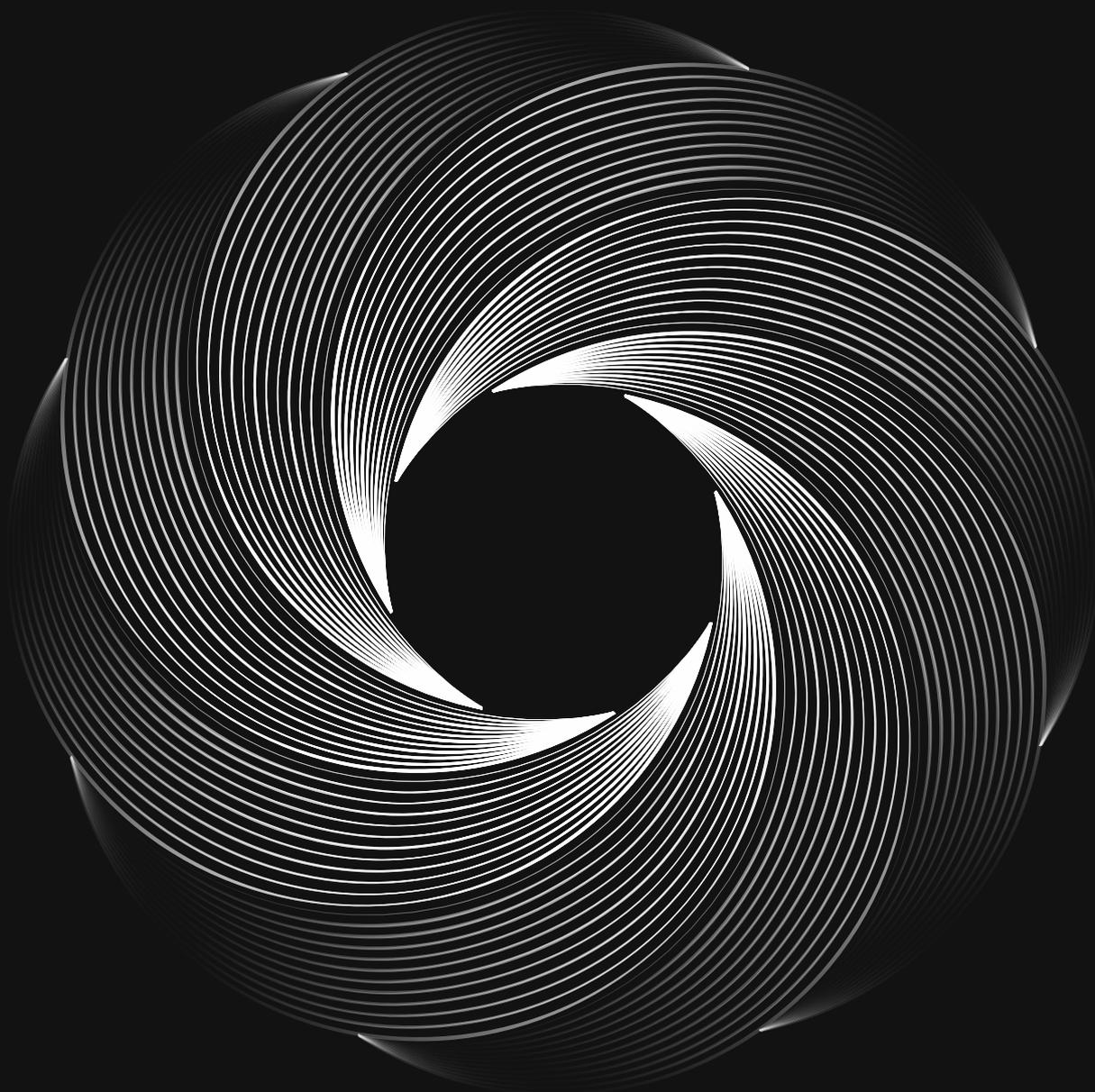


DIGITAL RIGHTS FALTER AMID POLITICAL
AND SOCIAL UNREST



Editors: Danilo Krivokapić, Andrej Petrovski, Sofija Todorović, Marija Ristić

Authors: Bojan Perkov, Anka Kovačević, Mila Bajić

Monitoring team: Anja Vladisavljević, Ákos Keller-Alánt, Marcel Gascón Barberá, Elma Selimović, Bojan Perkov, Bojan Stojkovski

Opinion Pieces:

Bosnia and Herzegovina: Dalio Sijah, Maida Salkanović

Croatia: Oriana Ivković Novokmet

Hungary: Peter Erdelyi

North Macedonia: Filip Stojanovski

Romania: Marcel Gascón Barberá

Serbia: Milica Jovanović

Copy-editor: BIRN

Design: Olivia Solis Villaverde

SHARE Foundation, June, 2021.

This publication was produced with the financial support of the Sida, NEF, Civitates, Open Society Foundations and the Partner Foundations. Its contents are the sole responsibility of the SHARE Foundation and BIRN and do not necessarily reflect the views of the donors.



Contents

Foreword and Executive Summary	4
Definitions, Numbers and Methodology	6
Featured Cases: Common Trends	8

Bosnia and Herzegovina	12
Fact sheet	12
Featured cases	13
Op-ed	15

Croatia	19
Fact Sheet	19
Featured cases	20
Op-ed	22

Hungary	26
Fact sheet	26
Featured cases	27
Op-ed	30

North Macedonia	35
Fact sheet	35
Featured cases	36
Op-ed	38

Romania	44
Fact sheet	44
Featured cases	45
Op-ed	48

Serbia	53
Fact sheet	53
Featured cases	54
Op-ed	57

Foreword and Executive Summary

When the global pandemic halted our “offline” lives, we moved meetings, dinners and parties, shopping, protests to the online sphere. As we sought comfort, education, business and social life in the digital, our only public sphere also became overwhelmed with content designed to manipulate and misinform citizens.

Journalists, officials and the general public have faced vicious attacks – including verbal abuse, trolling, smear campaigns and undue pressure to retract content – in response to publishing information online. Many of our data were stolen, and our privacy endangered. Surveillance flourished.

In the period from August 2019 until December 2020, BIRN and the SHARE Foundation were gathering information on digital rights violations in Bosnia and Herzegovina, Croatia, North Macedonia, Hungary, Romania and Serbia, and our monitoring shows violations of digital rights continued at an alarming rate in all six countries.

As all six held elections during this period – local, general and/or presidential – our findings raise serious concerns about how the digital arena has been effectively hijacked to propagate fake news, hate-fuelled conspiracy theories and misinformation in support of offline efforts to sabotage democratic processes.

Just when people needed factually-correct information and governments needed close scrutiny to ensure high standards in public life, cyberattacks were launched against state bodies and the public were overwhelmed with false information and discriminatory content designed to manipulate voting and/or stoke hatred of particular groups.

Governments, on the other hand, used the pandemic to curb freedom of expression, abused health data, while many public institutions failed to meet standards of free and open internet.

During this period, BIRN and the SHARE Foundation verified more than 800 violations of digital rights including efforts to prevent valid freedom of speech (trolling of media and general public engaged in fair reporting and comment, for example) and at the other end of the scale, efforts to overwhelm users with false information and racist/discriminatory content – usually for financial or political gain.

Most online violations we monitored were under the category of pressures because of expression and activities (375) while the fewest violations monitored were classified as holding intermediaries liable (0).

Action was taken in just 21 per cent of cases, which usually entailed – depending on the type of violation – removing articles or deleting posts and/or comments by the general public and public sector organisations. During the COVID-19 crisis, we saw a rise in arrests of citizens accused of causing panic by publishing fake news on social media. Hungary, Serbia, Bosnia and Herzegovina were leading in this trend. Legal action, including arrests, penalties or other court action, was taken in less than 0.5 per cent of all monitored cases.

It is important to note that just as some violations included attempts to stifle free speech and frustrate freedom of expression through publishing falsehoods, not all legal actions launched to apparently hold intermediaries liable were legitimate attempts to protect freedom of speech. Some were cynical attempts against the public interest to block the publication of proven facts.

All these violations have contributed to an atmosphere dominated by fear and hatred with already vulnerable communities – such as LGBT+, groups identifying as female, migrants, particular ethnic groups – becoming subjected to worse and more frequent abuse, leaving them ever more isolated from support networks.

Those guilty of using the digital space to undermine democracy, intimidate others from publishing the truth or to spread malicious falsehoods operate with impunity, not least because there is no meaningful sense in the region of what constitutes digital rights – never mind the desire to or means to protect those rights.

Our report is the first effort on the regional level to map current challenges in the digital sphere and aims to fill in the gaps in the research. We took an interdisciplinary approach and looked at the problems from the legal, political, tech and societal angle, as an attempt to show that the problems and solutions to these violations should also be holistic and overarching. We also want to highlight these issues, as the lack of awareness of digital rights violations within society further undermines democracy, not only in times of crisis.

We don't see the internet only as open and transparent but also see digital evolution as a set of mechanisms and tools that have great potential to serve the needs of people, and let's not forget that internet access has proved indispensable in times of crisis such as in the COVID-19 pandemic.

We hope this report will serve not just for stock taking but be understood as a map showing what and how to further advance our rights, and also as an invitation to everyone to join forces in making our digital world healthy, too.

Definitions, Numbers and Methodology

Our definition of digital rights and violations

For the purposes of this report, we perceive digital rights as fundamentally the same human rights that exist in the offline world and we believe that they should be protected in the same manner.

To better understand how digital rights are being undermined, we have created seven broad [categories of violations](#):

- Information security breaches
- Information privacy and personal data breaches
- Pressures because of expression and activities on the internet
- Manipulation and propaganda in the digital environment
- Holding intermediaries liable
- Blocking and filtering of content
- Other breaches

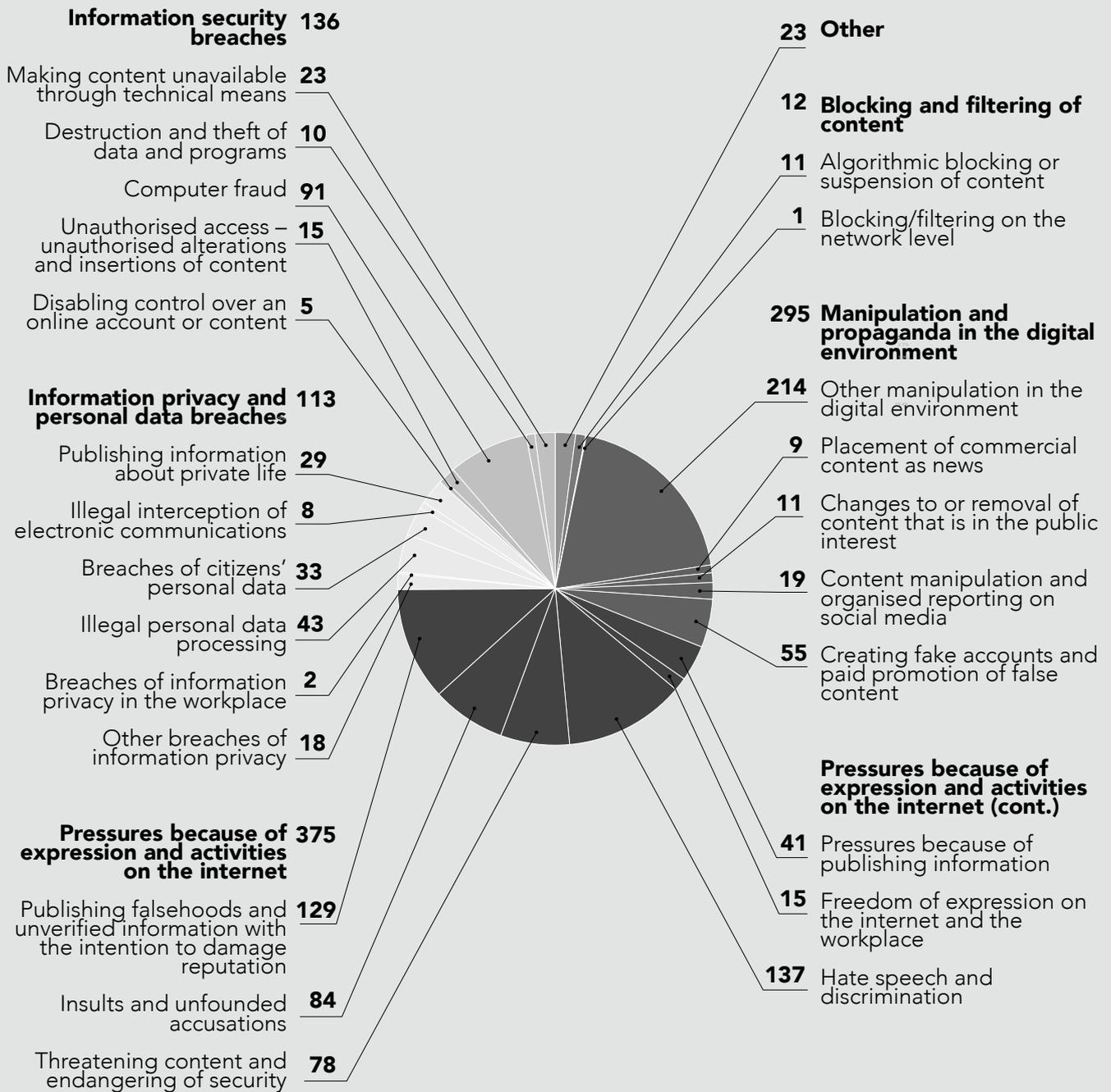
As our lives are increasingly dependent on the internet and we increasingly exercise our freedoms online, it is vital digital rights are afforded the same protections as offline human rights. Of course, we acknowledge that digital right definitions will need to be redefined to keep pace with rapidly-evolving cyberspace development and world events.

