(Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia

Rashid Gabdulhakov

Submit your article to this journal ⤤

View related articles ⤤

View Crossmark data ⤤

Routledge
Taylor & Francis Group

ARTICLE

(Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia

Rashid Gabdulhakov

Department of Media and Communication, Erasmus University Rotterdam, the Netherlands

ABSTRACT

This article applies Haggerty and Ericson's *surveillant assemblage* concept to the recent wave of social media user arrests in Russia. In doing so, it addresses the legislative frameworks applied to online self-expression, depicts the nuances of legal charges pressed against select social media users, assesses the role of formal law enforcement and vigilant citizens recruited to extend the state's watchful gaze, and elaborates on citizen counter-forces resisting the tightening state control over the digital domain. The article argues that Russia's internet users appear to be *trolled* by the ruling elite through the use of obscure legal frameworks and the stampede of actors and practices where select individuals face legal charges for their activities on social media, while other users face no consequences for the same engagements. Such unpredictability stimulates self-censorship, making the system effective by virtue of its dysfunctionality. Methodologically, the study relies on desk research and field interviews.

KEYWORDS
Internet governance; Russia; social media; surveillant assemblage; vigilantism

For my friends, everything; for my enemies, the law.[1]

1. Introduction

In November 2016, a regional coordinator of Open Russia Foundation[2] in Chuvashia, Dmitry Semenov faced administrative charges for posts on his VKontakte page (Russia's analogue of Facebook). The posts exposed Russia's parliament member wearing a shirt with a sign 'Orthodoxy or death', and were qualified by law enforcement as an offence for 'production and distribution of extremist materials'.[3] While the police did not go after the politician being the source of such 'materials', Semenov faced charges and was fined.[4] This is one out of hundreds of similarly preposterous cases that rambled across Russia following waves of amendments to the criminal code. The 2014 amendments incorporated online speech into offences governed by anti-extremism laws; the 2016 *Yarovaya law package* intensified punishment for such offences[5]; and 2019 'anti-fake news' legislation made it illegal for citizens to express disrespect at those with political power. As the

---

definitions of 'extremism'[6] and 'disrespect' remain open to interpretation, a mere 'like' on social media can lead to criminal charges, sentences and fines, making all internet users in Russia potentially vulnerable to legal repercussions. Indeed, over several years there has been a steady increase in extremism charges in Russia, with most of the cases concerning online speech.[7]

The study identifies legal frameworks and investigates formal and informal forces serving the state in web control; while also elaborating on citizen counter-forces opposing these control measures. Among state actors are 'Centre E' – Russia's extremism-countering police[8] – involved in heavy monitoring of the digital domain.[9] In 2011, the state has established the Safe Internet League[10] and recruited citizen Cyber Guards[11] to monitor, identify and report on dangerous online content. Other pro-state vigilante formations include *Je Suis Maidan* [I am Maidan][12] and SILOVIKI [Security officers][13] who engage in what Lovelock classifies as 'hounding'[14] by exposing protestors, opposition leaders and activists and calling on the followers to retaliate on these targets.

Counter-forces to the state include the civil analytics project *Database*, which specialises in exposing the snitches[15] and 'those responsible for human rights violations and corruption in Russia'[16]; the *Internet Protection Society*, opposing censorship, excessive regulation, and administrative arbitrariness in internet governance[17]; and *Roskomsvoboda*, a public organisation 'countering Internet censorship and promoting the ideas of freedom of information and self-regulation of the Internet industry'.[18] While the analysis of select user arrests seeks to identify themes in 'offences' that cost users their freedom, mapping the actors and forces allows for an informed analysis of their capacities, inter-relations, and the clashing interests in regulation of online self-expression.

The article relies on Haggerty and Ericson's concept of the 'surveillant assemblage' – a compendium of surveillance practices where extra state institutions, machines, flows, and other components come together in rhizomatic practices that level surveillance hierarchies.[19] The concept is applied to the case of Russia, where the ruling elite's quest for securing control over online self-expression has led to the adaptation of strategic regulatory and punitive practices targeting users. A variety of methods and actors are instrumentalised by the state in this endeavour.

While current literature on surveillance addresses an array of issues related to Internet governance,[20] platforms,[21] authoritarian states,[22] and surveillance in post-communist societies,[23] the case of Russia requires further scholarly attention as the country represents a peculiar case of selectivity in the application of restrictive legislation. Strategic legislation adapted by the Kremlin faces challenges in implementation when actors struggle to serve-up to the state amid the vagueness of legal definitions. As a result, Russia's digital domain and social media users appear to be *trolled*[24] by the ruling elite through the use of obscure legal frameworks and the stampede of actors and practices where select individuals face legal charges for their activities on social media, while other users face no consequences for the same engagements.

The article first elaborates on the methods and proceeds to introduce theoretical frameworks operationalised to address the Kremlin's attempts to discipline social media users. After unpacking Russia's surveillant assemblage and discussing its past-oriented governance measures, the article proposes and addresses three pillars for understanding current practices of online self-expression control in the country – (1) legal frameworks; (2)

targeted individuals/online speech; and (3) state-loyal vigilantes/citizen counter-forces. The discussion of key findings is followed by a conclusion.

2. Methods

This article utilises several methodological approaches, including desk research and field interviews. Desk research focused on strategic legislation and criminal cases instigated against social media users. Semi-structured in-depth interviews were conducted with a diverse set of informants, including lawyers working on internet-related cases, rights defenders, academics working on issues of internet freedom and online activism in Russia, representatives of NGOs, and law enforcement authorities. Interviewees were selected based on their expertise in the domain of Russia's internet governance and were recruited with the aim of representation of various clusters of actors. The informants were asked questions concerning online activism, vigilantism, and internet governance in the country. Interviews were conducted in 2018 and 2019 in-person and via online messengers. The author transcribed and translated content from Russian into English.

To protect the privacy and safety of the informants, their names will not be disclosed in this article. Instead, a reference to the general position of informants will be made, i.e. 'academic', 'lawyer', 'rights defender', 'police officer', etc. Such anonymisation has no impact on the data and its quality. Legal cases addressed in the scope of this work are public, thus will not be anonymised. Annexe 1 provides a list of interviewees along with information on the location, date and type of interview. Interview materials are used throughout the text of the paper in the form of short and extended quotations, providing expert and insider views and knowledge on given cases, notions, or practices.

3. Theoretical background

Surveillance studies gained momentum in the second half of the twentieth century due to an increase in the 'number and type of surveillance technologies'.[25] Building on Jeremy Bentham's panoptic architectural design, Michel Foucault proposed the idea of a 'discipline society' in which an individual is not only watched but is 'carefully fabricated'.[26] Taking the analogy of prisoners and the all-seeing yet discrete guard, Foucault applies power structures and hierarchies to society beyond the prison cell in 'the relations of discipline'.[27] For several decades, Foucault's *panopticism* dominated scholarship as the primary and canonical foundation in the conceptualisation of surveillance practices.[28] Yet, with technological advances, surveillance capacities and approaches have transformed vastly since the 1970s, leading to the search for new theories and analogies.

Having proposed not to stretch *panopticism* too far in trying to apply it to contemporary post-disciplinary-confinement surveillance practices, Haggerty and Ericson build upon Deleuze and Guattari's ideas of 'a convergence of what were once discrete surveillance systems' in the societal shift from discipline to control[29] and propose the concept of the *surveillant assemblage*.[30] The authors describe the assemblage as a sphere where there is a 'desire to bring systems together',[31] meaning that all separate clusters, institutions, mechanisms, machines, and so on are coming together in an all-seeing and all-tracing entity. Thus, being comprised of various mechanisms, *modus operandi* of the assemblage

is no longer solely state-centric as it tends to incorporate 'extra-state institutions'.[32] As such, Haggerty and Ericson argue that surveillance is no longer carried out in a purely top-down approach of Orwellian 'Big-Brother', but rhizomatic practices allow for bottom-up scrutiny of *the powerful* by the wider masses and by institutions through levelling of surveillance hierarchies, thus bringing new groups which were 'previously exempt from surveillance' under the watchful gaze.[33] Escaping the gaze of the assemblage is a nearly impossible task, because the conglomerate of mechanisms, measures, and practices of control breeds the phenomenon of 'disappearance of disappearance',[34] as social institutions are increasingly armed with far-reaching surveillance apparatuses.

