan, Jennifer, and Alexandra A. Siegel. 2020. "How Saudi Crackdowns Fail to Silence Online Dissent." *American Political Science Review* 114 (1): 109–125.

Porlezza, Colin, and Rana Arafat. 2022. "Promoting Newsafety from the Exile: The Emergence of New Journalistic Roles in Diaspora Journalists' Networks." *Journalism Practice* 16 (9): 1867–1889.

Rochel, Johan. 2021. "Connecting the Dots: Digital Integrity as a Human Right." *Human Rights Law Review* 21 (2): 358–383.

CONCLUSION TO THE ENGLISH-LANGUAGE EDITION

Françoise Daucé, Benjamin Loveluck, and Francesca Musiani

On February 24, 2022, Russia's large-scale military aggression against Ukraine marked a turning point in the lives of Ukrainians, brutalized by the violence of war, the occupation by Russian troops, and the material destruction inflicted on the country. While this rupture brings to mind the memory of the great military and political violence of the twentieth century, it is now also taking place in the digital world. In Russia, the war was immediately accompanied by massive repression of war opponents, a strengthening of political controls over the national segment of the internet, a tightening of blockades on online resources, and the withdrawal of many international partners as a result of the sanctions. The controls and censorship imposed on the digital space, on the territory of the Russian Federation, and in the occupied territories of Ukraine, are a continuation and extension of the digital authoritarianism described in this book, which was incrementally set up during the 2010s. The war in Ukraine itself did not begin in 2022, but in 2014, with the annexation of Crimea and the start of the war in the Donbass. Control of the Russian internet was strengthened from this period onward. The multifaceted research presented in this collective book provides us with valuable material for thinking about the transformations of the Russian internet and the dynamics that saw its shift from peace to war.

DIGITAL AUTHORITARIANISM IN THE CONTEXT OF WAR

The invasion of Ukraine has had an immediate impact on the way in which the Russian government controls the internet, and in how Russian society

uses it. All the coercive mechanisms gradually deployed during the 2010s were suddenly tightened to ensure that the national internet became a key tool serving the aims of war. It was not a change of nature, but a change of scale. The same control and surveillance mechanisms have been maintained and strengthened. This capacity for rapid adaptation is based on the plasticity of the Russian internet as a result of the decentralized and plural nature of regulations, which are constantly adapting to the challenges arising from the war. The rules, practices, and actors adapt their activities to the requirements of state institutions. Although the political injunctions come from above, they are implemented by a wide range of actors who adjust to the new political demands.

Legal provisions, infrastructures, algorithms, and data are being aligned, monitored, and censored in order to serve long-term war aims. Following some of the actions and strategies presented in this book (chapters 1, 2, 3, and 5), the coercive laws adopted throughout the 2010s have been amended to tighten controls on digital actors and published content. The powers of Roskomnadzor, the communications surveillance agency, have been extended. Digital companies have to comply with state requirements. The major Russian digital platforms, such as Yandex, have been placed under the direct control of the presidential administration. In March 2022, the main Russian media (Ekho Moskvy, *Novaya Gazeta*, Dozhd, etc.) and international digital platforms (Facebook, Instagram, Twitter, etc.), which had remained largely outside the control of the state, were blocked. The frequency of bans suddenly accelerated. This dynamic has continued ever since. In the summer of 2024, Roskomnadzor ordered the blocking of Signal messenger and asked that YouTube be throttled in Russian territory.

The control of the digital public space gives Vladimir Putin, his party, and his administration undivided control over Russian political life. It allows them to stifle any criticism of the war. The major media and news aggregators have aligned their positions with those of the Kremlin and adopted the language of its press secretary. The word "war" has been banned when referring to the military intervention in Ukraine. While plural content is still circulating on Telegram, the loudest voices are those of war supporters. The most radical actors, such as the "Z bloggers" (Russian war supporters)

on Telegram channels, are also the most vocal, while supporters of peace are silenced. In August 2024, the arrest in Paris of Pavel Durov, the founder of Telegram, raised the question of the future of this platform. Praised by Russian opponents for his contribution to digital freedoms, Durov is being prosecuted in Europe for his complacency toward illegal trafficking on his application. The future of Telegram is now not only a Russian issue, but also an international one.