The numbers

As evidenced by the graph below, there is an almost dizzying array of ways in which digital rights were violated during the monitoring period (1 August 2019 to 1 December 2020). We have sorted the data into seven categories and 25 sub-categories.

The 832 violations tracked by BIRN and the SHARE Foundation cover government websites, media outlets and social media accounts owned by prominent public figures, celebrities and members of the public. These examples are a mere fraction of the true number of violations that occurred during the time period covered by the report.

For deeper insights into how digital platforms have been used to undermine democracy and pit people against each other – often inciting violence against marginalised groups - we have included an op-ed piece in each country-specific report.



Methodology

BIRN and the SHARE Foundation have verified and analysed 832 instances we identified as violations of digital rights. These cases were either reported directly to BIRN by journalists, bloggers or members of the public or were picked up by monitoring – individual researchers – at both BIRN and the SHARE Foundation.

Through our [unique monitoring methodology](#), we have defined violations of those rights into seven broad categories as listed earlier in the report. Of course, developing a methodology to classify and monitor digital rights and breaches of freedoms is a continuous process, bearing in mind the expansion of technologies and tools in the online sphere.

Featured Cases: Common Trends

Democratic elections undermined

With elections at local, parliamentary or presidential level taking place in each country during the reporting period and most citizens online far more often than usual because of the pandemic, electioneering was marred by numerous digital rights violations ranging from highly organised cyberattacks against state institutions and services to smear campaigns targeting political figures or outspoken individuals.

Public service websites hacked

Overall, our monitoring findings have shown a rise in the number of cyberattacks on public service and media websites. In North Macedonia, a [denial of service \(DDoS\) attack on the website of the Electoral Commission \(DIK\)](#) on polling day stopped the publication of confirmed voting results for three hours. Oliver Derkovski, Chairman of the DIK, [said](#) the attack did not cast any doubt over the legitimacy of the vote as the hack only affected the publication of the results. However, such a technical attack on an election information system could, under some specific circumstances, affect election results, and therefore needs to be analysed very carefully. Hacking attacks are covered in more detail in the country-specific sections of this report.

Provocation and exploitation of social unrest

People across the region took to the streets – not always peacefully – to take part in anti-migrant, anti-government and anti-COVID-19 lockdown measures protests and also in counter-demonstrations against alleged police brutality toward minority groups and discrimination.

Protests were most often organised online with people motivated to take part by content shared on social media. Disinformation spread like wildfire, causing ever-deepening distrust in state institutions, government and authority figures.

Doctored photos, fake statements and profiles have been used to undermine journalism and have led to direct attacks and threats against journalists. In Bosnia and Herzegovina, fact-checking websites identified fake news items focused on ethnic discord and ethnically-charged notions of national interest on an almost daily basis.

As ever, calling out fake news and challenging the content with the facts has not proved an efficient way to counteract widespread misinformation and coordinated

online manipulations.

In all countries, public debate in both analogue and digital spheres was loudly opinionated and highly emotional with scant – if any - regard for the facts. Existing prejudices against ethnic groups were reinforced and exploited to weaken regional democracies and reverse progress made in recent years toward becoming tolerant, properly-informed, open and progressive societies.

Conspiracy theories and fake news

The ongoing migrant crisis and widespread anti-migrant sentiment sparked a marked increase in xenophobic and racist content produced and shared online, with media outlets and social networks sharing conspiracy theories blaming migrants for the spread of COVID-19. Animosity towards migrants has noticeably increased in Croatia, as have accusations of police brutality and pushbacks at the border.

The COVID-19 pandemic triggered a large number of conspiracy theories related to the vaccines, the causes of the pandemic and how the virus is being spread, many of these theories had political connotations.

Numerous fake news articles and web portals were detected in the online sphere during the whole monitoring period but they flourished online during COVID-19. Online media were categorised as one of the most frequent violators of citizens digital rights (media were defined as attackers in 177 cases), while in 58 cases media were defined as victims.

Online hatred leaves vulnerable more isolated

The general public was the most targeted group in terms of online hostility and hatred, particularly those from the LGBT+, Roma, Jewish, female-identifying and migrant communities. Online attacks contained discriminatory language and derogatory terms with women facing misogynistic and gender-based harassment and the LGBT+ community facing hated-fuelled homophobic attacks.

Roma communities were exposed to discriminatory and racist online behaviours predominantly in Romania and North Macedonia. Migrants were the most common target of various far-right groups across the region and were most often described as dangerous and blamed for crimes despite the absence of any reliable proof. Widespread impunity for those perpetrating these online harms and a low level of accountability generally has not helped to create a safer or healthier online environment or increased tolerance among people from the region.

The most vulnerable groups, namely LGBT+, Roma, Jewish and female-identifying communities, remain the easiest targets for xenophobic and prejudiced social media content. The current priority in this regard should be establishing levels of protection where they do not currently exist to ensure the security of at-risk populations. The harmful patterns of behaviour from the offline world are simply transposed to the online sphere, where perpetrators feel more able to attack without fear to be held accountable for any wrongdoing.

Tech shortcuts fail to solve complex societal problems

The pandemic taught us that we can't rely solely on technology to solve complex societal problems or overcome the challenges posed by weak rule of law, deep health care issues, inequalities and highly corrupt governance. An example of such use of easy but disputable solutions were contact tracing apps in North Macedonia and Croatia, which turned out to be not so useful since the public were not keen to download them.

On the other side, one of the biggest tech security violations was caused by the not-so-responsible use of online systems in Serbia. The username and password to access the state's COVID-19 information system were publicly available on a health institution's web page for eight days. This period of time was long enough for the page to be indexed by Google and, although invisible on the website, it was accessible through a simple search. After discovering the breach on 17 April 2020, the SHARE Foundation immediately informed the competent authorities: the Commissioner for Information of Public Importance and Personal Data Protection, the National CERT and the Ministry of Trade, Tourism and Telecommunications.

A BIRN investigation discovered tech used to calculate COVID-19 cases in Serbia led to the authorities grossly under-reporting infections and related deaths. The true death toll was more than double the official figure given.

What Next?

Online attacks seem to be the most common mode of communication and this is due at least in part to the COVID-19 pandemic, which has made people more dependent on the internet generally and social media specifically as the key forum for public debate. Acknowledging this does not, however, excuse the malicious intent of those – particularly state officials and politicians – who engage in online harassment and hate-fuelled commentary.

In particularly fragile democracies, state-of-the-art technology is being used not only

to improve the lives of citizens but to control society, especially organisations and individuals vocal in their criticism of democratic backsliding.

Moreover, the consequences of these negative trends and tendencies will continue to severely affect civil liberties by spreading fear, especially among marginalised groups, which inevitably leads to curbs on guaranteed freedoms and rights and increases the risk of exploitation and violence, which can be easily transferred from the virtual world to real life.

Big companies and relevant stakeholders have to increase the level of understanding and sensitivity towards these complex and worrying trends. Protection mechanisms are poor and those that exist need to be brought closer to the general public in language it can comprehend.

The report findings acknowledge the need for legislative, political and social change within the monitored countries. However, digital evolution must be seen as a set of mechanisms and tools that have great potential to serve the needs of the people. The COVID-19 pandemic has proved internet access is indispensable in times of crisis.

Our societies are becoming ever more digital and this represents a powerful incentive to increase the capacity of organisations dealing with digital development and regulations in Southeast Europe.

Without accountability, democratic norms will continue to be undermined and space for non-hostile debate will shrink yet more, further endangering of human rights and online safety. While free speech must be protected, the lack of accountability for discriminatory content and hate speech will make upholding democracy hugely challenging. Failing to ensure access to fact-checked information, providing online education rather than feeding misinformation poses an equal threat to democracy.

Defining digital rights and responsibilities, educating people about then defending those rights and responsibilities is the only way to continue making inroads towards creating long-lasting, progressive, open and tolerant societies.

BIRN and the SHARE Foundation recognise the need for a more coherent, cross sector approach in addressing the range of digital rights challenges that have become particularly visible during the COVID-19 pandemic, as the use of fast-evolving, advanced technologies, online violations and privacy breaches pose serious concerns.

Bosnia and Herzegovina

Fact sheet

Total number of cases verified by BIRN and the SHARE Foundation between 1 August 2019 and 30 November 2020: **94**

Number of verified incidents by month:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	Ma 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
8	11	4	3	5	6	6	7	12	8	5	6	3	4	2	4

The most common violations by category

1. Pressures because of expression and activities on the internet: **39**
2. Manipulation and propaganda in the digital environment: **27**
3. Information security breaches: **18**

The most common subcategories of violations

1. Other manipulations in the digital environment: **19**
2. Threatening content and endangering of security: **17**
3. Publishing falsehoods and unverified information with the intention to damage reputation: **17**
4. Other violations: **14**
5. Computer fraud: **10**

The most frequently targeted parties

1. Citizens: **62**
2. Public persons: **10**
3. Online media: **5**
4. State official: **8**
5. Political party: 5 and private company: **5**

The most common attackers

1. Citizens: **39**
2. Online media: **22**
3. Unknown: **23**
4. State institution: **6**
5. Blogger: **2**

Featured cases

Biased reporting, fake news and digital content denigrating ethnic groups, women and LGBT+ communities dominate the digital space in Bosnia and Herzegovina (BiH). Still bitterly divided, BiH is run by a highly complex and multi-layered government structure set up to manage ethnic tensions unleashed during the devastating 1992-5 war.

The three largest ethnic groups – Bosniak (Bosnian Muslim), Serb and Croat – are represented within two separate entities (the Federation of BiH and Serb-majority Republika Srpska), one semi-autonomous district (Brčko) and 10 local government cantons in the Federation of BiH.

Widespread inter-ethnic discord, anti-liberalism and a lack of trust in public institutions and government have been further stoked and exploited during the COVID-19 health crisis and the local elections of November 2020 – provoking a storm of biased, fake and hate-fuelled news coverage and social media content.

Biased reporting and fake news

Manipulation and propaganda flourished in Bosnia and Herzegovina; one of the [most divided countries in the monitored region](#). Fake news dominates traditional and online media in BiH, with the fact-checking website [raskrinkavanje.ba](#) finding new examples on an almost daily basis. Fake and biased reports are published to instil fear of other ethnicities, stir up hatred and reinforce the message that only particular political parties will protect “their own”.

Just a few weeks before polling day, news portal [banjaluka.net](#) published [an article](#) claiming it had evidence a group of Bosniak Salafists were plotting to assassinate both Milorad Dodik, the Serb member of Bosnia’s tripartite presidency, and the Serbian President, Aleksandar Vucic.

The story was fake but many other outlets had already republished the article - attracting numerous comments and shares among readers - by the time Raskrinkavanje had established it was a false conspiracy theory. Banjaluka.net, a keen supporter of Dodik’s Alliance of Independent Social Democrats party (SNSD) , later published [a correction stating the story was wrong and apologised to its readership](#). However, the uncorrected story is still available on the website of Serbia’s [oldest mainstream newspapers Politika](#).