In 'Postscript on the Societies of Control' Deleuze proposes to replace an 'individual' that was relevant to the Foucauldian 'discipline society' with the concept of 'dividual'[35] as surveillance is no longer body-centric. Haggerty and Ericson further develop the idea that not only has surveillance moved beyond state institutions and towards a multi-actor assemblage, but it has also moved beyond the physical body and towards 'a decorporealized body, a 'data double' of pure virtuality'.[36] (In)dividuals, leave a constant digital trace by virtue of continuous scanning and storing of interactions, purchases, movements, expressions, habits, searches etc., etc.

While such turns in surveillance affordances certainly affect all social strata, *online vulnerabilities*[37] can be directly linked to offline fragile statuses of persons in question. For instance, building his arguments on the example of intensified welfare monitoring in Canada, Sean Hier demonstrates how by means of the surveillant assemblage social institutions intrude into the lives of already disadvantaged people with prejudicial evaluations and populist underpinnings.[38] In this regard, in the words of Virginia Eubanks, inequality is 'automated' in the system that puts 'the poor' and disadvantaged people into further conditions of fragility.[39]

Over the years, the scholarly thought surrounding surveillance has moved beyond the Foucauldian panopticism and proposes the idea of an *assemblage* where amid the near-impossibility to avoid the gaze due to the rhizomatic nature of its [the assemblage's] components, anyone can watch anyone. Here, of course, it is important to consider various capacities and power asymmetries[40] of actors involved. Beyond the departure from institutions and top-down surveillance, there is a departure from viewing the physical body as a sole subject amid digital traces that make up the digital twins of (in) dividuals. 'Sub-assemblages' are comprised of groups, systems, and counter-forces. Per Haggarty and Ericson, these assemblages are 'themselves multiple', consisting of 'different discrete assemblages'[41] each having own agenda, ambitions, and approaches.

4. Unpacking Russia's surveillant assemblage: towards the 'digital iron curtain'?

Having secured control over traditional media,[42] Russia's ruling regime entered a battle with content shared on social media 'to consolidate an information dominance over citizens'.[43] The online sphere imposes several perceived threats on regime stability in Moscow, including counter-narratives to official propaganda,[44] dissent, activist resistance practices,[45] and coordination of potential revolutionary forces.[46] At the same time, digital media is not solely a challenge but is also an opportunity for the ruling elite; as is argued by Oates, it provides a set of 'particular advantages to a repressive regime that can pro-

actively shape the media narrative'.[47] Beyond the direct control over broadcasters through ownership, and indirect control over domestic social media secured through the loyalty of platform owners, Russia's political elite does not tolerate competition when it comes to strategic discourse. As Oates puts it, 'it is not so much about who owns or controls the media, it is more about who is constructing and disseminating the most compelling national narrative ... '[48] While traditional media adapts its pitching tactics, amid new challenges imposed by the online sphere the regime finds itself in need of taking further actions to protect its monopoly on the digitally-dispersed information.

Current actions and practices of control applied to the digital domain resemble an echo from Russia's Soviet past. The concept of 'post-communism' implies the state of 'in-betweenness', where past legacies and 'poor institutional performance and leadership' are preventing positive transformation in certain pollical contexts.[49] During the period of transition, which in itself does not bond to any specific time frame, the regime, while certainly adapting to new realities with new strategies, may, nevertheless, turn to familiar past practices such as censorship, showcase arrests, adaptation of punitive legislation, and recruitment of vigilant citizens.

Selective social media user arrests are a by-product of Russia's surveillant assemblage which is programmed to secure state-approved narratives at any cost and is aided by strategic legislation. While appearing to be inspired by China's firewall, Russia's approaches and capacities are different. As a Moscow-based rights defender explained:

> Russia does not have the required resources to build a firewall, nor does it put such a task for itself. Russia's regulatory framework grounds itself on the idea of a broad definition of restrictions with their selective consequent application ... It is quite obvious, as a thousand people can make the same post, and only one will suffer the consequences.[50]

Therefore, Russia's throwback to authoritarianism is accompanied by opaque conditions for understanding what is allowed and what is not in online self-expression. This lack of clarity influences the assemblage by making its function subjective and flexible in the hands of multiple sub-assemblages.

The term 'Digital Iron Curtain' that appears in the title of this subsection is intended to illustrate this past-oriented motion in the Kremlin's attempt to control the internet, referring to the Soviet Iron Curtain which worked towards isolation of the Soviet people from contact with the 'evil West'. In Russia, the internet is framed by the regime as a 'CIA tool'[51] – something that threatens national security and endangers users. Furthermore, the Kremlin is taking steps towards potential isolation of Russia's internet users from the world wide web by making the country's internet 'sovereign'.[52] The state justifies these measures as an intent to make the internet more stable and immune to external attacks. Yet, rights defenders and activists are concerned that 'sovereign internet' law would give the state more opportunities for control and would jeopardise internet freedom even further.[53]

5. Legal frameworks applied to social media

The web of forces comprising Russia's surveillant assemblage certainly includes legislative frameworks targeting social media users. In the majority of cases, criminal code articles

dealing with terrorism, extremism and xenophobia are applied to social media activity. 'Nearly every day in 2017 and first half of 2018' criminal charges were being pressed against users over 'likes', posts, and other social media engagements.[54] As such, in 2017, 460 social media users were charged under Article 282 Part 1[55]:

> Actions aimed at the incitement of hatred or enmity, as well as abasement of dignity of a person or a group of persons on the basis of sex, race, nationality, language, origin, attitude to religion, as well as affiliation to any social group, if these acts have been committed in public or with the use of mass media … [56]

Other users faced charges under Article 280 'public appeals for the performance of extremist activity' and Article 205 'act of terrorism'.[57]

User arrests based on Article 148 of the Criminal Code 'incitement of hatred and insult to the religious feelings of believers' take root in the "offence" committed by a protest punk rock band Pussy Riot. In 2012, three band members performed a 'punk prayer' in which they 'danced around and shouted their song, "Virgin Mary, Get Putin Out"'.[58] In their act, Pussy Riot simultaneously encroached on two untouchables in Russia – the Russian Orthodox Church and the president. Criminal code Article 213 – hooliganism was applied and all three members were sentenced to two years in the penal colony.[59] This incident was followed by amendments to Article 148 of the criminal code of the Russian Federation in 2013 'in the aim of protecting religious convictions and feelings'.[60]

In addition to Article 148, amendments were introduced to other criminal code articles, including the above-mentioned Article 282, and Article 205[61] that concerns terrorism and public security, defining the former as:

> … the perpetration of an explosion, arson, or any other action endangering the lives of people, causing sizable property damage, or entailing other socially dangerous consequences, if these actions have been committed for the purpose of violating public security, frightening the population, or exerting influence on decision-making by governmental bodies, and also the threat of committing said actions for the same ends …

When applied to the social media sphere, charges under Article 205 can be pressed for 'reposting of blogs or other online messages',[62] creating uncertainty and confusion as 'likes' and 'shares' on social media can be interpreted as an endorsement of terrorism.

A Moscow-based lawyer working on social media-related cases described these amendments as 'reactionary'; 'any new event leads to the development of new articles and amendments to the criminal code'.[63] The lawyer further explained that after the amendments that expanded its scope and made it applicable to online activity, Article 205 is increasingly applied to social media cases. 'First, 282, and now a trendy one is Article 205 – terrorism. Terrorism implies long sentences. Terrorism is a trendy article'.[64] While the scope of Criminal Code articles widens, and punishment for offences gets harsher, the 'officials' can 'interpret a wide range of government opposition as "extreme"'.[65] Even civil servants are interpreted to be a 'separate social group',[66] and criticisms of this group on social media can cost users their freedom.