In this context, the repression of political opposition continues, and any protest within Russia, offline or online, has become impossible. In February 2024, Alexei Navalny, who was serving a long prison sentence for politically motivated reasons, was left to die in a penal colony in the far north. His supporters took substantial risks to pay tribute to him at his funeral. In March 2024, Putin was reelected for another six-year term with a particularly high score, after tightly controlled elections and in the absence of any political competition. He immediately reappointed his previous government, with the notable exception of the defense minister, who was replaced. Whereas elections had usually given rise to opposition mobilizations since the mass protests of 2011–2012, the 2024 elections were marked only by symbolic actions (such as voters going silently to the polling stations at midday to show their opposition to the incumbent authorities). There were no public protests either online or offline. The repressive measures taken against protesters have stifled most, if not all, criticism. According to OVD-Info, an independent human rights defense and media group, 20,056 persons were detained for expressing antiwar views from February 24, 2022 until August 22, 2024.[1] Some still post antiwar content on social media, but what might be dubbed "slacktivism" elsewhere carries a real price in Russia, with numerous convictions linked to antiwar publications on social networks.[2]

THE RESILIENCE OF RUNET AND THE CIRCUMVENTION OF SANCTIONS

As the war in Ukraine continues, its impact on digital reconfigurations in Russia is lasting—particularly as a consequence of the international sanctions imposed on the country. These involve not only traditional trade embargoes

but sophisticated digital sanctions, as underlined by Park and Shin (2023). They include restrictions on quantum computing, IT services, manufacturing, aerospace technology, and financial technologies. The imposed EU sanctions include bans on semiconductors and software and IT-related consulting and engineering services. Cogent Communications and Lumen Technologies, two major internet service providers (ISPs), have terminated their operations within the country, while companies like Microsoft have stopped their product sales. The sanctions and the exit of international IT and digital companies in the spring of 2022 sparked a significant exodus of Russian IT specialists. According to Park and Shin (2023), "The situation presents a significant challenge for Russia's future digital development and innovation landscape."

Despite the economic and infrastructural sanctions imposed upon it, the Russian internet has remained surprisingly resilient (Burkhardt and Wijermars 2022). This surprise deserves some explanation. As several chapters in this book have illustrated, the Russian internet has long been a pluralistic digital space, where international (Google, Apple, Microsoft, and Meta) and national (Yandex, VK, Sber, etc.) stakeholders coexisted. For several years now, this coexistence has been challenged by a policy of attempting to replace international players with national ones. This process of gradual so-called sovereignization of the Runet accelerated sharply with the war, which justified the banning of the main international platforms. Many international players have also chosen to leave the Russian market as a protest against the aggression in Ukraine—or have been compelled to do so following Western restrictions and sanctions against the Russian market. This reorganization of the Russian digital space has benefited Russian companies (Yandex, VK, Sber, etc.), which have gotten rid of any competition and now enjoy monopolistic access to the domestic market, at the price of the disappearance of political and civic freedoms. The war has strengthened the process of sovereignization, which was announced as of 2019 with the set of amendments dubbed "sovereign internet law" (see chapter 1). The national companies that provide the technical means for implementing this model of internet regulation are being permanently reinforced.

Another, more unusual explanation for the enduring capacity of the Russian internet to function is linked, ironically, to the ability of Russian players to circumvent barriers—including official or loyalist actors. For more than ten years, growing constraints on the Russian internet have encouraged the development of practical know-how to get around the blockages and digital obstacles that have stood in the way of internet users. Opponents of Putin's regime have become increasingly proficient at circumventing restrictions and evading surveillance. This book (chapter 4) documents the knowledge of activists who have learned how to route around digital obstacles by acquiring expert skills to circulate online, using various tools and adopting specific behaviors for protection. This knowledge, which is widespread among Russian digital users, can also be a resource for adapting to wartime constraints. The resilience of the Russian internet can be partially explained by the tricks players use to adapt to constraints, and this even includes official actors. For instance, banking sanctions (the end of the SWIFT protocol in Russia), which are jeopardizing the domestic digital market, are partially offset by the use of cryptocurrencies to continue buying and selling internationally. Similarly, copyright enforcement policies, which had been gradually implemented since the 2000s (see chapter 6), are being relaxed to facilitate the unrestricted circulation of cultural content. The arts of circumvention now also benefit the avoidance of sanctions and contribute to their relative ineffectiveness.