Our monitoring shows that fake news stories were published by 14 different news

outlets. These false stories included incorrect reports that Bosnian politician Fahrudin Radončić had been arrested, that migrants were found in possession of explosive devices and various falsehoods about some politicians' private lives and COVID-19. A [pledge to ban LGBT+ parades](#) purportedly tweeted by the newly-elected head of Sarajevo's Ilidža canton, Nermin Muzur, was later proven to be false. Muzur wrote on his Instagram account that the Twitter profile was fake and then set up his own official Twitter profile. The author(s) of the fake profile is still unknown.

Free but irresponsible speech

Women, LGBT+ communities, migrants and acutely vulnerable minority groups such as Roma are all freely and frequently abused by voters and their elected representatives – deepening divisions and fuelling intolerance.

In a televised debate on FACE TV broadcast in February 2021, SDP politician Vojin Mijatović belittled his debate opponent, Our Party member Sabina Ćudić, accusing her of “screaming” her words - thereby insinuating she was a hysterical woman.

BIRN and SHARE Foundation researchers have seen a significant uptick in online hate speech [against migrants](#) among the press and public in BiH since August 2019, with content falsely accusing migrants of committing large numbers of crimes including rape and assault and also publicly vilifying activists working with migrants as “delusional communists”.

COVID-19 inspired numerous [fake news stories](#) including [dubious cures](#), conspiracies theories linking the pandemic to [5G networks](#) and a “[mysterious powder](#)” sprayed from planes.

While politicians might be expected to be fully aware that freedom of expression must be accompanied by responsibility for publishing facts and legitimate opinion, the same sophisticated understanding of digital rights and responsibilities cannot be assumed among the general public.

In July 2020, a [man was arrested](#) for publishing racist and antisemitic threats on different online platforms and communications channels. He was also charged with public calls for acts of terror.

Cyberattacks further undermine trust

Alongside the usual incidents of online fraud and phishing scams, there were two serious cyberattacks targeting government online services.

In June 2020, Sarajevo's Centar canton [issued a statement](#) explaining their archive - containing residents' personal data such as residency status, addresses etc. - had been hacked "by a virus that locks documents". The municipality apologised for the suspension of services such as obtaining public records including copies of birth certificates. While the problem was resolved a few days later there has not been any investigation and it remains unknown if confidential data was stolen.

In August there were three more [hacking attempts](#) to illegally access public records held by municipal offices in Sarajevo Centar, Bihać and Lukavac cantons. The primary goal of these attacks seems to have been to disable access to the public records database but the cantons have not said whether data was accessed and/or stolen and there has been no information on whether the attacks were separate or simultaneous.

In the absence of robust security measures to protect the public's data and ensure delivery of secure e-services, breaches of these kind only add to the pervading sense that public institutions and the government cannot be trusted to provide secure e-services.

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

Fake News Thrives Amid Pandemic and Migrant Crisis

By Dalio Sijah from the government/political communications monitoring NGO [Istinomjer.ba](#) and Maida Salkanovic from media fact-checking platform [Raskrinkavanje.ba](#)

At the very heart of Bosnia-Herzegovina's numerous challenges – alleged election fraud, simmering inter-ethnic distrust and discord, the ongoing migrant crisis and corruption, to name but a few – lie irresponsible and disreputable media outlets churning out large amounts of fake news for political or financial gain.

Some argue the digital sphere merely reflects the offline world but it is also a space where political and social events are commented on, shaped and even entirely invented – courtesy of fake news, biased reporting and hate-fuelled opinion pieces.

This type of online content has shaped public perception of numerous issues, including provoking vociferous anti-migrant sentiment to the extent that widespread public

sympathy has now turned to fear and contempt. The emotions news outlets (real or fake) stir up are inevitably amplified by citizens on their own social networks.

While the targets differ, one thing all these platforms including well-established media, fake media, anonymous and individual social accounts have in common is a total lack of accountability for inciting violence, hatred and spreading misinformation.

Media whips up migrant storm

BiH has been a transit country for migrants and refugees hoping to reach wealthier European nations since the crisis first began in 2015. According to the [Service for Foreigners' Affairs](#), more than 6,000 migrants are currently staying in overcrowded reception centres with most staying in Una-Sana canton (which borders EU-member Croatia).

On August 29, anti-migrant protests erupted in Una-Sana amid allegations that migrants were criminals and posed a threat to security. Well-known local councillor Sej Ramić helped organise the protest, telling the media that migrants had committed a total of 4,000 crimes in the area.

Addressing the protesters, Ramić also invited migrants to leave the country in the English language with the words: "Migrants go home!"

At the end of July this year, however, the cantonal government issued a report stating that crime had fallen in the first half of 2020. Istinomjer analysis of data going back to 2018 shows the claim of 4,000 crimes is unfounded as migrants were linked to just under 300 crimes during 2018 and 2019.

Similar allegations were made by other government officials in other parts of the country, despite there being no basis for these accusations. Not only are such false claims very often reported by domestic media as fact without any evidence whatsoever, many outlets have adopted openly hostile anti-migrant rhetoric.

Fake news, voting and COVID-19

The local elections and Coronavirus generated an extraordinary amount of fake news – serving only to further undermine confidence in democratic processes, politicians and journalists (including those of deservedly good repute).

During campaigning, fake news featuring candidates appeared on media outlets and social networks [to discredit and ridicule them](#). As is always the case before elections, there was a surge in anonymous online media outlets promoting policies put forward

by particular parties or politicians.

Political bots (automated programs influencing the direction of debate on social media) and astroturfers (fake profiles falsely promoting particular viewpoints as politically independent) contributed to misleading the public about the accomplishments of certain political options. [Some examples](#) can be found in analysis conducted by Raskrinkavanje in 2018, including the leaking of a document by the nationalist party SDA in which they promoted [recruitment for astroturfer positions](#).

Insults were thrown around lightly, greatly diminishing the quality of political and public debate. There was certainly no lack of rhetoric referencing the horrific events of the 1992-5 war to stoke fears of renewed violence and ram home the message that only particular parties would protect particular groups.

Lack of regulation in campaigning and media reporting plus little transparency of media ownership has allowed the unscrupulous to take advantage of low levels of media and digital literacy to promote nationalist political agendas that stymie progress by keeping the population in constant fear of conflict.

There were [several cases](#) of elected officials spreading fake news that played into conspiracy theories surrounding COVID-19, including claims that the virus is a lie motivated by financial gain or that it is caused by the 5G network. Elected officials, with certain influence over their constituents, used their position to spread unverified information with potentially damaging consequences. Many public figures and the media offered their alleged "cures" for COVID-19, which proved to be dangerous in an environment where trust in the public health system is already seriously shaken.

Chilling effect of hate speech

Unchecked online comments that often include hate speech are a good reminder that the democratisation of the online public space is not always a positive thing.

Even though some surveys, including a [famous 2016 survey by the Guardian newspaper](#), show that this type of online harassment has a detrimental effect on the journalists experiencing it - including self-censorship, health issues, increased anxiety and in some cases also the decision to leave journalism - this is still not taken seriously in Bosnia-Herzegovina.

Cultural expectations of stoicism contribute to journalists' hesitancy to raise these issues, together with the lack of support networks or mechanisms that would help deal with this issue, which, even when reported to the authorities, are rarely resolved. Women are disproportionately affected by this phenomenon, keeping the online

public space predominantly male through intimidation.

Without wishing to stifle genuine freedom of expression or stray into online censorship, democracy in the Bosnian context cannot be protected without enforceable legislation that ensures public figures, the media and individuals are held to account in the online public sphere.

This is especially important in an environment such as Bosnia-Herzegovina, where the wounds of the recent war have not yet healed and are actively exploited to advance certain political goals and agendas.

Croatia

Fact Sheet

Total number of cases verified by BIRN and the SHARE Foundation between 1 August 2019 and 30 November 2020: **161**

Number of verified incidents by month:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	Ma 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
7	8	9	5	10	11	8	18	13	8	8	8	9	9	16	14

The most common violations by category

1. Pressures because of expression and activities on the internet: **70**
2. Manipulation and propaganda in the digital environment: **66**
3. Information privacy and personal data breaches: **22**

The most common violations by subcategory

1. Other manipulations in the digital environment: **52**
2. Hate speech and discrimination: **33**
3. Publishing falsehoods and unverified information with the intention to damage reputation: **25**
4. Computer fraud: **22**
5. Creating fake accounts and paid promotion of false content: **13**

The most frequently targeted parties

1. Citizens: **120**
2. Journalists: **16**
3. Public persons: **13**
4. Online media: **10**
5. State official: **10**

The most common attackers

1. Citizens: **71**
2. Unknown: **40**
3. Online media: **35**
4. Public persons: **10**
5. State official: **10**

Featured cases

Hate speech and anti-migrant sentiment

Inflammatory anti-migrant content on known media outlets, anonymous platforms and individual profiles accounted for the majority of digital rights violations we verified in EU-member state Croatia. Right-wing media outlets repeatedly published and recycled stories portraying refugees and migrants as violent and dangerous criminals while often calling for open intolerance towards them.

[One article referred to us was published](#) on konzerva.hr under the headline Turkey has proven that refugees are weapons, so treat them like that. It claimed that Europe has already allowed in “hordes” of migrants, resulting in rapes, bombings and public attacks on the streets. The Croatian website kamenjar.com [published an article](#) insisting migrants and refugees living on the border with BiH were carrying out an “invasion” of Croatia while using highly negative racial and ethnic slurs. A couple of days later, sloboda.hr [followed up with a piece](#) in which they referred to migrants and refugees as a “well-organised army”.

Our data corroborates reports of border officials refusing entry to migrants. Accusations of police violence have sharply increased. [Testimonies from migrants](#) crossing to Croatia were collected by the Danish Refugee Council complete with explicit photos of brutal beatings that were attributed to Croatian border police officers. The head of home affairs for the European Commission also said that she was taking the allegations “very seriously”. The Border Violence Monitoring Network [submitted a report](#) to the UN Human Rights Office about the increasing role of technology in illegal pushbacks from Croatia to Bosnia and Herzegovina and Serbia in 2020.

Some politicians helped peddle conspiracy theories about refugees and migrant workers. Ivan Pernar, a former MP and founding member of the Party of Ivan Pernar, used his [Facebook account](#) to claim migration would result in “population structure change”; an apparent reference to the Great Replacement theory, which contends migrants will oust white workers in European nations.

Tomislav Majnaric, a member of the right-wing Croatian Party of Rights, shared a video inciting intolerance of migrants and refugees passing through the mountainous region of Gorski Kotar. Dressed as a mountaineer, he described migrants and refugees as “Talibans” (Islamic fundamentalist nationalists) who are armed and warned his followers not to come “unprepared” or “empty-handed” to Gorski Kotar.

Fake news, phoney profiles and doctored photos

Tensions between the dominant Croat population and ethnic Serbs always increase before elections and the 2020 presidential vote was no exception, with right-wingers in particular trying to denounce politicians by highlighting ties to Serbs or deflect criticism of themselves by engaging in anti-Serb rhetoric and/or slanging matches.

Željko Sačić, a right-wing Croatian MP from the Homeland Movement party attacked Novosti, a weekly paper for ethnic Serbs, after it reported that Sačić had once been a member of the former ruling League of Communists of Yugoslavia. Sačić [attacked the paper on Facebook](#), calling them “criminal anti-Croat bastards” and “Greater Serbia Chetniks” – a highly insulting term.

The presidential election held in December 2020 saw doctored photographs designed to compromise politicians shared online and the creation of fake social media accounts set up in the name of known politicians carrying content intended to defame or undermine them.

One widely-shared [doctored photograph](#) “showed” centre-left Social Democrat presidential candidate Zoran Milanović holding three fingers in the air (a common Serbian nationalist salute) – created to spark controversy among voters and persuade them his alleged closeness to Serbia would render him not patriotic enough to assume the highest office. Milanović won the election.

Similarly, a fake Facebook profile for a member of the Social Democratic Party (SDP) was discovered pledging support for a rival candidate in the election. Fake photos portraying Croatian MP Anja Šimpraga (a member of the Serb minority in parliament) as a Serb nationalist sympathiser [were widely shared on social media](#). The profile was taken down.

In another incident one police officer [falsely claimed](#) that Zagreb Deputy State Attorney Gordana Knaus raised a Serbian flag on a mountaineering expedition allegedly organised by Serbian war veterans and a doctored photograph [was shared on Facebook](#). All of the incidents described above were proven to be fake by the fact-checking website Faktograf, which was picked up by BIRN and SHARE Foundation monitors.