In March 2019, President Vladimir Putin signed the law on 'fake news' and 'disrespect' of the government, making it a crime to 'insult' the authorities.[67] A month later, the law was used against an internet user[68] over a social media post referring to Russia's president

in an obscene manner. Focus on the nature of offences in social media user arrests will further illuminate the themes that get users into trouble in Russia.

6. Targeted individuals and online speech

There is an intricate approach to reporting on litigation against social media users. On the one hand, media reports are an important tool in showcasing the type of activities that are not welcomed by the regime, thus disciplining others by letting them know about the consequences. On the other hand, an abundance of reports may portray the regime as overly repressive. Not all cases of social media user arrests are reported on in the media or otherwise made public. Internet Protection Society (IPS) NGO maintains a database of cases concerning online speech across the country. IPS compiled a map of criminal and administrative charges, staring with 2015.[69] As of 21 October 2019, the database contained 990 cases coming predominantly from the archives of a Moscow-based NGO SOVA. While IPS' map desegregates cases by regions of the Russian Federation, by dates, and by platforms,[70] it does not provide a thematic categorisation. The author seeks to expand the understanding of the types of targeted speech and individuals through own analysis of the categories of charges. This classification should be regarded as a flexible structure, subject to expansion upon newly emerging cases.

Among the recurring themes in online speech that cost users their freedom, this study identifies xenophobia (including Nazism and anti-Semitism); calls for unsanctioned protests; faith and lack thereof; challenging state authority (ruling elite, police, judges); and Russia-Ukraine conflict. This section of the article will provide several snapshots from the pool of cases, to illustrate the abovementioned classification.

6.1. Xenophobia

Most cases of litigation against social media users concern xenophobia. The details of posts and activities that lead to charges, arrests and fines are not always provided by the police or mass media. As per pressed charges, this category of offences includes anti-Semitism, fascism, nationalism, Nazism, racism, ultra-right views, etc. Some cases concerned xenophobia targeting people from Central Asia and the Caucasus; other cases, on the contrary, implied targeting ethnic Russians.

Following a period of tolerance towards neo-Nazi and far-right formations, Russia's domestic security apparatus cracked down on both in the last few years.[71] Amid the cultural and political significance of Soviet victory in WWII, display of any Nazi attributes is considered to be an extremist act. As such, the situation with social media posts of Nazi symbols at times reaches absurd levels as users have faced the law over posts in which they condemn fascism.[72] Moreover, posts about Soviet victory in WWII, displaying the surrender of Nazi soldiers in 1945 have also attracted the attention of the state.[73] Due to the vague definition of *extreme* speech, practically anyone can be arrested for virtually anything in Russia. A photo from a museum, or historical textbook, a research-related survey,[74] or a screenshot from a movie or TV programme can get a person arrested or fined, while the source of the content would suffer no consequences.[75]

6.2. Calls for unsanctioned protests

Several cases of litigation over online activity involved 'calls for unsanctioned protests'. Here, the assemblage reacts to the expected targets such as the opposition leaders and activists,[76] as well as random internet users. One of such examples concerns a student in Saint Petersburg, Oksana Borisova, who shared a post about an unsanctioned protest to be taking place in another city – Mineralnye Vody – on her VKontakte page. The next morning police came after her to the university. Up to six officers were flown in from another region to capture Borisova, who was found guilty and served one day of administrative arrest.[77]

6.3. Faith and lack thereof

Another recurring theme for charges pressed against social media users is centred around faith and atheism. Convicts are usually charged on the basis of a conjunction of several criminal code articles. Article 148 'incitement of hatred and insult to the religious feelings of believers' along with Article 282 'Incitement of hatred or enmity, as well as abasement of human dignity' and later Article 138 'violation of the secrecy of correspondence, telephone conversations, postal, telegraphic and other messages' were used to press criminal charges and convict a 22-year old blogger Ruslan Sokolovsky to 3.5 years of suspended sentence (reduced to 2.3 years of a suspended sentence upon appeal)[78] for playing *Pokémon Go* inside of a church.[79] Evidence was produced by Sokolovsky himself as he posted his prank video on YouTube, catching Pokémon inside of the Russian Orthodox Church of All Saints in Yekaterinburg.[80] Commenting on the case, Sokolovsky's lawyer stated that such a harsh response is intended to '"frighten and intimidate" bloggers and other internet users in Russia and to prevent them from speaking freely online'.[81] Sokolovsky's name currently appears among extremists and terrorists listed on the website of the Federal Financial Monitoring Service of the Russian Federation.[82]

In another case of incitement of hatred and insult to the religious feelings of believers, atheist Viktor Krasnov faced charges for denying God's existence on VKontakte social network.[83] Charges against Krasnov were eventually dropped, but his lawyer believes that those who initiated the case 'were used by law enforcement to "complete a plan" to produce a certain number of convictions'.[84] This practice of 'plan fulfilment' implies that law enforcement authorities are assigned a quota for a certain number of cases on different offences, and 'they have to find lawbreakers, even if the latter do not exist'.[85]

In the Siberian city of Barnaul, 23-year-old Maria Motuznaya faced charges on extremism and incitement of hatred and insult to the religious feelings of believers under Articles 282 and 148 of the criminal code of the Russian Federation.[86] Combined charges could have costed Motuznaya up to 6 years of freedom for the memes she posted in a private album on her page on VKontakte social network.[87] Motuznaya appeared among extremists and terrorists listed on the website of the Federal Financial Monitoring Service,[88] and decided to leave Russia in 2018. The case against her was discontinued in 2019.

Other cases varied thematically and included posts allegedly targeting Christians, Muslims, non-Christians, non-Muslims, etc. Given that Jehovah's Witnesses are deemed extremist in Russia since 2017,[89] several charges targeted related content.

6.4. Challenging state authority

Even before the law on 'fake news' and 'disrespect of authority', posts about civil servants, including the president, could lead to arrests. In 2018, Vladimir Egorov of Tver was convicted to 'a two-year suspended sentence and three years of probation'[90] for his post on VKontakte social network where he referred to President Putin as 'the main rat in the Kremlin'.[91] Egorov currently appears among extremists and terrorists listed on the website of the Federal Financial Monitoring Service.[92]

In March 2018, 10 people faced charges on extremism under Article 282 for establishing an 'extremist' organisation called *Novoe Velichie* [The New Greatness],[93] through the use of social media. Two of the arrested are teenagers.[94] The case received wide media coverage and resulted in numerous protests known as Mothers' March.[95] The case of Novoe Velichie is surrounded with controversies and is believed to be an entrapment organised by law enforcement – ' … they developed all official documentation themselves and they rented an office for this organisation and they themselves turned this organisation in!'[96]

6.5. Russia-Ukraine conflict

Russia-Ukraine conflict and annexation of Crimea were recurring themes in internet-related charges and arrests. In 2015, VKontakte user Andrey Bubeyev faced charges under Article 282 for sharing a video, which referred to Russia as a 'fascist aggressor'[97] in the context of the conflict in Ukraine. Convicted to 10 months and while in custody, Bubeyev faced new charges under Article 280 part 1 for a different post on VKontakte, stating that 'Crimea is Ukraine',[98] which was interpreted as a threat to Russia's territorial integrity.[99] Bubeyev currently appears among extremists and terrorists listed on the website of the Federal Financial Monitoring Service of the Russian Federation.[100] Among several internet users who faced litigation over shared music is Roman Grishin of Kaluga, charged under Article 282 part 1. On his VKontakte page,[101] Grishin shared a video clip to a song by Boris Sevastyanov 'New hit from Kharkiv: This, baby, is Rushism,' which questions and criticises Russia's presence in Ukraine.[102]

What can be concluded about targeted individuals and online speech is the fact that cases include both people who are already under the radar as well as random social media users. There is a certain geographical context in the nature of police reactions to online activity. As an academic in St. Petersburg explained:

> The application of anti-terrorism legislation is geographically subjective. What is possible in Moscow and St. Petersburg can cost users their freedom in, say, Tumen. It is not just about the laws, it is about the implementation practices.[103]

A representative of a public opinion NGO in Moscow confirms this idea of differentiation between Russia's two major cities and the rest of the country, and emphasises the lack of clarity in the interpretation and implementation of legislation:

> People who get in trouble for their posts are selected based on their activism. Sometimes there are random arrests, of course. Many cases come from Russia's regions and not from Moscow. Perhaps, people in Moscow are more cautious or more informed. In general, what is allowed and what is not allowed is not clear. It really is a gamble.[104]

In general, litigation concerned thematically polar topics and could target users for homophobia[105] and gay propaganda;[106] hate towards women[107] and radical feminism-[108] at the same time. Although partial decriminalisation of Article 282[109] at the dawn of 2018 lead to suspension of several cases, the system is functioning in such a way that potentially any social media activity can lead to charges and sentences, if necessary.