DIGITAL OCCUPATION VERSUS DIGITAL DEFENSE IN UKRAINE

Another major development is that the principles of digital authoritarianism documented in this book are currently being expanded to Ukraine. On the one hand, Russia is contributing to the physical destruction of the Ukrainian internet. Digital networks and electrical infrastructures are severely damaged by the bombings. The quality of the local internet has deteriorated, as evidenced, for example, by the increase in data exchange latency (Jain and al. 2022; Luconi and Vecchio 2023). On the other hand, the coercive rules

of the Russian internet now apply in the occupied territories, since 2014 in Crimea and since 2022 in the new occupied territories of the Donetsk, Luhansk, Mariupol, Kherson, Mykolaïv, and Zaporizhzhia regions. In these areas, the Russian state immediately instituted digital authoritarianism, with actors and infrastructures having to submit to the demands of the digital occupier. Regulatory bodies such as Roskomnadzor are opening subsidiaries in these regions to enforce Russian digital law. Players deemed to be excessively independent from the Russian state are banned from local digital landscapes: this includes American-based global services such as Facebook and Instagram, but also local Ukrainian media and online Ukrainian services. Internet service providers are controlled by Moscow, and their data are routed to Russia. According to Reporters Without Borders (RSF), "The Russian forces are colonizing the Ukrainian digital infrastructures and are installing their telecommunications companies in Southern Ukraine."[3] This annexation of the internet in southern Ukraine is depriving its citizens of access to freely reported news and information.

In contrast, Ukraine is fighting to preserve its online freedoms and defend itself from the digital authoritarianism pushed by Russia. The internet has become a vital resource for protecting the civilian population. Thanks to a public system of online alerts on mobile phones, citizens are warned of attacks so that they can take shelter. The Ukrainian government has invested heavily in modernizing its digital administration to facilitate administrative procedures for a population severely destabilized by war. Ukraine's Diia is a crucial element of the country's infrastructure that has enhanced Ukrainian society's ability to withstand the Russian invasion.[4] Digitalization of social services facilitates the protection of internally displaced people and refugees (Ihnatenko and Sadzaglishvili 2023). Russian aggression resulted in Diia actively strengthening its code against potential hacking by adopting policies that ensure user protection (Rashkovan 2023). Digital uses are also controlled so as not to endanger civilian populations and to avoid geolocating internet users in combat zones. Activist initiatives have also appeared online to promote encryption (Ermoshina and Musiani 2023). Finally, on the cybersecurity front, the rise of the IT army of Ukraine, which mobilized

from the hacker underground, illustrates how nonmilitary and volunteer initiatives can organize digital resistance (Smith and Dean 2023).

In Ukraine, global digital companies have chosen which digital services should be supplied for one party of the conflict and blocked for the other. Thanks to electrical generators that compensate for power failures, along with Starlink antennas that provide satellite internet, connection infrastructures are being valiantly maintained. Ukraine is the first country to move its critical and sensitive data under fire, shifting them to cloud services outside the country's borders with the significant help of global cloud solution providers. According to Aviv and Ferri (2023), for the first time in Ukraine, "Global tech companies assume the role of digital nations and superpowers while taking sides . . . thereby shaping paradigms regarding digital sovereignty as digital resilience."

EXPORTING DIGITAL AUTHORITARIANISM

Beyond Ukraine, digital authoritarianism *à la russe* can be characterized by its ambitions to export and establish itself in countries near and far (Morgus 2019). Many Russian players (entrepreneurs, media, suppliers) are trying to promote their authoritarian know-how in a wider context of Russian influence in European and non-European countries. The best-known case is the role of the Russian channels RT and Sputnik, as instruments of both "soft" and "sharp" power (Glazunova et al. 2023), which broadcast pro-Moscow content abroad (Gulenko 2024; Henriksen et al. 2024). But beyond these transnational media projects, Russian digital influence is also based on the circulation of technical tools, legal regulations, and algorithmic know-how.

The Russian authoritarian model is being exported to countries where political pluralism is under threat and where local control measures are already in place (Daucé et al. 2024). These dynamics are evident in certain ex-Soviet countries allied with Russia, such as Belarus, but they are also gaining ground in border states that are struggling to remove themselves from Moscow's influence, such as Georgia, where a law on foreign influence (inspired by the Russian law on "foreign agents") was adopted in 2024

against the will of the population and in the face of massive demonstrations. Similar developments are also visible on other continents, in countries where Russian influence is growing at the expense of democracy. In Iran, Syria, and Niger, dictatorships are being strengthened by more or less sophisticated digital controls. The success of the Russian breed of digital surveillance and censorship is based on its relatively low cost and adaptability to a wide range of contexts, whether it involves installing surveillance boxes at ISPs, tweaking online search and recommendation algorithms, or censoring content by keywords and blacklisting.