Online death threats and harassment

Death threats against Croatian Prime Minister Andrej Plenković were shared on social media, leading to criminal charges being brought against the individual who posted them.

Journalists were a common target of online harassment and attacks, including social media group Family and Homeland - Us Croats that [called for the lynching of Živana Šušak Živković](#), a reporter from Dalmatinski news portal. Živković was verbally and physically attacked and suffered minor injuries while covering an illegal gathering of worshipers outside a local church on Easter Sunday mass. Her phone was also confiscated and broken. The gathering had been banned as a precautionary measure against the coronavirus pandemic.

Also, the fact-checking website Faktograf was targeted by several websites and politicians for their work in debunking fake news reports related to the COVID-19 pandemic. The website was accused of being biased in their investigations and censoring [certain news](#). Upset that the fact-checking website Faktograf is authorised to detect fake news on Facebook, the right-wing website [HOP reported](#) that Faktograf obtained this authority thanks to two Serbian journalists, Milica Saric from CINS and Ivana Jeremic from BIRN. HOP claims journalists from Serbia influence Faktograf, which they call a “non-objective team”. In right-wing circles in Croatia, a common way to discredit someone is to highlight or emphasise real or alleged connections with Serbia.

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

COVID-19 and the Anti-Vaxxers: Social Network Paranoia on the Streets

By Oriana Ivković Novokmet, Croatian democracy watchdog GONG

In September 2020, the COVID-19 denying conspiracy theories that had flooded Facebook overflowed onto Croatian streets. Disinformation arrived by the busload in Zagreb as [singing antivax protesters piled outside several old people's homes](#) reassuring old ladies, the most vulnerable group of all, that COVID-19 [wasn't such a terrible virus](#) after all and that they were being needlessly imprisoned. Thousands of protesters gathered in the nearby main square, carrying banners declaring: "Vaccinate your mum, you're not jabbing me."

In October, [anti-maskers verbally abused Alemka Markotić](#), the director of the Infectious Diseases Hospital, and an N1 News channel crew during an on-air interview filmed in Zagreb, "These are marginal characters," the doctor commented on air.

Later, a group of anti-maskers held a wake for her outside her home, complete with candles and a banner bearing the words: "The Margins".

The pandemic had barely knocked on the door in Croatia at this time and Prime Minister Andrej Plenković didn't hesitate in boasting that his government had beat the virus. His centre-right Croatian Democratic Union regained power during the July general election, which attracted the lowest turnout in the history of Croatian democracy.

However, by mid-December the rate of new infections saw Croatia ranked worst in Europe and the daily death toll came perilously close to 100. Many Croats clearly understood the government had not only demonstrably failed to beat Coronavirus but had in fact contributed to spreading the disease through miscalculations and inconsistent messaging. Allowing the annual remembrance procession for the victims of the 1991 siege of Vukovar to go ahead – attended by thousands – was seen as pandering to Roman Catholic church leaders and war veterans.

Anti-Vaxxers

While we waited for vaccines to come to Croatia, resistance to vaccines had grown thanks in large part to wild conspiracy theories that are no longer restricted to a narrow audience in the dark corners of the internet. The thousands of anti-vaxxers marching through the streets of Zagreb and Rijeka testify to this.

Some surveys suggest almost half of Croatia's 4.1m population do not want the jab. According to a survey conducted on a representative sample for a TV network, 18 per cent of Croats believe the vaccines contain microchips.

When the vaccine finally arrived in Croatia, citizens learned that many public officials, as well as the powerful and rich, were vaccinated in secret, outside the regulations. Although the public was given the impression that interest in vaccination had increased, citizens, who are mostly offered the AstraZeneca vaccine, believe it to be of lower quality, giving the anti-vaccination movement another boost.

Anti-vaxxers also enjoy the support of certain right-wing politicians, renegade scientists, flamboyant nutritionists, the odd concerned parent and sections of the Catholic Church.

A video containing false information about COVID-19 vaccines recorded by the student chaplain of the Archdiocese of Rijeka, Ivan Dominik Ilicic, went viral on social media. The priest said vaccines like Pfizer's or Moderna's could affect the genetic code of the recipient. To his followers, he is the standard-bearer of truth, who isn't

in the pay of Satanists, various Soroses, Gateses and similar knaves. Jesus is their vaccine and they need no "Satanist rubbish". His Facebook account has 73,000 followers.

Throughout the pandemic Faktograf, the only Croatian media outlet that specialises in fact-checking, has so far published more than 300 texts as part of its fight against disinformation. Websites espousing conspiracy theories and social networks are at the forefront of the spread of falsehoods and half-truths.

A book blogger with 500,000 followers - until recently celebrated for her championing of entrepreneurship and spreading positive vibes - bragged about telling off the taxi driver who asked her to put on her mask as he lived with his 80-year-old father. Her reply was that she failed to see the connection between her refusal to wear a mask and his father, triumphantly concluding that, although trembling, he did drive her to her destination.

Social networks have opened the door to and amplified the voice of the margins, who have now entered the mainstream. It is not hard to spot the link between social media platforms and the increasing influence of anti-maskers. Online paranoias have migrated onto the streets where people protest because "there is no virus" and "mask-wearing is unnecessary" because masks are merely "muzzles forced on people". The regulations mandating mask-wearing are "a rights violation".

A Reddit comment under the heading "Mask Equals Muzzle" which noted that whatever an American fool spouts a Croatian fool will spout a week later, also testifies to the power of the social media machine in perpetuating antivaxxer narratives.

Turning back the tide of lies

It won't be easy to put a stop to the lies and half-truths that grew and flourished on Facebook and other social media networks. This is not a job solely for fact-checkers or indeed regulators. Investing in education in place of persistently undervaluing it might produce results, but that is a long-term affair.

Citizenship education, including media literacy, and support for high-quality and independent journalism are vital if we are to defend democracy and democratic values. In a country where the government often relies on conservative, right-wing values and opposes the introduction of citizenship education in curricula, it is important to stress that the majority of the population do not possess the knowledge and tools that would enable them to consume media content critically – including articles on news sites and posts on social networks.

During times of crisis and isolation, radical attitudes are normalised and extreme reactions and behaviours justified. Clusters of new world-views are created online but are not contained there – they then manifest in “real life”. The interlinking of clusters by sharing views and content increases the effect and reach of conspiracy theories.

It is therefore necessary to regulate the platforms on which such content is published and disseminated and whose algorithms amplify such content. There is growing criticism of social network business models that profit from skyrocketing advertising revenues thanks to relaxed policies on misinformation peddlers, manipulative advertising and hackers.

Social media seems free to use but it’s clear we have already paid for their services through exposure to hate speech, misuse of personal data, the crisis of democracy, meddling of various malicious actors in elections and referenda. With the spread of antivaxxer propaganda that will hinder the fight against COVID-19, we might also pay – literally – with our lives.

Hungary

Fact sheet

Total number of cases verified by BIRN and the SHARE Foundation between 1 August 2019 and 30 November 2020): **173**

Number of incidents verified by month:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	Ma 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
7	17	11	9	10	10	9	15	12	8	7	7	13	18	7	13

The most common violations by category

1. Pressures because of expression and activities on the internet: **80**
2. Manipulation and propaganda in the digital environment: **52**
3. Information security breaches: **39**

The most common violations by subcategory

1. Publishing falsehoods and unverified information with the intention to damage reputation: **39**
2. Hate speech and discrimination: **38**
3. Computer fraud: **35**
4. Creating fake accounts and paid promotion of false content: **21**
5. Other manipulation in the digital environment: **16**

The most frequently targeted parties

1. Citizens: **126**
2. Political party: **41**
3. State institution: **16**
4. Public persons: **14**
5. State official: **13**

The most common attackers

1. Online media: **61**
2. Unknown: **57**
3. Political party: **23**
4. Citizens: **14**
5. State institution: **11**

Featured cases

It's been a turbulent year in Hungarian politics after multiple recordings and videos showing elected officials and opposition politicians — including right-wing Fidesz party member Zsolt Borkai and opposition candidate Tamas Wittinghoff — participating in lewd and illegal behaviour were leaked to Hungarian media in the run up to the local elections held in October 2019. The recordings, which included footage of yacht parties in which politicians were taking drugs and participating in orgies, [sparked serious accusations against the politicians of bribery, corruption and abuse of power](#). The footage did the rounds in the run-up to the election but then subsequently faded from public interest since the disgraced politicians apologised but didn't abandon their election runs.

In December, just a few weeks after the vote delivered surprise defeats for Prime Minister Viktor Orban's right-wing Fidesz party, a network of clickbait fake news sites that had been operating for years [was exposed by Hungarian media site HVG](#).

These sites masqueraded as news portals but carried no formal statement of ownership (usually found in "about us" pages) and published articles without bylines or cited sources. The websites, [which were found to be connected to the leader of the centre-right Civil Movement party Maria Seres](#) and other affiliated organisations, were used to influence public opinion on political candidates in an effort to secure public funding and had considerable impact since their reach was vast.

Cyberattacks, phishing scams

Our monitoring verified several notable cases of online fraud and [digital security breaches](#) including the [Denial of Service \(DDoS\) attack](#) by Russian, Chinese and Vietnamese hackers on [several Hungarian financial institutions](#), as well as Magyar Telekom in Budapest, [making it one of the largest DDoS attacks of all time](#) in Hungary in terms of both size and complexity. This was just one in a series of cyberattacks that were detected in the country.

Fraudsters found multiple ways to scam the public and some businesses by promising to deliver PPE supplies but failing to ship anything after buyers had transferred the money. Other scams involved selling theatre tickets, mobile phones and grocery store coupons. The government's official coronavirus website was also targeted by hackers and disabled.

Covid-19 and xenophobia

In March, as COVID-19 spread across borders, Hungarian tabloids spread misinformation about the origin of the virus in the country. Unsubstantiated reports of international students from the Middle East bringing the virus into the country as the first cases started appearing were shared by major pro-government newspapers and websites. Some [pro-government news sites spread debunked news](#) that a [Pakistani migrant who refused to self-isolate](#) in Italy led to the spread of the coronavirus. Another pro-government news website, Pesti Srácok peddled [the conspiracy theory](#) that COVID-19 was created in a Chinese laboratory.

These reports were riddled with racist, xenophobic and anti-migrant sentiment. Disinformation and conspiracy theories spread through social media, casting doubt over factually-correct reporting while accusing independent media of spreading fake news and silencing whistle-blowers. Our monitoring has [mapped 38 cases](#) of hate speech and discrimination, out of which 13 were directly targeting migrants and refugees labelling them as dangerous people and blaming them for the spread of the virus in the country.

The Hungarian parliament kept its previous agenda and voted to impose a set of new COVID-19 measures in March 2020. Among other things, the new measures allowed Prime Minister Viktor Orban to [rule by decree](#).

Media freedom further eroded

The media landscape in Hungary is already highly centralised as the number of government watchdog media keeps increasing. Their role as administration mouthpieces is blatantly obvious, with their negative reporting on independent journalists, civil society organisations and minority groups and continued praise for the government. In August, a number of false stories were published by pro-government sites such as Origo, which aimed to discredit the owners of some of the few remaining independent media including HVG and 24.hu.

Radio Free Europe/Radio Liberty recently published series of stories alleging editors at Hungary's state news broadcaster MTI were instructed to effectively ["whitewash the news"](#) in an effort "to please Orban's government".

In July, the establishment continued to tighten its stronghold over the county's media, when Miklos Vaszily, a businessman with close ties to PM Orban [became a major stakeholder](#) in [Index.hu](#), one of Hungary's biggest independent news websites. See the following Hungary op-ed piece for more details.

The action caused the resignations of a large majority of the website's journalists and [major outrage and protests](#). The move was reported by outlets that had once been independent but now operate pretty much as the administration's mouthpiece; an editorial shift that often happened after suffering the same fate as Index.

Transphobia and homophobia

From the outset of monitoring, we have mapped a large number of violations targeting the LGBT+ community in Hungary. The frequency of violations generally intensifies around the time of Pride parades or during public campaigns that promote solidarity and love. In August 2019, [advertisements by Coca-Cola](#) around a music festival in Hungary that promoted gay acceptance prompted many hateful reactions. Billboards bearing the slogan Love is Love featured images of couples in love, including same-sex couples.