7. Sub-assemblages: authorised law enforcement and pro-state vigilantes

To proceed further in the pursuit of unpacking approaches to social media control, we must address forces and sub-groups in the assemblage. One of such sub-assemblages is the Chief Directorate of the Ministry of Internal Affairs of the Russian Federation for Combating Extremism, also known as 'Centre E'. Established in 2008, the Centre constitutes an independent unit within police forces and its mandate includes 'development and implementation of state policy and legal regulation, as well as enforcement powers in the field of countering extremist activities and terrorism'.[110] 'Centre E' is the main law enforcement body responsible for monitoring and reacting to extremism expressed online. In an interview to Meduza – a Latvia based online newspaper and aggregator of manually selected news, texts and podcasts in Russian and English languages – the Centre's former agent explained that while some of the units 'fight the true evil of our time'; in principle, people are charged with extremism through two approaches; the first one involves high profile 'public figures who get charged after the government machine decides to "take them out"'; while the second category is a product of the so-called 'stick system' – police quotas for the number of crimes reported in a given area.[111] These revelations are illustrative of both the power in the hands of the ruling elite and its sub-assemblages, and the danger of the system where police are assigned a quota.

In terms of collaboration between vigilant citizens and police, there is an intriguing link. As Daucé, Loveluck, Ostromooukhova, and Zaytseva explain it, in 'the coexistence of several online citizen surveillance models', including 'expert investigators' (internet companies and security specialists) and 'political cyber patrols' (state-loyal vigilantes) there is a competition-driven tension.[112] At the same time, the evolving legislation is establishing a stage for 'mutual vigilance between law-enforcement agencies and online surveillance volunteers'.[113]

Areas of the intersection of sub-assemblages are not necessarily perceived as highly productive by either party. As one law enforcement officer put it, 'at the end of the day, they [vigilantes] still turn to the state, but instead of helping the state they just get in the way'.[114] When asked about potential ties and resemblances between Soviet-era citizen involvement in matters of justice and contemporary vigilantes, the police officer expressed nostalgia for the Soviet times, when police had greater control over citizen volunteer groups.[115] These insights led to questions concerning unity in the vision of different sub-assemblages. Is there a unifying vector or is the system a compendium of

broad visions, interests and motivations that are handy for the regime as long as the regime itself is not targeted? As an academic in Saint Petersburg put it:

> You see, in order for the institutions to function, people who are part of these institutions should possess a respective motivation. This is related to the size of salary, discipline, organisational issues. When people are involved in crackdowns on demonstrations, they do not understand themselves what they are cracking down on, or why they capture these people.[116]

Thus, the assemblage appears to be functional within its dysfunctionality. Weak institutions, lack of professionalism, and absence of the rule of law lead to a scenario where no one is immune to retaliation, and this uncertainty is a significant motivator for self-censorship. At the same time, vagueness allowed for control over each sub assemblage, as the diversity of motives for participation leads to diversity among actors willing or forced to join the assemblage, without necessarily understanding its overarching objectives.

Sub-assemblage participants can be categorised into those generating counter-dissent content (pro-Kremlin bloggers, trolls) and those engaged in tracking and reporting on dissent content (kiberdruzhinas, anti-maidaners).[117] This active citizenry can conveniently assist the ruling elite in muting repellent voices. Contrary to the traditional understanding of vigilantism, which implies autonomy of citizen actors,[118] in Russia, vigilant citizens can be recruited by the state,[119] sometimes representing a quasi-citizen-led force with a façade agenda.

In addition to the amended legal framework, new initiatives were passed to encourage reporting on crime. The previously 'rare and unregulated'[120] practice of financially rewarding citizens for their contribution to crime-solving was turned into an official plan by the Ministry of Interior on 6 June, 2018.[121] Furthermore, under new provisions of the Yarovaya law package, failure to report on a witnessed crime can in itself be regarded as an act of crime, which further encourages snitching. Beyond this, the law package has called on the telecommunication operators to increase their storage capacities 'by 15 percent annually for the next five years' and 'to store correspondence, audio recordings of conversations, videos' and other types of user communications from 30 days to six months, depending on their type.[122] These regulations, however, are viewed with scepticism:

> The Yarovaya law package will not be fully implemented, it is too costly to store all data in Russia and they will just not do it. As usual, there is the law, but no one is implementing it.[123]

There are several groups whose objective is to seek, expose and report on information and users that are perceived as dangerous. Among these groups is a 'collective' that calls itself *Je Suis Maidan*. Based on the limited description available on its website and social media accounts, the group's objective appears to be centred around identification of 'participants of opposition protests', and to link their faces to respective social media profiles through 'various face recognition systems'.[124] The website features people across Russia with links to their social media profiles. Visitors are encouraged to send in photos of 'the heroes' to be listed on the website. This practice is not a novelty, according to a Moscow-based rights defender.

> The nationalists used to do this around ten years ago. They would make a post with a person's full address and invite people to retaliate. There were cases when retaliation took place.[125]

It is unclear what is done or is expected to be done to protest participants exposed on *Je Suis Maidan*. The website can serve as a convenient source of 'evidence' for law enforcement, and can potentially encourage harassment of the listed individuals. Equally, it may simply lead to no outcomes. The very presence of such a platform, however, can potentially deter protest, with an assumption that having seen own faces online, or faces of other protesters, people would be discouraged from participating in such events. The impact and popularity of *Je Suis Maidan* appear to be marginal, given the mere 137 members on its VKontakte social network page.[126]

Another group, SILOVIKI [Security officers], describes itself as a 'community of security departments of the Russian Federation' and enjoys a following of 65,865 subscribers on Telegram, 6,956 followers on Instagram, 2,990 followers on Twitter, and 660 subscribers on YouTube.[127] It is unclear who stands behind the group. SILOVIKI specialises in the exposure of activists, protestors, and opposition leaders. In some of the posts, they provide an image, full name, date of birth, address, phone number, vehicle description and licence plate numbers, names of parents and other relatives of the targets and openly call on their followers to 'say hello' to the exposed person via the provided phone number or to 'decorate' the target's car.