The world of liberal democracies is not immune to these attacks on digital freedoms. In many Western societies, there is widespread concern about Moscow's attempts to destabilize the digital field (as evidenced by the strategies of the RT news channel in Europe, for example, as well as the uncovering of large-scale networks of fake websites and social network accounts,[5] but also the intensifying waves of cyber-attacks in France, for instance[6]). In response, Western public authorities often deploy repertoires of sanctions that undermine the very principles they claim to defend and uphold against the Russian model. Reciprocal blockades are put in place, prohibiting access to the digital infrastructures and content of the opposing country. These reciprocal dynamics contribute to the political differentiation of contemporary internets, which are placed under different regimes of governance. From the US, European Union, Russia, or China, competing approaches to digital governance are emerging that challenge the original model of the "Silicon Valley open Internet" (O'Hara and Hall 2021). They raise questions about the possibility of a so-called splinternet that would fragment the global network (Mueller 2017; Perarnaud et al. 2022).

They also show the paradoxical circulation of repressive measures on a global scale. National and regional institutions are not only increasingly involved in regulating existing digital services and infrastructures, but also seek to promote specific norms and models for the digital environment. These digital differentiation processes are driven by different political conceptions. While the market and liberal paradigms have (at least until recently) dominated in the US, the patriotic and traditional conceptions are at the heart of digital policies in authoritarian countries. In the European Union, a model

of civic regulation is taking shape with legal provisions such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). This reflects a dynamic process of competition as well as imitation between different digital regimes that deserves closer attention in future research.

A COUNTERMODEL: THE RUSSIAN INTERNET IN EXILE

As a counterpoint, a digital Russia in exile is emerging, made up of political activists, workers in the digital sector (*itichniki*), independent journalists, and tens of thousands of exiled citizens who both feed and use resources and content of an alternative Runet abroad. Threatened in its own country (see chapters 7 and 8), this displaced community is trying to maintain a free, plural, and open internet, which connects its members and provides them with support in the face of the digital oppression that reigns in their country. The main independent media now banned in Russia have moved abroad after 2014 (Meduza) or after 2022 (Dozhd, *Novaya Gazeta*, The Insider, Proekt, Mediazona, etc.). New activist media have been relocated and developed by journalists in exile (Doxa, Kholod, Vërstka, etc.). All these journalists have created a rich and diversified media space, now free from Moscow's censorship. Russia's leading digital freedom activists, whether members of Alexei Navalny's Anti-Corruption Foundation (FBK), the Internet Protection Society (OZI), Roskomsvoboda, or Teplitsa, are now acting from their new host countries. For instance, the Internet Without Borders conferences and hackathons organized across Europe (Paris, Berlin, Prague, Warsaw, etc.) and former Soviet countries (Tbilisi, Vilnius, Yerevan, etc.) in 2022–2023 fostered an antiauthoritarian and antiwar agenda among the Russian tech community that has dispersed abroad.

From their exile, these multiple players are also developing new reflexivities to understand the fatal drift that has led to digital authoritarianism and war. Displaced against their will into new host societies, these exiles are participating in political debates about the Runet—its nature and its scope and how to reappropriate it. To the question "What do we have—digital sovereignty or digital dictatorship?," they answer without hesitation that it is the latter. Digital dictatorship involves new opportunities for dictators to

pursue their ultimate goal of retaining power, which is achieved by knowing about potential threats and grievances (gathering and analyzing information), manipulating beliefs (proregime propaganda, censorship, and discreditation), and influencing behavior (digital repression and co-optation) (Schlumberger et al. 2023). Contemporary Russia fits this model perfectly, with the added dimension of a new imperialism, based on the extension of its digital borders.