Pestisracok.hu, a news portal closely linked to the governing Fidesz party, published an op-ed about the campaign in which the author, László Vésey Kovács, [attacked the campaign as "homosexual propaganda"](#), which he said was abnormal, damaged the young and promoted paedophilia. The article was followed by similar ones in government-friendly media. Fidesz MP István Boldog called for a boycott of Coca-Cola on his Facebook page. András Mészáros, mayor of Érd, posted an anti-gay joke relating to Coca-Cola on his Facebook page. The evangelical church Hit Gyülekezete shared an online petition against the campaign. Far-right party Mi Hazánk (Our Homeland Movement) held demonstrations against the campaign.

In the second week of August, Coca-Cola removed the billboards featuring same-sex couples. The company insisted the move had nothing to do with the anti-LGBT campaign. Meanwhile a 19-year-old female was attacked in the village of Bénye in Pest County. The victim said she was attacked at a fair because she had a rainbow-coloured bag with her.

Public figures also spread homophobic and transphobic content online. After TikTok blocked a video of the Hungarian singer ByeAlex because it featured a gun, the presenter complained on Instagram that TikTok has no problem about 11-year-olds coming out or boys dressing as girls. When asked to apologise, he said it was disgusting to see 11-year-olds kissing others of the same sex and coming out.

In May 2020, Hungary's parliament passed a [law](#) making it impossible for transgender or intersex people [to legally change their gender](#) – putting them at risk of harassment, discrimination and even violence whenever they need to use identity documents.

Students, who have supported transgender rights, were targeted on two occasions by the pro-government Origo outlet. Some far-right, pro-government websites, such as Pesti Srácok, even published a long, homophobic article demanding, among other things, the criminalisation of “gender propaganda” and the “promotion” of homosexuality. At the end of September 2020, a storybook was published that contained re-worked children’s tales, some of which feature heroes who are also LGBT+. After Dóra Dúró, a politician from the far-right Mi Hazánk party, shredded a copy of the book in public, [various homophobic and anti-LGBT+ articles were published in pro-government media.](#)

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

Sex Scandal and COVID-19 Hasten Demise of Digital Freedoms

By Peter Erdelyi, senior editor at news portal 444.hu. Disclaimer: The 444.hu news site was set up by former Index Editor-in-Chief Szabolcs Dull.

Index.hu was more than Hungary's largest independent news portal; it symbolised the brightest hopes of the democratic transition of 1989. Founded in the late 1990s, it gained prominence as free internet spread and Hungary joined the European Union in 2004. At a time when it seemed there was a path ahead toward a western-style liberal democracy and prosperity, Index became synonymous with these ideals.

So when pro-government businessman [Miklos Vaszily bought a large stake](#) in Index’s advertising agency (and therefore its revenue stream) in 2020, it meant more than just the latest restriction of the free, digital media space in Hungary. It meant the dreams of 1989 and the modicum of progress made since then were being undone.

Vaszily - who ran the state media conglomerate MTVA between 2015 and 2019 and oversaw the 2014 [takeover of Index competitor Origo.hu](#) and its subsequent repositioning as a pro-government news outlet – claims he has no interest in exerting editorial control. However, the former Editor-in-Chief Szabolcs Dull says [he was ousted](#) after defending Index’s editorial independence. Staff began to [resign in protest](#).

The ruling right-wing Fidesz party, led by Prime Minister Viktor Orban, has spent years and vast sums of money buying up independent media to replace critical, inde-

pendent reporting with pro-government propaganda dressed up as objective news. But to fully understand [why Index's fate was irreversibly sealed in 2020](#) we have to go back to the 2019 local elections.

A few weeks before the vote, a major sex scandal shook [Fidesz](#). Hidden camera footage of an orgy on a yacht on the Adriatic surfaced, featuring senior Fidesz party member Zsolt Borkai, the mayor of the industrial centre and Fidesz stronghold Győr. He was filmed in the company of Zoltán Rákosfalvy, [a Győr lawyer who was involved in lucrative deals around the city](#).

News outlets including Index, which is read by millions of Hungarians, covered the story in great detail and this probably contributed to some of the surprise defeats Fidesz suffered in the 2019 local elections. The mega-media machine they constructed over the years proved obsolete as news of the video spread like wildfire in the digital space where most of Hungary's independent media operates.

If Fidesz was to further increase its control over the public discourse in Hungary, it had to solidify its position in digital media. Then 2020 came along.

The pandemic left little space in people's minds for issues like media freedom. The first wave of Covid spared Hungary and the [government enjoyed a boost in popularity](#). With the general elections scheduled for 2022, this was a perfect storm of opportunities and incentives and the results are all too familiar: another outlet taken over, except this time it was Hungary's largest digital portal and one of the very last bastions of critical journalism in the country.

Index also operated Hungary's largest open blogging platform used by the most prominent NGOs and civil society groups. After the takeover, many of these – including the highly respected Hungarian Civil Liberties Union and Hungarian Helsinki Committee – chose to leave what is now widely regarded as a biased, pro-government mouthpiece. In the interests of full disclosure, many of these organisations now blog at 444.hu.

Smear campaigns

The ever-growing pro-government media machine is well used to smearing and intimidating real or perceived opponents of the regime. Opposition politicians, civil activists, journalists and basically anyone who dares to publicly criticise the government is considered "fair game".

After a high school student cursed MPs and the president at an anti-government rally [she became the target of a concentrated smear campaign](#), with one prominent

pro-government opinion leader calling her a slut in the media. Another published upskirt photos of her, while others reported on what grades she got in school. She is reported to be considering launching legal action against the news outlets involved.

The frequency and viciousness of such smear attacks has greatly intensified over the last two years.

Access to public information in the digital space has never been more difficult. As the pandemic erupted, the government essentially centralised all related communication. Only the surgeon general and a few select police officers are authorised to speak to the press on COVID-19 issues and they routinely ignore questions put by independent media.

[Freedom of information \(FOI\) legislation was amended](#) to extend deadlines for state institutions to provide answers - rendering FOI requests nigh on useless.

Viewers of the government's daily pandemic broadcast are told that only the official government communication is to be trusted. Independent outlets are often [portrayed as sources of fake news](#) and viewers are constantly reminded that sharing anything other than official government communications could land them in serious trouble.

And it really can.

Not long after [parliament adopted new legislation against "scaremongering"](#), an offence now carrying a possible five-year prison sentence, the police conducted a number of highly publicised raids and [detained two Hungarian men](#) after they criticised the state's COVID-19 response on Facebook.

One shared the number of people sent home from his local hospital after the government ordered healthcare providers to free up space during the first wave of the pandemic in the spring of 2020 and a link to details of an in-car demonstration against these measures.

The other [criticised plans to lift a curfew](#), ironically suggesting the move might be aimed at pensioners who were "a burden on the national budget". He also referred to Orban as "dear leader" and "a dictator" – something he says local police officers were keen to explore in detail.

In the end no charges were brought in either case but the incidents had a massive chilling effect on public debate, with one of the detained men telling reporters he would not openly criticise the government again for fear of police harassment.

Subverting digital rights

Various officials, [including the Justice Minister](#), are increasingly [calling for national regulation](#) of Facebook because the platform occasionally restricts content it deems too hateful – examples of which have often been posted by government-aligned actors.

This is somewhat ironic given Facebook is often criticised for not doing enough to restrict hate speech. But in the Hungarian context the little Facebook does to limit hate speech combined with its independence, sheer size and impact – which can be used by opposition politicians, activists, NGOs and journalists – has irritated the government.

Some of Facebook’s decisions to remove or add cautions to content have been presented as

[“evidence” of a global conspiracy to silence the Hungarian government](#). In 2019, the Hungarian Competition Authority [fined the company an unprecedented 3.63 million euros](#) after ruling it had falsely advertised its services as free. The authority ruled that users pay for Facebook with their data.

Just as the second wave of the pandemic hit Hungary, Fidesz introduced an amendment that [redefines what qualifies as “public funds”](#). From now on many state institutions, foundations and state-owned companies will likely be able to shield their spending from the public eye. The lack of public oversight will create new opportunities for corruption and make it very difficult to track how public funds are used for party political purposes by the government.

In addition, powerful business groups are increasingly using EU General Data Protection Regulation to silence unfavourable coverage of their business activities in the media. The owners of popular drink company Hell Energy [used GDPR to have their names removed from Forbes’ richest Hungarians list](#) despite having received almost 30 million euros in public funds to develop their businesses over the years.

Also, some of the Hungarian courts seem to value privacy over access to public information. The Supreme [Court of Hungary ruled in 2019](#) that Istvan Tiborcz, a recipient of huge amounts of EU funding and Orbán’s billionaire son-in-law, does NOT qualify as a public figure.

Over the past years, public affairs have gradually become the private concern of people with power, and every relevant law, regulation and practice echoes this shift in perspective – leading to Hungary’s reclassification as [a hybrid regime](#) rather than

a democracy by US NGO Freedom House. The changes - including curbs on digital rights and freedoms – have negatively affected the daily lives of millions of Hungarians.

North Macedonia

Fact sheet

Total number of cases verified by BIRN and the SHARE Foundation from 1 August 2019 to 30 November 2020: **122**

Number of incidents verified by month:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	May 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
4	7	7	8	5	8	4	13	10	8	12	11	5	6	9	5

The most common violations by category

1. Manipulation and propaganda in the digital environment: **59**
2. Pressures because of expression and activities on the internet: **50**
3. Information privacy and personal data breaches: **26**

The most common violations by subcategory

1. Other manipulations in the digital environment: **50**
2. Hate speech and discrimination: **25**
3. Publishing falsehoods and unverified information with the intention to damage reputation: **20**
4. Computer fraud: **12**
5. Illegal personal data processing: **10**

The most frequently targeted parties

1. Citizens: **71**
2. State official: **28**
3. State institutions: **18**
4. Political party: **18**
5. Public persons: **14**

The most common attackers

1. Citizens: **51**
2. Unknown: **37**
3. Journalists: **20**
4. Online media: **20**
5. Public persons: **7**

Featured cases

The snap parliamentary elections, [postponed](#) to 15 July 2020 because of COVID-19, generated a large number of rights violations across the internet including cyberattacks and fake and manipulative content on social platforms including Twitter and Facebook.

[The denial of service \(DDoS\) attack on the website of North Macedonia's State Electoral Commission \(DIK\)](#) on polling day delayed the publication of confirmed voting results for three hours. Oliver Derkovski, Chairman of the Electoral Commission, [said](#) the attack did not cast doubt over the legitimacy of the vote as the hack only affected the publication of the results.

However, a technical attack on an election information system could, under some specific circumstances, affect election results and thus this needs to be analysed very carefully. Monitoring findings have seen a rise in the number of [cyberattacks](#) on public institutions and media outlets during the period covered by the report.

At the same time as the DIK DDoS attack, several Macedonian media sites were forced offline, including [TIME.mk](#), the most read news aggregator in the country. Igor Trajkovski, the site founder, [tweeted](#) that their security system was forced to block 3 million IP addresses, adding: "We have never had such a DDoS attack before. Someone paid a lot of money to do this."

[The attack was later claimed by a hacker group](#) calling itself Anonymous Macedonia, which left a [message](#) on the website voicing displeasure with the election process, citing "empty promises from all political parties in this beautiful country".

"We had yet another 'democratic election process' and as we can see, it is the same story repeating every three to four years," the message explained: "It had to be your website because it has the highest number of visitors – no hard feelings."

Almost ten months after the elections the hackers have still not been traced.

Fake profiles, false vote predictions

[A Facebook profile calling for protests against the Electoral Commission over alleged electoral fraud](#), allegedly organised by the Levica Party, gained significant support before and during the election. However, Levica denied it was behind the fake profile on their official Facebook account. In the run-up to election day, [false vote predictions](#) appeared on fake Twitter accounts claiming to be based on the results of early

voting by COVID-19 infected citizens and those in self-isolation.

Various [Facebook](#) and [Twitter](#) accounts [urged voters to cross out the word “North”](#) from the name of the country - Republic of North Macedonia - on their ballots. While seeming innocent enough, doing so would render the ballots invalid and therefore constituted an attempt to deprive people of their vote. This manipulation was inspired by the long-running name dispute with Greece that was [resolved in 2018 following an historical agreement](#) between the two countries. This incident prompted a massive debate on social media platforms as well, with opposition supporters claiming that ruling party supporters had tried to con them.