The Safe Internet League was established in 2011 with the support of the Ministry of Digital Development, Communications and Mass Media; the Ministry of Internal Affairs; and State Duma Committee on Issues of Family, Women and Children.[128] The League's objective is to find and 'eradicate dangerous content through community action by IT professionals, industry players, and regular internet users'.[129] Under the umbrella of the Safe Internet League there operates the Kiberdruzhina [Cyber Guards] which is a 'cross regional public youth movement' in its own words, consisting of 'over 20 thousand volunteers from across Russia and the CIS'.[130] The League's website explains that Kiberdruzhina is inspired by the 'Soviet-era druzhinnik neighbourhood watch units' who 'helped the authorities maintain law and order'.[131] Such a reference to the past once again underlines the re-packaged nature of control measures in contemporary Russia. Unlike the Soviet times, fear of punishment for the failure of reporting and ideological convictions alone are not doing all the justice anymore. Financial stimulation is used as a tool. 'In Tyva, they have announced this competition … to compete in reporting on suspicious online activity. The victor would receive 3,000 rubles'.[132] Such rewards can lead to false accusations and sabotage of deviant members of communities. Money is a unique variable, capable of overshadowing political, ideological, and moral motivations to snitch. 'There will definitely be willing people, especially in the provinces, they will do this outside of any political interest, just to make money'.[133] Diversity of motives for becoming part of the assemblages further widen its scope of reach. While legally obliged reporting on witnessed crime, at the background of the vagueness of the definition of this very crime, can lead to ubiquitous snitching; financial rewards for reported crime, in the system with a weak rule of law, can turn snitching into a business. This comes hand-in-hand with police forces who are assigned a quota to be fulfilled.

At the same time, rights defenders specialising in working with vigilantes believe that Cyber Guards are ineffective and that 'the media blows their significance out of proportion',[134] and further add that:

> The Cyber Guards are a completely dysfunctional entity. There is no functional activity. Russia's security apparatus is equipped with automated internet monitoring programmes and uses them where necessary.

> The only purpose of these Cyber Guards entities is to educate the youth, to get them involved and to lecture them on the danger of certain ideologies. [135]

Constituting sub-assemblages, formations such a Cyber Guards, SILOVIKI and others, resemble a force of opportunists who can gain certain benefits from serving up to the state. At the same time, by recruiting such forces, the state fulfils several objectives at once – the watchful gaze seems to be omnipresent; citizenry appears to be politically active on social media; and while searching for dangerous content online, technologically savvy and state-loyal vigilantes educate themselves on what is right and what is wrong.

8. Citizen counter-forces

At times, methods utilised in the assemblage work against the regime, as is evident from the case with the Cossacks[136] whose involvement in the dismissal of a public protest on 5 May 2018 created a wide resonance. In this case, face-recognition systems were used by the regime opponents to identify individuals who beat the protesters. A prominent example of a counter-force to the controlling assemblage is the civil analytics project Database, which publishes 'free-to-use investigations based on open data'.[137] The website maintains a list of provocateurs, propagandists, law enforcement officers, judges, snitches, and civil servants among other actors. It is not clear how this data can be used against pro-regime actors. The project itself describes the applicability of their investigations as follows:

> A significant part of our work is done in closed mode and stored in encrypted form according to all national and international personal data legislation. Access to these data is granted individually on request from official authorities as part of the investigation.[138]

State support and incentives created for specific forms of vigilantism lead to inequalities in operation modes. As researcher in Saint Petersburg explained:

> The difference between "allowed" activists and "not-preferred" activists is that the former enjoy access to state resources such as the FSB (Federal Security Service). Quite often they [vigilant audiences] post some data which is impossible to acquire without the assistance of special services, such as police and MVD [Ministry of Internal Affairs].[139]

Other citizen-led initiatives include the already mentioned Roskomsvoboda and Internet Protection Society (IPS). Both organisations counter online censorship and excessive internet control. While IPS is closely linked with Putin's main opposition leader Alexei Navalny, Roskomsvoboda has been invited to the advisory group of State Duma Committee on Information Policy, Information Technology and Communications.[140] In countering repressive measures of the state, the largest problem for counter forces is lack of unity. As St. Petersburg-based lawyer explained:

> I don't believe that users can be unified in one way or another. In Armenia, we recently saw how the people collectively stood up in opposition to the state. This will not be the case in Russia because opposition or social movements will not be able to unite. They oppose the state from very different standpoints.[141]

Thus, not only citizen counter-forces are scarce and inferior to the state in their capacities; they are also not necessarily unified. While technological affordances allow citizens to monitor and expose the 'previously exempt' actors; immunities, asymmetries, and other capacities must be considered in this uneven landscape. In Russia, with the greatly defined and enforced *vertical of power*, the ruling elite is in advantage in spite of any 'leveling of the hierarchy of surveillance'.[142]

9. Discussion

In the current understanding of surveillant mechanisms applied to the digital domain, the virtual other, or the 'data-double',[143] is constantly monitored and can attract institutional gaze towards the conventional self. In some cases, this dynamic is reversed as conventional 'offences' get tied to the concerned individual's digital trace, leading to arrests and fines. In other words, a person facing charges for online speech can already be in the focus of security forces for their offline activities. Amid the conveniently vague legislation governing online speech in Russia, for the law enforcement authorities, it is a matter of linking one element with the other – i.e. offline activism with the digital trace. Contrary to the 'data-double' theorisation, the physical person is selected first. As a Moscow-based rights defender explained:

> It is quite obvious that a person is selected first, and then they select online content that could be attached to the case. It is just so easy to find something [in the content shared online] that violates the law.[144]

Therefore, the original author of a given social media post may not suffer any consequences, while those who shared or otherwise engaged with this content might face the law, depending on the nature of their offline activities. The vagueness of definitions and police forces equipped with quotas establish dangerous realities where any user can face charges over any online activity.

Hand in hand with the legislative measures, the Kremlin employs and endorses[145] activists who engage in vigilantism and snitching. The lines between authority and citizens blur in this regard as vigilant citizens become an extension of the state. Thus, amid the increasing control over the digital domain, the state is allowing regime-loyal citizens to be active online, creating an illusion of citizen-led participation in domestic affairs, while reinforcing the fear of ubiquitous surveillance and the all-seeing gaze of the state. This dynamic opens a window of opportunity for actors willing to serve-up to the state, while the actual effectiveness of such formations is questionable.

With legislative frameworks that are open to interpretation and regulations that criminalise failure to report on a crime (accompanied with measures that encourage snitching by offering financial and other rewards), it could be expected that user arrests would be counted in tens of thousands, if not in millions. Is Russia's 'surveillant assemblage' weak, or is it selective by virtue? What is the role of state-recruited vigilant citizens in denouncing users? As a Moscow-based human rights defender explained, 'what is taking place [in Russia] today with all these "concerned" citizens is a joke. It is on such a primitive level, you wouldn't believe it'. Their colleague adds, 'our law enforcement system is too weak to carry out arrests on a mass scale, they only do targeted arrests'.[146] Presumably, the logic behind this measure is the instigation of self-censorship. Having

seen others arrested for a social media post, users are expected to think twice before sharing, or even "liking" similar content. As such, the repressive system is rather unpredictable; yet, uncertainty and unpredictability of the assemblage can create fruitful grounds for self-censorship, making the system effective by virtue of its dysfunctionality.

The regime revealed itself as both devious and inconsequential. It is devious in the sense that it does not skimp on entrapment of citizens, or on targeting teenagers and single mothers. At the same time, the regime is inconsequential in its selective response to online offences. As is evident from the cases, content that is deemed dangerous when "liked" or shared by some users is not removed and continues to circulate online; rather, the regime removes select citizens who engage with this content.

Citizen counter-forces indeed represent a scenario where, as per Haggerty and Ericson, those previously exempt from surveillance also fall under the gaze. Citizens monitor and reveal cases of rights violations, and instrumentalise similar 'weapons' of exposure that are used against them. However, the state (represented by the ruling elite) is in an obvious advantage with its law enforcement apparatus, legislative framework and technological capabilities.

10. Conclusion

Despite the autocratic turn in its policies following the initial liberalisation in the 1990s, and in contrast to the perceived omnipotence of its security apparatus, when put under the magnifying glass, Russia's surveillant assemblage indicates that multiplicity of its components and dysfunctionalities therein require the state to rely on a set of superficial measures designed to stimulate self-censorship. Among such measures are random and selective arrests of social media users, as well as recruitment of vigilant citizens, intended to assist the ruling elite in battling undesired online content.