Finally, this authoritarian dynamic is accompanied by a deterioration in the quality of the Russian digital network, due to a transition to domestic and often lower-quality equipment, import substitution of services, as well as blocking of foreign applications, information sources, and VPNs. The authoritarian internet is not only a tightly controlled but also a degraded internet, which is gradually moving away from the most advanced international standards. Moreover, the partition of digital spaces is steadily altering the possibilities for exchange and communication between those who live inside and outside Russia. The issue of maintaining communication between them is now crucial. Digital autarky is threatening human relations and contributes to the brutalization of Russian society. Stopping the war and rebuilding a world of solidarity and peace will also involve paying close attention to how a virtuous digital environment can be set up and safeguarded.

Paris, September 1, 2024
The book coeditors

NOTES

1. https://antiwar.ovd.info/en
2. Dan Storyev, Daria Korolenko, and Laurent McCarthy, "The Hidden Strength of Russia's Anti-war Movement." Riddle, December 1, 2023, https://ridl.io/the-hidden-strength-of-russia-s-anti-war-movement/.
3. https://rsf.org/en/ukraine-s-colonisation-begins-its-internet
4. Mykhailo Fedorov, "Ukraine's Digital Revolution Is Proving Vital for the Country's War Effort," Atlantic Council, July 27, 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-is-proving-vital-for-the-countrys-war-effort/.
5. For example, operations nicknamed "Doppelgänger" or "Portal Kombat" uncovered since 2022 by the European NGO EU DisinfoLab (https://www.disinfo.eu/doppelganger/) and

the French agency in charge of identifying and documenting foreign influence operations online, VIGINUM (https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse).

6. See the 2023 threat report published by ANSSI, the French National Agency for the Security of Information Systems (https://cyber.gouv.fr/en/actualites/anssi-publishes-2023-cyber-threat-overview).

REFERENCES

Aviv, Itzhak, and Uri Ferri. 2023. "Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem." *International Journal of Critical Infrastructure Protection* 43. https://www.sciencedirect.com/science/article/abs/pii/S1874548223000501.

Burkhardt, Fabian, and Mariëlle Wijermars. 2022. "Digital Authoritarianism and Russia's War against Ukraine: How Sanctions-Induced Infrastructural Disruptions Are Reshaping Russia's Repressive Capacities." *SAIS Review of International Affairs* 42 (2): 21–43.

Daucé, Françoise, Ksenia Ermoshina, and Bella Ostromooukhova, eds. 2024. *Critiques et contournements du contrôle et de la surveillance sur Internet*. *TIC&Société* special issue. https://journals.openedition.org/ticetsociete/8532.

Ermoshina, Ksenia, and Francesca Musiani. 2023. "Encryption as a Battleground in Ukraine." In *Eaten by the Internet*, edited by Corinne Cath. Meatspace Press.

Glazunova, Sofya, Axel Bruns, Edward Hurcombe, Silvia Ximena Montaña-Niño, Souleymane Coulibaly, and Abdul Karim Obeid. 2023. "Soft Power, Sharp Power? Exploring RT's Dual Role in Russia's Diplomatic Toolkit." *Information, Communication and Society* 26 (16): 3292–3317.

Gulenko, Petr. 2024. "RT (Russia Today) from Soft Power to the Weaponization of Information." In *The Palgrave Handbook of Non-State Actors in East-West Relations*. Springer International.

Henriksen, Frederik Møller, Jakob Bæk Kristensen, and Eva Mayerhöffer. 2024. "Dissemination of RT and Sputnik Content in European Digital Alternative News Environments: Mapping the Influence of Russian State-Backed Media across Platforms, Topics, and Ideology." *International Journal of Press/Politics* 29 (3): 795–818.

Ihnatenko, Kateryna, and Shorena Sadzaglishvili. 2023. "The Digitalization of Social Services in Response to the War in Ukraine." *Social Work and Education* 10 (3). https://journals.uran.ua/swe/article/view/286626.

Jain, Akshath et al. 2022. "The Ukrainian Internet under Attack: An NDT Perspective." In *Proceedings of the 22nd ACM Internet Measurement Conference, edited by Chadi Barakat and Cristel Pelsser. Association for Computing Machinery*.

Luconi, Valerio, and Alessio Vecchio. 2023. "Impact of the First Months of War on Routing and Latency in Ukraine." *Computer Networks* 224. https://www.sciencedirect.com/science/article/pii/S1389128623000415.

Morgus, Robert. 2019. "The Spread of Russia's Digital Authoritarianism." In *AI, China, Russia, and the Global Order. Technological, Political, Global, and Creative Perspectives*, edited by Nicholas D. Wright. US Department of Defense.