A particularly bizarre example of fake news during campaigning was the false obituary of [Prime Minister and ruling SDSM party leader Zoran Zaev](#), which [was shared on Facebook](#) via a profile named “Zaev is dead” and contained a doctored image of Zaev with no hair and various insults.

[In another incident](#), Tanja Milevska, Brussels Correspondent of state news agency MIA, was targeted by anonymous users with [hate speech and death threats](#) after she wrote a [tweet](#) asking why Hungarian Prime Minister Viktor Orban had not used North Macedonia’s official name in a speech in which he endorsed the VMRO-DPMNE party ahead of the elections.

Personal data breaches

The uptick in COVID-19 cases also saw a variety of personal data breaches. In April 2020, the country’s Agency for Personal Data Protection filed criminal charges against an unknown perpetrator for publishing citizen’s personal data. The perpetrator [published](#) various lists on social networks of Kumanovo residents suffering from coronavirus, including their names, dates of birth and addresses.

However, the biggest privacy breach in the country that our monitors verified at the beginning of this year when a secret group on Telegram was revealed to have shared [explicit](#) pictures and videos of girls, some of whom were underage, among several thousand users. Some users even posted some girls’ phone numbers and addresses.

Our monitoring has also noted a spike in anti-Bulgarian rhetoric on social media after state officials [announced](#) that Sofia will block North Macedonia’s EU accession bid over the lack of implementation regarding a landmark friendship treaty signed by both sides in 2017.

A rise of hate speech generally, especially on Twitter, has been recorded by our monitors since the beginning of the pandemic. Even some quarantined citizens have been

the [target](#) of online attacks.

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

North Macedonia: Political and Social Unrest Vs. Digital Rights

By Filip Stojanovski, Partnership and Resource Development Director, [Metamorphosis Foundation](#)

Early parliamentary elections were supposed to take place in April but were delayed several times because of COVID-19. They were finally held in mid-July. The public was deprived of an explanation as to why the opposition party VMRO-DPMNE insisted on moving the government proposed polling day from July 7 to July 15, as the week of delay didn't offer any events that would affect the outcome.

None of the political parties put digital rights issues at the forefront of their plans for running the country over the next four years.

The main ruling party, the Social Democratic Union of Macedonia (SDSM), did reference some related issues as part of their commitment to adhere to the standards and systems of the EU and the Digital Agenda for the Western Balkans, as well as the challenge of hybrid war threats in the area of disinformation and cybersecurity.

The campaign of the biggest opposition party, the right-wing VMRO-DPMNE, focused instead on patriotism and tradition, paired with relentless criticism of their political opponents.

The vote was somewhat complicated as both of these parties, as well as ethnic Albanian parties from the government and the opposition, took part in the technical government formed in January, 100 days ahead of the initial election date. This meant that some key ministries, such as internal affairs and labour and social policy, were run by opposition ministers who had to make sure the elections were properly and fairly prepared.

Shared responsibility also involved a blame game campaign for failures and obstructions related to the spread of COVID-19 and other issues, including discord between the health authorities and law enforcement. For instance, the SDSM [blamed](#) VM-

RO-DPMNE for encouraging disrespect for COVID-19 restrictions after Interior Minister Nakje Chulev [stated](#) that he would not yield to pressure to sanction citizens who disrespect them but would rather focus on education.

This populist practice was evident in cases of [police tolerating large religious gatherings](#) without enforcing the law and anti-COVID-19 regulations, as that would alienate worshippers/voters.

Meanwhile, the government response to the health crisis generally did not involve an increased respect for privacy, which is a major concern from a digital rights perspective.

Before 2017, forms of doxxing involving “leaks” of private data from state institutions that were used by media affiliated with the then ruling party to target political opponents, independent journalists and civil society activists were commonplace. The practice has become rarer, which also helped lower the impact of [nationalist media attempts](#) to link the spread of the virus to irresponsible behaviour by members of certain ethnicities/religion and sow further distrust in the system.

The pre-election campaign period coincided with the government campaign to promote a contact tracing mobile phone app called [Stop Korona](#), run by the Ministry of Health, enabling the identification of clusters of infected citizens. The use of this application and voluntary sharing of data was based on the implementation of the EU-compatible Law on Personal Data Protection and favourably [responded to civil society demands](#) for increased transparency through publishing a privacy policy. The app was a donation by a private IT company which refused to publish the code as open source, but examination by experts showed that it has no access to private data within the mobile phones.

Use of the app became heavily politicised, as pro-opposition media outlets and troll armies fell into a pattern of criticising either the decision-making process, the actual measures or their implementation. [Coordinated propaganda discouraged the use of the Stop Korona app](#) by spreading disinformation that it would be used by the ruling party for spying on citizens. A similar disinformation pattern was used in the past to undermine public trust in other government issued apps, such as an app enabling partial VAT returns.

Since the tracing apps only work if they are widely used and their users are willing to share their data, [the disinformation campaign severely affected its effectiveness](#). In the weeks before the elections, the government discontinued the promotional campaign.

Roma: Police brutality allegations provoke racist backlash

Use of the online sphere for hate speech and discrimination remained a major problem during 2020, which is especially corrosive in a multi-ethnic society like North Macedonia.

On one hand, unlike most other Balkan countries, its legal framework is conducive to building social cohesion through acknowledgement of collective rights of ethnic communities, from political representation to use of languages within state institutions. Even the word 'minorities' is shunned both in the language of the laws and daily political discourse, reflecting the notion that some rights should not depend on the quantity of citizens from a certain group.

On the other hand, however, stoking ethnic and religious tensions remains a key weapon in the arsenal of populist politicians. Impunity for criminal behaviour online abets this trend, as public prosecutors and the courts very rarely investigate such cases.

While the main hate speech narratives usually aim to disrupt relations between the most numerous communities, the ethnic Macedonians and ethnic Albanians, Roma remain a favourite target of nationalists too. In particular, online discrimination against Roma serves as a proxy to target government officials who promote efforts aimed at integration. Nationalists from other ethnicities attempt to build on engrained prejudice to support perceptions of pro-Roma stances as equating tolerance for criminal behaviour based on corruption and incompetence.

Occasional alleged incidents of police brutality against Roma, such as [forced removal of a camp below a bridge near Skopje's main train station in early June](#) drew condemnation and demands for justice from Roma representatives and human rights organisations - but they also provoked a backlash of approval for "heavy-handed" police tactics.

One particular example was the campaign against Oliver Spasovski from the SDSM party, who served as prime minister of the technical government ahead of the elections. April 8, International Roma Day is held on 8 April and is an official state holiday in RNM. To mark it, Spasovski published a video with congratulations in the Romani language. Symbolic gestures like this don't usually draw much public attention and are considered a common courtesy.

However, during the weeks before the July elections the video was used to ridicule Spasovski via [numerous derivative clips and memes](#), including some featuring ani-

mations of aliens during first contact situations. Online media shared these clips as examples of fun and many social network users stressed the memes poked fun at Spasovski's diction and not Roma.

Members of the Roma community, however, concluded the memes were belittling to Roma language and culture. Indeed, much of the spread was through private messages via messenger services, which indicates that the perpetrators were aware that publishing them might get them in trouble with the law or at least mark them out as anti-Roma bigots.

The resulting polarisation reached a climax in September after a [video alleged to show police officers beating up ethnic Roma citizens](#) was shared on social media. The Ministry of the Interior immediately announced an internal investigation, Prime Minister Zoran Zaev called it "shameful," while the Helsinki Committee for Human Rights condemned the incident as an example of abuse of police authority.

During the following day, [more eyewitness videos were leaked to the media](#). However, this was followed by the spread of videos allegedly showing "the whole event" claiming that the people beaten by the police deserved it because they attacked the police first. The officers involved were [suspended](#) from duty pending a criminal investigation.

It is hard to estimate the net result of this counter-campaign, which brought together various tendencies, from authoritarian personalities demanding law and order through the militarisation of society, to general attempts to portray the current government's pro-human rights positions as meek or pro-crime.

This mixing of racism and attempts to discredit politicians bears a strong resemblance to the disinformation targeting liberals in the USA, revolving around misconceptions related to the "defund the police" slogan. The goal is to present pro-EU politicians as destroyers of law, order and, in the end, causing an unravelling of the country.

One thing is certain: human rights organisations continue to report incidents of alleged police brutality against Roma such as the beating of a mother and son purportedly by police officers who detained them for not wearing masks or carrying ID. Roma rights groups claimed that the officers taunted the mother and son by asking them to dare video them in an apparent reference to the September incident, raising concerns of [revanchism](#).

The polarisation and intolerance that pervades social networks hinders public debate about actual causes of criminal behaviour perpetrated by members of any ethnicity,

such as socio-economic factors or endemic corruption, therefore directing citizens within their social media bubbles that are primed to focus on ethnic features.

Troll armies fail to whip up protests

Even though there is an informal custom in North Macedonia of allowing each new administration a “grace period” of 100 days before opposition parties start heavily criticising its performance, the VMRO-DPMNE set a precedent in 2020, announcing a series of protests from August, just over a month after the elections.

Confessions by former VMRO-DPMNE officials revealed that the party operates a troll network centred around its communication centre, which produces content that is further spread by party followers on social networks via local committees down to the level of individual members who help out with unauthentic behaviours such as coordinated liking, sharing and commenting.

This troll infrastructure has existed for several years and seems to have received fine-tuning through the consulting services of Russian operatives in 2015, and played a role as promoter of voter apathy through disinformation during the campaign to boycott the consultative referendum of 2018, as noted within the report on disinformation in Western Balkans published by European Parliament. Over the years, certain trolls who control arrays of anonymous profiles or bots were revealed to share or exchange affiliations between VMRO and Levica.

The themes of these protests involved a grab-bag of various issues from pollution to the increase of electricity/utility prices to foreign policy issues, such as alleged betrayal of Macedonian identity and history by the government in its relations with Bulgaria. There have been no leaks from the party about the strategy behind the campaign but to outside observers it seems that the focus is on creating events that keep the media attention on them and the leader, and gloss over the internal discord related to losing the election and other failures.

Given the restrictions on large gatherings imposed due to COVID-19, as well as allegations that election campaign and party meetings fail to enforce mask-wearing and other COVID-19 measures, many of these protests are vehicular, based on the use of columns of cars driving through the capital, or other cities, and then parking for a while in front of government institutions blocking the traffic.

The protests have so far failed to attract even wider party membership. With just a few exceptions, most have had no more than several hundred participants.

Constant criticism and use of disinformation and spin by the opposition has not

helped its cause, since it has not distanced itself sufficiently from the rhetoric of the former PM and party leader Nikola Gruevski, nor has it offered viable alternative solutions to current problems.

The current party leader Hristijan Mickoski has not inspired confidence by stating that they will form a strategy on how to solve problems after the fall of the current government.

Various analysts, and their political opponents, have opined that the point of the uninspired protests is not winning new converts to the party cause, but that they are used as part of an internal conflict for power within the party hierarchy.

Romania

Fact sheet

Total number of cases verified by BIRN and the SHARE Foundation from 1 August 2019 to 30 November 2020: **92**

Number of incidents verified by month:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	Ma 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
4	5	4	5	2	7	5	5	11	8	4	6	7	6	7	6

The most common violations by category

1. Manipulation and propaganda in the digital environment: **47**
2. Pressures because of expression and activities on the internet: **27**
3. Information privacy and personal data breaches: **17**

The most common violations by subcategory

1. Other manipulations in the digital environment: **45**
2. Hate speech and discrimination: **21**
3. Citizens' personal data breaches: **14**
4. Insults and unfounded accusations: **7**
5. Unauthorised access - unauthorised alterations and insertions of content: **6**

The most frequently targeted parties

1. Citizens: **73**
2. State institution: **17**
3. Public persons: **8**
4. State official: **7**
5. Online media: **4**

The most common attackers

1. Citizens: **27**
2. Unknown: **24**
3. State institution: **12**
4. State official: **12**
5. Online media: **10**

Featured cases

High levels of hate speech and false information targeting ethnicity and the LGBT+ community were recorded during the reporting period. In August 2020, [homophobic slurs were used in a smear campaign](#) that saw two videos released that portrayed the reformist USR PLUS alliance as a “party of homosexuals”. USR PLUS believe the Social Democratic Party (PSD) was behind the incident, which occurred in the run up of the 27 September municipal elections.

In June 2020, Romanians protested against the [ban on gender identity studies](#), which was passed without any public debate. The move resembles similar measures imposed by the [Hungarian government against gender studies programmes](#) in 2018 and is regarded as a step towards more blatant discrimination against LGBT+ groups.