Having unpacked Russia's surveillant assemblage, this article provided an overview of the types of online engagements which can cost social media users their freedom; it elaborated on the means of retaliation, by focusing on legal frameworks applied to social media offences; and it unpacked the elements (sub-assemblages) that collectively, but not exhaustively, make up contemporary surveillance practices in Russia. The analysis revealed several intriguing nuances in the Kremlin's approaches to internet control. First of all, the adapted legislative framework creates an environment in which, if needed, virtually any online activity can be tied to repressive legislation. The applicability of the law, in this case, is selective. This selectivity exemplifies a reverse approach to the 'data-double', as conventional behaviour of an individual can lead to scrutinisation of their digital trace.

While the Kremlin has taken respective measures to mute, eradicate, discourage, and otherwise limit voices that challenge its authority, Russia's surveillant assemblage has a central goal but no central motivations that could unite all of its sub-assemblages. Motivation is a subjective concept inside each sub-assemblage – be it law enforcement, regional authorities, or vigilant citizens. Motives may also vary among citizen counter-forces opposing repressive state measures; however, issues of unity and collaboration also come into play in this domain.

Social media user convictions in Russia are a by-product of the system where the desire to control defies a systematic approach. While this defiance may be interpreted as

a weakness of the central structure, ambiguity and monomania of the structure make everyone potentially vulnerable. Due to technical and financial inability to replicate a Chinese-style firewall, Russia's ruling elite opted for 'trolling' the web through the spread of fear via repressive legislation, selective arrests, and regime-loyal citizens acting out in the manner that echoes the country's totalitarian past. As Daucé, Loveluck, Ostromooukhova, and Zaytseva put it, Russia can be viewed as 'a test laboratory for plural forms of citizen participation in online security'.[147]

In the global perspective, current measures adopted by the Kremlin serve as examples of 'best practices' to other autocratic regimes, seeking to establish control over online self-expression. As international, regional and domestic governance of the world wide web is entering discourse at the level of the United Nations,[148] an informed and sober outlook on the role and influence of political, legislative, social, and economic realities on internet governance is pressing.

Further research should focus on the role of international and domestic social media platforms, messengers, and content sharing outlets in Russia and beyond; enriching literature and policy through comparative analyses across governance approaches.

Notes

1. A quote by Óscar Raymundo Benavides Larrea. Quoted by "Lawyer I" during the interview
2. Advocating for democracy and human rights in Russia, founded by former businessman and democracy activist Mikhail Khodorkovsky. Website is banned in Russia since 2017 https://openrussia.org/about/.
3. See https://meduza.io/news/2017/02/13/na-aktivista-zaveli-delo-za-repost-novosti-o-ego-sude-za-repost-fotografii-milonova.
4. Semenov was fined again in 2017 for a social media post about the outcome of this court case https://www.svoboda.org/a/28593340.html.
5. See https://www.mk.ru/social/2018/06/26/ugolovka-za-reposty-v-socsetyakh-statistika-uzhasnula.html.
6. Kravchenko, "Inventing Extremists," 1.
7. Romashenko, "В России вчетверо выросло."
8. See https://мвд.рф/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivodejstviju_j.
9. See https://meduza.io/en/feature/2019/08/29/what-is-center-e.
10. See http://www.ligainternet.ru/liga/about.php.
11. See http://www.ligainternet.ru/en/liga/activity-cyber.php.
12. 'I am Maidan' – evidently inspired by merging 'Je Suis Hebdo' and Ukraine's 'Euro Maidan.'
13. Little is known about this formation's relationship with official state security forces. On several occasions SILOVIKI were cited in Russia's traditional media. For instance, https://russian.rt.com/russia/news/691109-zhena-shestun-hodorkovskii-vstrecha.
14. Loveluck, "The Many Shades of Digital Vigilantism."
15. Kustikova, "The Whisperers: Meet The Snitches."
16. See https://bewareofthem.org/en/about-us/.
17. See https://ozi-ru.org/ob-obshhestve/kto-my/.
18. See https://roskomsvoboda.org/about-us/.
19. Ibid.
20. Mueller, "Networks and States."
21. See for instance https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/798.

22. See for instance https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/authority.
23. See for instance https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/795.
24. To Troll – "to harass, criticize, or antagonize (someone) especially by provocatively disparaging or mocking public statements, postings, or acts" https://www.merriam-webster.com/dictionary/troll.
25. Galič, Timan and Koops, "Bentham, Deleuze and Beyond," 10.
26. Foucault, *Discipline and Punish*, 217.
27. Ibid., 208.
28. For a chronological overview of surveillance theories see Galič, Timan and Koops, "Bentham, Deleuze and Beyond."
29. Deleuze and Guattari, "A Thousand Plateaus: Capitalism and Schizophrenia."
30. Haggerty and Ericson, "The Surveillant Assemblage," 606.
31. Ibid., 610.
32. Ibid., 610.
33. Ibid., 606.
34. Ibid., 619.
35. Deleuze, "Postscript on the Societies of Control," 5.
36. Haggerty and Ericson, "The Surveillant Assemblage," 611.
37. Gabdulhakov, "In the Bullseye of Vigilantes."
38. Hier, "Probing the Surveillant Assemblage."
39. Eubanks, "Automating Inequality."
40. Monahan, "Counter-surveillance as Political Intervention?"
41. Haggerty and Ericson, "The Surveillant Assemblage," 608.
42. Becker, "Lessons From Russia."
43. Oates, "Russian Media in the Digital Age," 399.
44. Ibid.
45. Lokot, "Be Safe Or Be Seen?"
46. White and McAllister, "Did Russia (Nearly) Have."
47. See note 43 above.
48. Ibid.
49. Svenonius and Björklund, "Surveillance from a Post-Communist Perspective," 273.
50. Interview, Rights Defender III, Moscow, 2018.
51. Goncharenko, "Russia Moves Toward Creation."
52. See https://www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002.
53. See https://www.rferl.org/a/russia-s-controversial-sovereign-internet-law-comes-into-force/30247754.html.
54. See https://www.gazeta.ru/tech/2018/08/18/11899507/two_years.shtml?updated.
55. See https://memohrc.org/ru/monitorings/ne-tolko-pervaya-chast-za-kakie-posty-vas-vse-eshche-smogut-posadit-posle-popravok.
56. Criminal Code Of The Russian Federation.
57. See note 55 above.
58. Denber, "Pussy Riot And Russia's."
59. Released under state amnesty in 2013, three months before the end of the sentence term.
60. See http://en.kremlin.ru/events/president/news/18422.
61. See note 56 above.
62. Roudik, "Russia: Strengthening Of Punishment."
63. Interview, Lawyer I, Moscow.
64. Ibid.
65. Smyth and Oates, "Mind The Gaps: Media," 291.
66. See https://memohrc.org/ru/monitorings/kritike-nepodvlastny-kak-vydelyali-socgruppu-gossluzhashchih-i-opredelyali-stepen-ee.