Mueller, Milton. 2017. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. John Wiley and Sons.

O'Hara, Kieron, and Wendy Hall. 2021. *Four Internets. Data, Geopolitics, and the Governance of Cyberspace*. Oxford University Press.

Park, Jiyoun, and Boram Shin. 2023. "Conceptualizing Digital Sanctions as a New Type of Economic Sanctions in the Digital Era: Digital-Related Sanctions Measures against Russia and Their Consequences." *Journal of Eurasian Studies*. https://journals.sagepub.com/doi/10.1177/18793665231217303.

Perarnaud, Clément, Julien Rossi, Francesca Musiani, and Lucien Castex. 2022. "'Splinternets': Addressing the Renewed Debate on Internet Fragmentation." Report commissioned and published by the Panel for the Future of Science and Technology (STOA) of the European Parliament. Released July 11, 2022. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729530.

Rashkovan, Sonya. 2023. "Shaping Digital Government: Ukraine During the War." *Brown Political Review*, December 23. https://brownpoliticalreview.org/shaping-digital-government/.

Schlumberger, Oliver, Mirjam Edel, Ahmed Maati, and Koray Saglam. 2023. "How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship." *Government and Opposition* 59 (3): 761–783.

Smith, Margaret W., and Thomas Dean. 2023. "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict." In *Proceedings of the 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*. IEEE.

Russian-to-English Transliteration Table

Cyrillic	In the main text	In footnotes, glossary and references
Г, г	g	g
Е, е	e	e
Ё, ё	ë	ë
Ж, ж	zh	ž
И, и	i	i
Й, й	y	j
Х, х	kh	h
Ц, ц	ts	c
Ч, ч	ch	č
Ш, ш	sh	š
Щ, щ	shch	ŝ
Ъ, ъ	’	’
Ы, ы	y	y
Ь, ь	’	’
Э, э	è	è
Ю, ю	iu	û
Я, я	ia	â

List of Abbreviations

IN ENGLISH

BGP	Border Gateway Protocol
DNS	Domain Name System
DPI	Deep Packet Inspection
ECHR	European Court of Human Rights
GAFAM/ MAGMA	Google, Apple, Facebook, Amazon, Microsoft; then Meta, Apple, Google, Microsoft, Amazon (since 2022)
IP	Internet Protocol
ISP	Internet Service Provider
IXP	Internet Exchange Point
OONI	Open Observatory of Network Interference
OSINT	Open Source Intelligence
TOR	The Onion Router
VPN	Virtual Private Network

IN RUSSIAN

FAS	*Feministskoie antivoennoe soprotivlenie* (Feminist Resistance against War)
FBK	*Fond bor'by s korrupciej* (Anti-Corruption Foundation, founded by Aleksei Navalny)
FSB	*Federal'naâ služba bezopasnosti Rossijskoj Federacii* (Federal Security Service)
FZ	*Federal'nij zakon* (Federal law)
Gosuslugi	*Gosudarstvennye uslugy* (Public services)
MVD	*Ministerstvo vnutrennih del* (Ministry of Interior Affairs)
OZI	*Obŝestvo Zaŝiti Interneta* (Internet Protection Society)
RAEK	*Rossijskaâ associâciâ èlektronnyh kommunikacij* (Russian Association of Electronic Communications)
Revizor	System checking ISP compliance for blocking banned websites

RKN	*Roskomnadzor* (Federal Service for Supervision of Communications, Information Technology and Mass Media)
Rosreestr	*Federal'naâ služba gosudarstvennoj registracii, kadastra i kartografii* (Federal Service for State Registration, Cadastre and Cartography)
SORM	*Sistema operativno-razysknyh meropriiatij* (System for Operative Investigative Activities)
TSPU	*Tehničeskie sredstva protivodejsviia ugrozam* (Technical Means for Countering Threats)

Contributors

THE EDITORS

Françoise Daucé is a full professor at the School for Advanced Studies in the Social Sciences (EHESS), Paris, and former director of the Center for Russian, Caucasian, East-European and Central Asian Studies (CERCEC).

Benjamin Loveluck is a junior professor in political science, chair in digital regulation at Paris-Pantheon-Assas University.

Francesca Musiani is a research professor at the French National Center for Scientific Research (CNRS) and director of its Centre for Internet and Society (CIS).