In the months before the November presidential election, PSD politicians repeatedly compared Klaus Iohannis – who was re-elected president - to the Nazis because of his German origins. In one such instance, PSD senator Serban Nicolae on 8 August 2019 called Iohannis a “Gauleiter” or Nazi regional leader

Roma and Jewish people most targeted

In April 2020, acclaimed US-Romanian scholar Vladimir Tismaneanu [posted a meme](#) in which he compared Roma people to crows, a known derogatory term. He later apologised on Facebook for the meme. [Read the following op-ed piece for more details.]

Roma populations have historically been [vulnerable to hate speech, discrimination, and disinformation](#), and this has been exacerbated by the pandemic. Almost 40% of hate speech and discrimination cases we verified in Romania targeted Roma people.

Fake online news blaming Roma for the spread of the virus is commonplace, including frequent accusations by politicians. Nicolae Dobrovici-Bacalbasa, a PSD member of parliament, posted the following online: “The Chinese got the virus from bats, we will get it from our crows” – crows again being used in a derogatory sense. This type of hate-fuelled content further isolates a highly-marginalised group who often have no access to health insurance – greatly [increasing their exposure to COVID-19](#).

In the aftermath of the September 2020 municipal polls Ioan Nasleu, a member of Romania’s National Liberal Party and an adviser for the outgoing mayor of Timisoara, [asked in a Facebook post why](#) “all the candidates and so-called winners have Jewish names”. He then declared himself “tired” of President Iohannis and denounced those

he deemed “traitors” and “importers of foreigners”. He went on to attack those who voted German national and freshly-elected mayor of Timisoara, Dominic Fritz, of being “LGBT lovers”. A Romanian antisemitism watchdog called his musings “fascist” and “antisemitic” and demanded the ruling party take measures against him.

Additionally, Radio France International correspondent William Totok and two historians, Mihai Demetriade and Madalin Hodor, [were targeted by anti-Semitic attacks on Facebook](#) after they maintained that prisoners who tortured each other in the Communist-era prison of Pitesti between 1949 and 1951 did not do so on the orders of their jailers but because they were inherently violent, as many of them had belonged to the Fascist Iron Guard movement. Antisemitism is well ingrained in Romanian society. Between 280,000 and 380,000 Romanian and Ukrainian Jews were killed during the Holocaust in territories under Romanian control, and [antisemitic canards are still popular in Romania to this day](#).

Jewish people were the most targeted group in terms of hate speech and intolerance after Roma communities. Our monitoring found that anti-Semitic content accounted for a third of all verified hate speech while anti-Roma rhetoric accounted for 40 per cent of cases.

Corruption and conspiracy theories

On 6 November 2019, four days before the first round of the presidential election, Romanian media reported that the mayor of Slobozia Bradului, a town in eastern Romania, promised to [give priority to constituents](#) who voted for the Social Democratic candidate, Viorica Dancila, in the presidential election on November 10, when assigning 150 houses built by the municipality, during a live broadcast on Facebook. He later apologized for a “regrettable slip”.

While the Romanian authorities used emergency powers [to block a number of websites](#) peddling fake news about Coronavirus, conspiracy theories still gained traction and one post claiming the virus was a global hoax was shared more than 170,000 times on Facebook. The site circulating this information, <http://romania-veche.ro/>, was blocked for spreading fake news, originally collected from a fake Facebook account. Some sites that were blocked simply reposted misinformation and fake news on other online and social platforms.

[Facebook removed dozens of accounts from Facebook and Instagram](#) that were traced back to Romania, with people pretending to be Americans while posting content supporting then incumbent US President Donald Trump in his re-election bid in the 2020 US election. The platform removed the accounts but said it hadn’t estab-

lished whether it was money or ideological affinity that motivated people to create the fake accounts.

Fraud, data theft and vulnerable institutions

Another widespread category of violations involved online fraud. In September 2019, the Romanian [authorities bust the Romanian chapter of Megacart](#), an international crime syndicate that had launched malware attacks against more than 18,000 websites from which they stole the bank details of over 90,000 people over the course of a decade. In some cases, the alleged financial cybercriminals used the name of public institutions to conduct their scams or thefts of data. In April 2020 it was revealed that one such syndicate was sending victims an email claiming to come from the Romanian police. The message urged victims to open an attachment that contained a Trojan virus which took control of their computers. A similar violation was reported on 7 July 2020, when the Romanian and Italian authorities reported the dismantling of a criminal group operating in both countries that committed frauds online amounting to 1.6 million euros.

With many Romanian institutions still failing to observe the most basic cybersecurity precautions, hackers accessed their websites without authorisation on several occasions. [On 3 August 2020](#), hackers took control of the Legal Medicine Institute's website who then displayed a message against the ruling party and called on the public to attend an anti-government protest over the poor response to a recent murder of a teenager. On 17 August, a cyberattack left the authorities without access to a Ministry of Transport system needed to conduct driving tests of more than 150 people in the western city of Timisoara; the tests were subsequently postponed.

Cybercrimes against minors and women

Minors and women have often been the victims of sexual predators or human traffickers. Prosecutors told BIRN that COVID-19 restrictions have forced many criminals to recruit victims online. [On 1 August 2019](#), the authorities arrested a 49-year-old man from Oradea in Northwest Romania for allegedly using a fake Facebook account with photos of a younger, more attractive male to entice a 14-year-old girl into having sex.

On 27 October, 2020, [a 42-year-old Romanian man was sentenced to five years](#) in prison after being caught in April by police in the northern city of Satu Mare while trying to deliver a girl he had sold over Facebook for 400 euros to undercover police officers posing as human traffickers. He had previous convictions for trafficking girls to Italy. This time he used Facebook to tout the victim as Romania was under lock-

down and his contacts abroad were unreachable.

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

Politicians, Pimps, Thieves: Romania's Digital Rights Abusers

By Marcel Gascón Barberá, BIRN

Since starting work on BIRN's monitoring of digital rights programme in August 2019, we have witnessed tensions in the country's ever-turbulent political life - often taking the form of hate speech targeting minorities - continue to spread online.

Some Social Democratic Party (PSD) MPs – now in opposition after losing the parliamentary election in December - have made a habit of comparing centre-right President Klaus Iohannis with the Nazis. Iohannis is of German origin and the abuse has outraged the German embassy and the Jewish community, who regard this as also trivialising the Holocaust.

Attacks on the president increased markedly during election campaigning and Romania has held no fewer than three rounds of elections since August 2019: presidential in November 2019; municipal and regional in September 2020 and parliamentary last December.

Ethnic Germans, ethnic Hungarians, Roma and Jewish communities have all been abused online by various sections of society, including politicians, public figures and the public. Instead of leading the fight against prejudice, some high-profile public figures have used the elections and Coronavirus as launchpads for racist comment.

In April last year, shortly after the south-eastern town of Tandarei was put into lockdown, highly respected US-based Romanian professor Vladimir Tismaneanu posted a meme on Facebook featuring several crows on a wooden fence with the text: "Tandarei Airport. All flights have been cancelled". Tandarei has a sizeable Roma population and the word crow is a commonly-used derogatory term for Roma.

Tismaneanu was fined 1,000 euros (5,000 lei) by the National Council for Combating Discrimination (CNCD). He [successfully appealed](#) the decision arguing that he did not know the ethnic population make up of Tandarei and he was not aware of the

racist connotations of the meme. The court sided with Tismaneanu and scrapped the CNDC ruling.

Veteran journalist Cristian Tudor Popescu called former prime minister and presidential candidate Viorica Dancila a “gipsy” in [a sarcastic online article](#) - published a few days before the presidential election - in which he accused her of begging for votes. Roma minority rights activists condemned the piece but Popescu [denied any anti-Roma sentiment](#).

Similarly, the LGBT+ community are also frequently targeted and the digital space in Romania is awash with homophobic content. Just before the 2020 local election, two highly homophobic videos portrayed the reformist Renew Europe-affiliated USR PLUS alliance as a “party of homosexuals”. [One video featured people dressed in USR PLUS T-shirts](#) wearing wigs and trousers with holes revealing part of the men’s buttocks being booed and chased from a Bucharest neighbourhood.

The PSD itself has also been on the receiving end of online abuse. Its supporters are frequently mocked as backward and unsophisticated among certain circles, with some accusing the intellectual mainstream of sneering at leftist voters. Prominent PSD critic and advertising firm owner Robert Tiderle was [fined 410 euros \(2,000 lei\) for discrimination](#) after posting a job advert explicitly excluding PSD voters from applying.

President Klaus Iohannis was himself fined just over 1,000 euros (5,000 lei) in May last year after accusing PSD of “fighting behind the scenes in parliament to give Transylvania to the Hungarians”. He started [his intervention](#) by wishing “good day” to “Romanians” in Romanian and “Jó Napot Kívánok” (good day in Hungarian) to the PSD.

In 2019, the CNDC imposed fines totalling 76,000 euros (370,000 lei) in relation to off- and online discrimination. Despite this, the overwhelming majority of online hate speech still goes unpunished.

COVID-19, fake news and thieves

Numerous online violations were related to the COVID-19 pandemic. A state of emergency was imposed on 15 March, granting the government exceptional powers which were used to shut down websites peddling fake news about the pandemic considered to endanger public health or security in general.

Determining who should be classified as offender and who as victim has been chal-

lenging in these cases.

On the one hand, websites that had been shut down were clearly producing malicious exaggerations or plain lies aimed at creating fear of the government while dismissing the pandemic as a global conspiracy. On the other, was it legitimate for the government to simply shut down these websites?

Several NGOs and media experts determined this impinged on press freedom as it did not solve the problem but set a dangerous precedent that could be used in the future to silence inconvenient media. BIRN and the SHARE Foundation categorised both the fake news websites and the government as offenders; the former for spreading fake news and the latter for compromising a fundamental freedom.

Romania is a well-known haven for highly-skilled hackers and simple fraudsters alike; both of whom can make a killing by launching malware attacks or conning people into buying non-existent products online, as evidenced by the 18 verified cases of financially motivated cyberattacks and internet scams BIRD identified during the reporting period.

The majority of the cyberattacks included in our database use malware to infect systems with a virus after luring victims into accessing a link. During the pandemic such links pretended to offer useful information to avoid infection or details on government restrictions. Hackers steal data they subsequently use to break into the victims' bank accounts or directly demand money to restore systems they've closed down (also known as ransomware attacks).

Most of the time the perpetrators of these attacks remain unknown – or are not revealed by the authorities. However, successful official investigations and the busting of criminal networks specialising in such offences show that Romanian hackers are a redoubtable force on the international cybercrime scene. We saw a prime example on 19 November 2020 when Romania's anti-mafia agency dismantled a syndicate that specialised in the development and commercialisation of tech that alters malware in order to dodge antivirus programs.

During the monitoring period, cyber-security state bodies have repeatedly called on individual users and institutions to be on guard against these kinds of threats online, noting the limited attention Romanian society gives digital protection.

Because it doesn't require programming skills, traditional fraud carried out online is more common than malware attacks. Our monitoring tells us that fraudsters normally create fake accounts on online commerce platforms where they advertise products.

The victims are told to pay in cash, in advance. The product, of course, is never delivered.

Top-notch Romanian online scammers target victims in more affluent societies where internet commerce habits are more ingrained, like those in Western Europe and North America.

On November 11, Romanian authorities [busted a gang](#) accused of defrauding more than 2,000 victims abroad of about one million euros. Six suspects are now under pre-trial investigation.

Trafficking gangs

Romania is also notorious for gangs trafficking sex workers and is listed as the most common country of origin of trafficked people in the EU, according to several official and civil society reports including [one by the US government](#) and another by the European Commission.

Traffickers seem to be increasingly recruiting online as evidenced by recent police investigations that have shown victims were either seduced by gang members or conned into taking up legitimate-looking fake jobs.

A suspect was arrested last April after police officers posing as interested buyers caught him trying to sell a young woman via Facebook for 400 euros. [The Libertatea newspaper reported](#) in October 2020 that he was sentenced to a five-year jail term. A trafficking ring supplying Western European markets with Romanian sex workers was broken up last November after investigators discovered gang members imprisoned for other offences were enticing girls on Facebook using their mobile phones from their jail cells.