67. See https://www.themoscowtimes.com/2019/03/18/putin-signs-fake-news-internet-insults-bills-into-law-a64850.
68. Chudovsky District Court, http://chudovsky.nvg.sudrf.ru/modules.php?name=press_dep&op=1&did=377.
69. See https://ozi-ru.org/proekty/internet-repressii/karta/
70. Most of the charges concern posts and activity on VKontakte, but incidents concern a wide variety of platforms.
71. See https://www.aljazeera.com/indepth/features/2017/11/death-russian-171123102640298.html.
72. See https://www.svoboda.org/a/28943937.html.
73. See https://lenta.ru/news/2018/02/15/antinazi/.
74. See https://meduza.io/news/2018/02/12/student-poluchil-2-5-goda-za-ekstremistskie-kartinki-on-ispolzoval-ih-dlya-diplomnoy-raboty-pro-ekstremizm.
75. See Meduza.io, 2017, https://meduza.io/news/2017/02/13/na-aktivista-zaveli-delo-za-repost-novosti-o-ego-sude-za-repost-fotografii-milonova.
76. https://www.znak.com/2017-12-01/glavu_predvybornogo_shtaba_alekseya_navalnogo_leonida_volkova_arestovali_na_30_sutok .
77. See http://novayagazeta.spb.ru/articles/9466/utm_source=-/.
78. See https://agora.legal/cases/show/Delo-lovca-pokemonov-Ruslana-Sokolovskogo/98.
79. See https://www.hrw.org/news/2017/05/11/russia-pokemon-go-blogger-convicted.
80. Ibid.
81. Ibid.
82. See http://www.fedsfm.ru/documents/terrorists-catalogue-portal-act.
83. See https://agora.legal/cases/Internet/Delo-ateista-Viktora-Krasnova-ob-oskorblenii-chuvstv-veruyushih-vo-%C2%ABVKontakte%C2%BB/4.
84. See https://www.themoscowtimes.com/2017/02/15/russian-court-drops-charges-against-atheist-for-saying-god-doesnt-exist-a57156.
85. Interview, NGO employee, Moscow, 2018.
86. See https://www.agora.legal/cases/Internet/Delo-Marii-Motuznoi-Barnaul/275.
87. See https://www.themoscowtimes.com/2018/07/25/russian-woman-reportedly-faces-6-years-in-prison-for-insulting-memes-a62341.
88. See note 82 above.
89. See https://www.themoscowtimes.com/2019/09/20/6-jehovahs-witnesses-jailed-for-extremism-in-russia-a67356.
90. See https://meduza.io/en/news/2018/06/06/the-russian-internet-is-safe-from-yet-another-extremist-out-to-get-vladimir-putin.
91. See https://www.svoboda.org/a/28866295.html.
92. See note 82 above.
93. See https://memohrc.org/ru/monitorings/delo-novogo-velichiya-kto-eti-lyudi-i-za-chto-ih-sudyat-gid-ovd-info.
94. See https://meduza.io/en/news/2018/08/14/the-mothers-march-is-coming-to-moscow-plus-a-flashmob-is-headed-for-yekaterinburg.
95. See https://www.themoscowtimes.com/2018/08/15/mothers-march-moscow-against-novoye-velichiye-extremism-case-a62534.
96. See note 63 above.
97. See https://www.themoscowtimes.com/2017/08/23/engineer-jailed-over-crimea-is-russia-social-media-post-released-a58741.
98. Ibid.
99. See https://www.agora.legal/cases/Internet/Delo-Andreya-Bubeeva-za-reposty-VKontakte-o-Kryme-Tver/35.
100. See note 82 above.
101. See https://www.sova-centre.ru/en/misuse/news-releases/2017/01/d36176/.
102. Ibid.
103. Interview, Academic I, St. Petersburg, 2018.

104. Interview, public opinion NGO, Moscow, 2018.
105. See https://www.sova-center.ru/racism-xenophobia/news/counteraction/2017/02/d36294/.
106. See https://zona.media/news/2018/08/07/bijsk.
107. See https://www.sova-center.ru/misuse/news/persecution/2018/08/d39886/.
108. See https://www.sova-center.ru/misuse/news/persecution/2018/08/d39885/.
109. First offence would lead to a fine of 10 to 20 thousand rubles, or 100 hours of mandatory social service, or arrest for up to 15 days. For a repeated offence committed within a year, the law implies punishment of 2 to 5 years in prison. http://duma.gov.ru/news/29223/.
110. See note 8 above.
111. See note 9 above.
112. Daucé et al., "From Citizen Investigators to Cyber Patrols," 67.
113. Ibid.
114. Ibid.
115. Online interview, Law Enforcement, 2018.
116. Interview, Academic II, St. Petersburg 2018.
117. See https://www.theguardian.com/world/2015/feb/26/russia-anti-maidan-protest-moscow.
118. Johnston, "What is Vigilantism?"
119. Gabdulhakov, "From Comrade's Courts to Dotcomdrade Vigilantism."
120. See https://www.themoscowtimes.com/2018/08/23/russian-police-reward-informants-150k-under-new-plan-a62629.
121. See http://publication.pravo.gov.ru/Document/View/0001201808160030.
122. See https://www.vesti.ru/doc.html?id=3033594.
123. See note 116 above.
124. See https://jesuismaidan.com/.
125. Interview, Rights Defender III, Moscow 2018.
126. See https://vk.com/jesuismaidan.
127. December 2019.
128. See http://www.ligainternet.ru/liga/about.php.
129. Ibid.
130. See http://www.kiberdruzhina.ru/o-nas.
131. See http://www.ligainternet.ru/en/liga/activity-cyber.php.
132. Interview, Rights Defender I, Moscow.
133. Ibid.
134. Ibid.
135. Ibid.
136. See https://www.nytimes.com/2013/03/17/world/europe/cossacks-are-back-in-russia-may-the-hills-tremble.html .
137. See https://bewareofthem.org/en/about-us/.
138. Ibid.
139. Online interview, Academic III.
140. See http://komitet5.km.duma.gov.ru/Ekspertnye-Sovety.
141. Interview, Lawyer I, St. Petersburg.
142. Haggerty and Ericson, "The Surveillant Assemblage," 606.
143. Haggerty and Ericson, "The Surveillant Assemblage."
144. Interview, Rights Defender I, Moscow 2018.
145. Gabdulhakov, "From Comrades' Courts to Dotcomdrade Vigilantism."
146. Interview, Rights Defender II, Moscow.
147. See note 112 above.
148. See https://news.un.org/en/story/2019/11/1052241.

Acknowledgements

Disclosure statement

Funding

Notes on contributor

Rashid Gabdulhakov is a Ph.D. Candidate at the Department of Media and Communication at Erasmus University Rotterdam, the Netherlands. As a member of an international team of scholars, he is researching the phenomenon of digital vigilantism and its manifestation in Russia and other former Soviet republics.

ORCID

Rashid Gabdulhakov   http://orcid.org/0000-0003-0266-8381

Bibliography

Agora. "Дело Марии Мотузной (Барнаул)" [The case of Maria Motuznaya (Barnaul)]. 2018.
Agora. "Дело атеиста Виктора Краснова об оскорблении чувств верующих во 'Вконтакте'" [The case of an atheist Viktor Krasnov on insulting the feelings of believers on 'VKontakte']. 2018.
Agora. "Дело Андрея Бубеева за репосты Вконтакте о Крыме (Тверь)" [The case of Andrei Bubeev for VKontakte reposts about the Crimea (Tver)]. 2018.
Agora. "Дело Евгения Каракашева (Крым)" [The case of Evgeny Karakashev(Cimea)]. 2018.
BBC. 2018. "Кибердружины от 'Единой России' будут искать в интернете нелегальный контент" [Cyberguards from United Russia will search the Internet for illegal content]. November 2.
Becker, J. "Lessons From Russia." *European Journal of Communication* 19, no. 2 (2004): 139–163. doi:10.1177/0267323104042908
Bevza, D. 2018. "Нарисовать дело: как в России сажают за репосты" [Drawing a case: How they lock up for reposts in Russia]. *Gazeta.ru*, August 19.
Daucé, F., B. Loveluck, B. Ostromooukhova, and A. Zaytseva. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia." *Laboratorium: Russian Review of Social Research* 11, no. 3 (2020): 46–70. doi:10.25285/2078-1938-2019-11-3-46-70.
Deleuze, G. "Postscript on the Societies of Control." *October* 59 (1992): 3–7.
Deleuze, G., and F. Guattari. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Continuum, 2004.
Denber, R. 2018. "Pussy Riot and Russia's surreal 'Justice'." *CNN*, August 17.
Eubanks, V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. First ed. New York, NY: St. Martin's Press, 2018.
Federal Financial Monitoring Service. Россинмониторинг - перечень террористов и экстремистов (Действующие) [Rosfinmonitoring - List of Terrorists and Extremists (Active)]. 2018.

Foucault, M. *Discipline and Punish: The Birth of the Prison*. 2nd Vintage Books ed. New York: Vintage Books, 1995.