THE CONTRIBUTORS

Olga Bronnikova is an associate professor at Bordeaux-Montaigne University and member of Plurielles—Langues, Littératures, Civilisations.

Ksenia Ermoshina is an associate research professor at CNRS and member of CIS.

Valéry Kossov is an associate professor at Grenoble-Alpes University and member of the Institute of Languages and Cultures of Europe, America, Africa, Asia and Australia (ILCEA4).

Bella Ostromooukhova is an associate professor at Sorbonne University and member of the research unit Eur'ORBEM (focus on Eastern, Balkan and Central Europe).

Perrine Poupin is an associate research professor at CNRS and member of the Research Centre on Sound Space and the Urban Environment (CRESSON).

Anna Zaytseva is an associate professor at University Toulouse II Jean Jaurès and member of the research unit Letters, Languages and Arts—Creation, Research, Emergence in Arts, Texts, Images, Shows (LLA CREATIS).

Index

INFORMATION POLICY SERIES

Edited by Sandra Braman

Virtual Economies: Design and Analysis, Vili Lehdonvirta and Edward Castronova

Traversing Digital Babel: Information, e-Government, and Exchange, Alon Peled

Chasing the Tape: Information Law and Policy in Capital Markets, Onnig H. Dombalagian

Regulating the Cloud: Policy for Computing Infrastructure, edited by Christopher S. Yoo and Jean-François Blanchette

Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Kenneth A. Bamberger and Deirdre K. Mulligan

How Not to Network a Nation: The Uneasy History of the Soviet Internet, Benjamin Peters

Hate Spin: The Manufacture of Religious Offense and Its Threat to Democracy, Cherian George

Big Data Is Not a Monolith, edited by Cassidy R. Sugimoto, Hamid R. Ekbia, and Michael Mattioli

Decoding the Social World: Data Science and the Unintended Consequences of Communication, Sandra González-Bailón

Open Space: The Global Effort for Open Access to Environmental Satellite Data, Mariel John Borowitz

You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches, Josephine Wolff

The Blockchain and the New Architecture of Trust, Kevin Werbach

Digital Lifeline? ICTs for Refugees and Displaced Persons, edited by Carleen F. Maitland

Designing an Internet, David D. Clark

Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century, Rita Zajácz

Human Rights in the Age of Platforms, edited by Rikke Frank Jørgensen

The Paradoxes of Network Neutralities, Russell Newman

Zoning China: Online Video, Popular Culture, and the State, Luzhou Li

Design Justice: Community-Led Practices to Build the World We Need, Sasha Costanza-Chock

Fake News: Understanding Media and Misinformation in the Digital Age, edited by Melissa Zimdars and Kembrew McLleod

Researching Internet Governance: Methods, Frameworks, Futures, edited by Laura DeNardis, Derrick L. Cogburn, Nanette S. Levinson, and Francesca Musiani

Red Lines: Cartoons and Political Censorship, Cherian George and Sonny Liew

Seeing Human Rights: Video Activism as a Proxy Profession, Sandra Ristovska

Farm Fresh Broadband: The Politics of Rural Connectivity, Christopher Ali

Cyberinsurance Policy: Rethinking Risk for the Internet Age, Josephine Wolff

Resistance to the Current: The Dialectics of Hacking, Johan Söderberg and Maxigas

Universal Access and Its Asymmetries: The Untold Story of the Last 200 Years, Harmeet Sawhney and Hamid R. Ekbia

The Power of Partnership in Open Government? Reconsidering Multistakeholder Governance Reform, Suzanne J. Piotroswki, Daniel Berliner, and Alex Ingrams

Managing Meaning in Ukraine: Information, Communication, and Narration since the Euromaidan Revolution, Göran Bolin and Per Ståhlberg

The Character of Consent: The History of Cookies and the Future of Technology Policy, Meg Leta Jones

Science Competes: Informing Policy in a Time of Distrust, Fracture, and Chaos, Barry Bozeman

Declaring Independence in Cyberspace: Internet Self-Governance and the End of U.S. Control of ICANN, Milton L. Mueller

Content Confusion: News Media, Native Advertising, and Policy in an Era of Disinformation, Michelle A. Amazeen

Digital Authoritarianism in the Making: Repression and Resistance on the Russian Internet, edited by Françoise Daucé, Benjamin Loveluck, and Francesca Musiani