Gabdulhakov, R. "Citizen-Led Justice in Post-Communist Russia." *Surveillance and Society* 16, no. 3 (2018): 314–331. doi:10.24908/ss.v16i3.6952.

Gabdulhakov, R. "In the Bullseye of Vigilantes: Mediated Vulnerabilities of Kyrgyz Labour Migrants in Russia." *Media and Communication* 7, no. 2 (2019): 230–241. doi:10.17645/mac.v7i2.1927.

Galič, M., T. Timlan, and B. J. Koop. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy and Technology* 30, no. 1 (2017): 9–37. doi:10.1007/s13347-016-0219-1.

Gershkovich, E. 2018. "A 'Mothers' March' in Moscow for teenage girls charged with extremism." *The Moscow Times*, August 15.

Goncharenko, R. 2018. "Russia moves toward creation of an independent internet". *Deutsche Welle*. January 17.

Haggerty, K. D., and R. V. Ericson. "The Surveillant Assemblage." *British Journal of Sociology* 51, no. 4 (2000): 605–622. doi:10.1080/00071310020015280.

Hier, S. P. "Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control." *Surveillance & Society* 1, no. 3 (2003). doi:10.24908/ss.v1i3.3347.

Human Rights Watch. *Russia: Pokemon Go Blogger Convicted*. 2017.

Johnston, L. "What Is Vigilantism?" *The British Journal of Criminology* 36, no. 2 (1996): 220–236.

Kravchenko, M. *Inventing Extremists: The Impact of Russian Anti-Extremism Policies on Freedom of Religion or Belief*. United States Commission on International Religious Freedom. 2018.

Kustikova, A. 2017. "The Whisperers: Meet the snitches making a return to Russia." *The Moscow Times*, May 26.

Lindenau, J. 2019. "Russia's sovereign internet law comes into force." *The Moscow Times*, November 1.

Lokot, T. "Be Safe Or Be Seen? How Russian Activists Negotiate Visibility And Security In Online Resistance Practices." *Surveillance & Society* 16, no. 3 (2018): 332–346. doi:10.24908/ss.v16i3.6967.

Loveluck, B. 2019. "The many shades of digital vigilantism. A typology of online self-justice." *Global Crime*, (2019): 1–29. doi:10.1080/17440572.2019.1614444.

Maetnaya, E. 2018. "Где было гестапо– теперь администрация." [Where the Gestapo used to be, now there is the administration]. *Radio Liberty* November 21.

Meduza. 2017. "Активиста 'Открытой России' осудили за репост. А потом на него завели дело за репост новости про суд." ['Open Russia' activist convicted for a repost. And then a case was brought against him for reposting the news about the court hearing]. February 13.

Meduza. 2018. "The Russian Internet is safe from yet another 'extremist' out to get Vladimir Putin." June 6.

Meduza. 2018. "The Mothers' March is coming to Moscow, plus a flashmob is headed for Yekaterinburg." August 13.

Memorial. "Критике неподвластны? Как выделяли соцгруппу госслужащих и определяли степень ее обиды" [Defying criticism? How they distinguished the social group of civil servants and determined the degree of hurting its feelings]. 2018.

Memorial. "Не только первая часть. За какие посты вас все еще смогут посадить после поправок Путина" [Not only section one. Posts that can still cost you freedom after Putin's amendments]. 2018.

Memorial. "Дело 'Нового Величия' — кто эти люди и за что их судят" [The case of 'Novoe Velichie' – who are these people and why they are being sued]. 2018.

Monahan, T. "Counter-Surveillance As Political Intervention?" *Social Semiotics* 16, no. 4 (2006): 515–534. doi:10.1080/10350330601019769.

Moncada, E. "Varieties of Vigilantism: Conceptual Discord, Meaning and Strategies." *Global Crime* 18, no. 4 (2017): 403–423. doi:10.1080/17440572.2017.1374183.

Mueller, M. "*Networks and States: The Global Politics of Internet Governance*" Information Revolution and Global Politics Cambridge, Mass: MIT Press, 2010.

Oates, S. "Russian Media in the Digital Age: Propaganda Rewired" *Russian Politics* 1, no. 4 (2016): 398–417. doi:10.1163/2451-8921-00104004.

Ozerova, M. 2018. "Уголовка за репосты в соцсетях: статистика ужаснула." [Criminal charges over social media reposts: horrifying statistics]. *Mk. ru*, June 26

Petkova, Mariya. 2017. "The death of the Russian far right. How the Kremlin destroyed the far right in Russia, while backing it in the West." *Al Jazeera*, December 16.

President of Russia. 2018. "Amendments to Criminal Code and certain legislative acts in the aim of protecting religious convictions and feelings." *The Kremlin*, June 30.

Radio Liberty. 2017. "Активист обжаловал в ЕСПЧ штрафы за репост фотографии Милонова" [Activist appealed to ECHR over fines for a repost of Milonov's photo]. July 3.

Roudik, P. *Russia: Strengthening of Punishment for Extremism*. Global Legal Monitor, 2018.

Romashenko, S.. 2018. "В России вчетверо выросло число осужденных за разжигание вражды" [The number of convicts for inciting hostility has quadrupled in Russia]. Deutsche Welle, April 19.

SOVA. "Misuse of anti-extremism in December 2016." 2018.

Smyth, R., and S. Oates. "Mind the gaps: Media use and mass action in Russia." *Europe-Asia Studies* 67, no. 2 (2015): 285–305. doi:10.1080/09668136.2014.1002682.

"State Legal Information Portal". Publication.Pravo.Gov.Ru, 2018. http://publication.pravo.gov.ru/Document/View/0001201808160030

Svenonius, O., and F. Björklund. "Editorial: Surveillance from a post-communist perspective." *Surveillance & Society* 16, no. 3 (2018): 269–276. doi:10.24908/ss.v16i3.12684.

The Moscow Times. 2017. "Engineer jailed over 'Crimea is Ukraine' social media post released." August 23.

The Moscow Times. 2017. "Russian court drops charges against atheist for saying 'God doesn't exist." February 15.

The Moscow Times. 2018. "Russian police to reward informants up to $150K under new plan."

Interviewee	Comments	Date
Academic I	St. Petersburg-based. Specialising in Russia's online activism. Online interview.	2018
Academic II	St. Petersburg-based. Specialising in Russia's online activism. Online interview.	2018
Academic III	Finland-based. Specialising in Russia's digital media and online culture. Online interview.	2018
Lawyer I	Lawyer specialising in Russian cases in the European Court for Human Rights. In-person interview, St. Petersburg.	2018
Lawyer II	Specialising in internet-related arrests. In-person interview, Moscow.	2018
Law Enforcement I	Lieutenant colonel. State penitentiary service. Online interview.	2018
NGO I	Specialising in public opinion monitoring. In-person interview, Moscow.	2018
Rights Defender I	Specialising in vigilantism . In-person interview, Moscow.	2018
	Online interview.	2019
Rights Defender II	Specialising in vigilantism. In person interview, Moscow.	2018
Rights Defender III	Specialising in xenophobia. In-person interview, Moscow.	2018

August 23.
The Moscow Times. 2018. "Russian woman reportedly faces 6 years in prison for insulting memes." July 25.
Trottier, D. "Digital vigilantism as weaponisation of visibility." *Philosophy and Technology* 30, no. 1 (2017): 55–72. doi:10.1007/s13347-016-0216-4.
Vesti.ru. "'Пакет Яровой' вступил в силу 1 июля." [The 'Yarovaya law package' entered force on 1 June]. July 1
White, S., and M. Ian. "Did Russia (nearly) have a Facebook revolution in 2011? Social media's challenge to authoritarianism." *Politics* 34, no. 1 (2013): 72–84. doi:10.1111/1467-9256.12037.
WIPO Lex."Russian Federation: Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (As amended up to Federal Law No. 18-FZ of March 1, 2012)."

Annexe I. Anonymised list of interview participants