Child sex abuse – including the sharing of indecent images - is another scourge in Romania. Our monitoring suggests most of these crimes are related to the internet in one way or another. Many adults who engage in the production, collection or distribution of such material use Facebook to make contact with victims, convince them to sexually interact with them or demand images of a sexual nature from them. Social networks such as Facebook and others are then used to distribute the content they produce or receive.

The recruitment of police officers and prosecutors specialised in informatics and digital crime is one of the top demands of a network of [Romanian NGOs that are highly critical of official inaction](#) on human trafficking and child abuse – demonstrating the growing relevance of the online sphere for Romanian criminals.

However, to also effectively tackle the impact of fake news and reduce online hate speech – and give the general public a thorough understanding of their digital rights and responsibilities - most experts emphasise the need to educate people.

And a legislature willing to back effective education programmes.

After the right-wing Alliance for the Union of Romanians (AUR) – an amalgamation of religious ultraconservatives, nationalists, anti-vaxxers and those disillusioned with EU and US influence – took seats in parliament for the first time after winning almost 9 per cent of the vote, willingness to tackle these issues remains very much to be seen.

Serbia

Fact sheet

Total number of cases verified by BIRN and the SHARE Foundation between 1 August 2019 and 30 November 2020): **190***

Time period in which the violations were most common:

Aug 19	Sep 19	Oct 19	Nov 19	Dec 19	Jan 20	Feb 20	Mar 20	Apr 20	Ma 20	Jun 20	Jul 20	Aug 20	Sep 20	Oct 20	Nov 20
6	14	12	11	6	13	9	19	23	17	12	11	13	2	9	13

**Monitoring of digital rights began in Serbia in March 2014 and a total of 668 cases have been verified up to 30 November 2020. Only the 190 cases recorded during this reporting period have been included in this country fact sheet.*

The most common violations by category

1. Pressures because of expression and activities on the internet: **109**
2. Manipulation and propaganda in the digital environment: **44**
3. Information security breaches: **25**

The most common violations by subcategory

1. Insults and unfounded accusations: **47**
2. Threatening content and endangering of security: **35**
3. Other manipulation in the digital environment: **32**
4. Publishing falsehoods and unverified information with the intention to damage reputation: **23**
5. Pressures because of publishing information: **23**

The most frequently targeted parties

1. Citizens: **62**
2. Journalists: **60**
3. Online media: **25**
4. Public persons: **14**
5. State official: **9**, Activist: **9**

The most common attackers

1. Citizens: **55**

2. Unknown: **44**
3. Online media: **29**
4. State institution: **21**
5. Political party: **17**

Featured cases

With campaigning for the June 2020 parliamentary elections taking place mainly online, there was a depressingly predictable increase in smear campaigns, verbal abuse and threats against independent media outlets and journalists.

In May 2020 an [anonymous Twitter user](#) threatened BIRN Serbia journalist Slobodan Georgiev, Serbian TV host Ivan Ivanovic and Serbian opposition politicians Dragan Djilas and Bosko Obradovic. According to the Independent Journalists' Association of Serbia, the suspect was promptly arrested.

Originally scheduled in April, the vote was postponed because of the pandemic. However, the ruling party, President Aleksandar Vucic's Serbian Progressive Party, didn't miss the opportunity to dominate campaigning in both advertising content and news coverage. The election saw the country's first online political rally with Vucic addressing his supporters via dozens of television screens. Several opposition parties boycotted the election because they claimed the vote would be unfair.

Under-reported COVID-19 deaths

An investigation by BIRN, published the day after the election, showed [the COVID-19 death toll was more than double the official figure released by the authorities](#). Hundreds more people had tested positive for the virus than was admitted.

In the week before the election, the number of people who became infected was at least 300 per day while the official figure recorded was a maximum of 97 new cases in a single day during that period.

After the elections, when the number of deaths and infections again started to increase, many towns and cities in Serbia announced states of emergency linked to the pandemic. On 7 July, [demonstrators took to the streets of Belgrade](#) to protest against government measures to prevent the spread of COVID-19. The demonstrations lasted several days and spread to other Serbian cities, triggering an unusually violent police response. Social networks were flooded with images and video of police officers beating protesters and using tear gas.

Media freedom watchdogs at home and abroad condemned one incident showing unidentified men [seizing a device](#) from a journalist and deleting recordings he had made. Without common organisers and shared goals, the protests were followed by all sorts of online [misinformation, speculation, manipulations and conspiracy theories about the origins of the protests](#). The confusion sparked more verbal abuse and threats.

The pandemic has led to many data breaches, the [most serious of which was discovered by the SHARE Foundation in April 2020](#). Login credentials for Serbia's COVID-19 information system giving access to confidential patient health data were publicly available on the website of a health institution for eight days. SHARE Foundation researchers stumbled on the page while searching for information about the new legal framework for personal data processing in response to the pandemic. The relevant state authorities were notified and further access was disabled promptly.

In mid-November 2020, unknown person(s) came into possession of a picture of a secretly photographed female patient getting undressed while changing in one of the COVID-19 hospitals in Belgrade. The woman was changing in her cubicle, since patients are separated in COVID hospitals. The picture was taken from above, and secretly focused on her breasts. A set of infusions next to the patient's bed is also captured. A Twitter user shared the photo on his Twitter profile with the caption: "The better side of Covid". When the photo went viral, the user deleted the post, but the screenshot can have been saved by anyone who accessed it.

Migrants and LGBT+ communities targeted

Migrants featured heavily in online hate speech during the reporting period. In February 2020, right-wing opposition party Dveri published a [YouTube video](#) in which their leader illustrated an anti-immigrant theory on mixed populations by mixing clear and dirty water.

The same month, a Facebook group called for anti-migrant protests under the banner ["United Citizens of Subotica"](#) after sharing an edited video showing migrants rioting which presented them as terrorists. The video had since been removed from YouTube and Vimeo.

In April, Vestinet.rs and Pravda-esque websites published a series of [anti-immigrant articles](#), recirculating already debunked allegations that migrants "are being smuggled" into Serbia and "given Serbian citizenship like candy". Facebook was used to live stream a [racist attack](#) on a migrant centre in May last year.

The annual Pride parade sees a sharp rise in off- and online homophobic rhetoric in Serbia. After the September 2020 parade was cancelled because of COVID-19, false rumours circulated claiming a parade was to be held in Leskovac, Southern Serbia. These were accompanied by calls for violence against the LGBT+ population shared on social media. [A large group of high school students protested – some violently – against the LGBT+ community.](#) Eggs were thrown at the police securing the protest, gay slurs were shouted and one reporter was physically attacked.

Algorithms block legitimate content

While there is much to write about the government's control of media outlets and the news agenda generally, our [monitoring findings](#) show that seven out of eight cases of algorithmic blocking of accounts or content have involved civil society organisations, media outlets and individual journalists. All mapped cases occurred in September 2019.

Two BIRN videos were temporarily removed from YouTube over alleged breach of privacy. Daily newspaper Danas's Twitter account was blocked for seven days because the account launch date was incorrectly interpreted as a date of birth. Twitter informed Danas that the account was blocked because it violated rules about the minimum age of Twitter users (18 and over). As soon as the misunderstanding was cleared up, the account was re-enabled.

Facebook disabled the link to a statement by the Autonomous Women's Center, making it impossible to share. The statement was about the Belgrade Court of Appeals verdict in the case of the rape of a Roma girl which was deemed to violate Facebook's standards.

A lack of accountability among big tech companies and platforms remains a huge issue in the region. Removing content and blocking accounts by mistake leaves organisations waiting for these companies to get back to them, which often takes a lot of time while their readership is left with limited access to these media on online platforms.

In terms of cyberattacks, there were only a few [technical attacks](#) over the reporting period, including the June 2020 attack on regional TV station N1's mobile app and website, which were both rendered unavailable following an unusually large number of access requests. N1's website had previously been targeted in January the same year.

Finally, the contested introduction of a mass biometric surveillance system in Belgrade remains a looming threat to rights and freedoms. There is considerable [con-](#)

[cern](#) over the lack of public debate on whether such an intrusive system should be installed, contradictory official statements and the fact the cost and terms of the deal with Huawei - the Chinese firm contracted to install the system – have still not been made public.

All featured cases can be accessed through the SHARE Monitoring database; further information on affected parties, attackers, means of attack, dates, and outcomes can all be found at <https://hu.bird.tools/>.

Op-ed

Serbian Voters Bombarded with Pro-Government Messaging

By Milica Jovanovic, the SHARE Foundation

After a series of seemingly [unnecessary snap](#) elections, [the parliamentary vote](#) scheduled for 26 April 2020 would have been the first regular ballot held in the past eight years.

But with Serbia plummeting down various global human rights and political freedom indexes to the point where [a 2020 report](#) by American NGO Freedom House classified the country as “a hybrid regime” that is [no longer a democracy](#), some opposition parties pledged to boycott the vote. President Aleksandar Vucic’s ruling SNS party, however, wasn’t deterred. Even as a global health crisis loomed.

About a week before the first COVID-19 case was recorded on 6 March, scientists appeared at government-sponsored events to reassure the public that COVID-19 posed no great threat to Serbia. Indeed, at one such event on 26 February 2020, renowned paediatric pulmonologist Branimir Nestorović joined President Vucic at a press briefing and joked that women were [“especially resistant” to Coronavirus “because of oestrogen”](#) and that they “could do their fashion shopping in Milan [Italy]” – where the virus was raging at that time.

Nine days after that first COVID-19 case, the government performed an abrupt U-turn and declared a [state of emergency](#). Election campaigning was suspended the next day, followed by some of the [strictest restrictions](#) in the world, including week-end-long curfews, lockdowns and the suspension of parliament.

Critics including the Lawyers’ Committee for Human Rights, decried the declaration of a state of emergency as heavy-handed and [potentially unconstitutional](#), with some commentators wryly observing the change of tune over the threat posed by

COVID-19 only happened after the SNS had collected the necessary signatures for its election candidate lists.

Campaigning by stealth

And while election campaigning had been halted there was no such let up of state officials appearing at daily media briefings to tell the public all about the authorities' success in managing the crisis and purchasing medical equipment.

The SNS party's omnipresence was echoed in the digital space in the form of an extraordinary amount of pro-government messaging. In early April [Twitter revealed](#) it had deleted 8,558 accounts after identifying in late 2019 clusters of accounts engaged in "inauthentic coordinated activity" to promote the ruling party and its leader in Serbia.

[Analysis](#) published soon after by the Stanford University Internet Observatory revealed that within a couple of years these accounts had produced or multiplied tens of millions of tweets. In more than 95 per cent of cases, their role was to spam the platform with praise for the ruling party and especially of its leader, while increasing the ranking of official party Twitter accounts.

While deleting these accounts didn't put an end to pro-government messaging masquerading as genuine public opinion (astroturfing), it did provide rare proof from an independent and reliable source that the online space in Serbia has been strategically captured in favour of the ruling party and its agenda.

While exact figures for social media advertising are not necessarily given in the required disclosure of campaign funds, [political ads](#) run on social media, particularly adversarial campaigns on Facebook, usually targeting journalists, human rights activists and prominent figures in academia or the arts who voice dissent. Pro-government messaging regularly denounces critics as unpatriotic traitors who are in the pockets of unnamed but malicious foreign actors.

Gag orders and information control

An unpleasant side-effect of this monopoly on national media coverage was that displeasing questions from independent media about the impact of the virus, the state's response and claims state officials were using their position to unofficially campaign and muster voter support got significant public attention. A problem the ruling party soon solved by [removing journalists](#) from press conferences altogether.

At the end of March 2020, the government [took steps to further control](#) the flow

of information about the pandemic by issuing a gag order on local authorities and healthcare institutions preventing them from releasing any information related to COVID-19. A couple of days later a journalist was arrested after she published a story about a shortage of basic medical equipment for hospital staff at the Clinical Centre of Vojvodina. Her devices were seized by the police. No charges were brought against her and the gag order was revoked on 2 April last year.

The government has steadfastly refused to release information to journalists or the public about the number of ventilators it had, how many it would buy and where they could be bought. The same goes for vaccines with Vucic himself chiding journalists for asking such questions.

Similarly, the government has refused to comment on how information held about patients who had been tested for, hospitalised or died of COVID-19 – and that of their contacts – could be accessed after a login username and password for the state COVID-19 Information System were publicly available on a health institutions webpage for eight days. Long enough for the page to be indexed by Google and found via a simple search.

The same COVID-19 database would later confirm suspicions that the true number of people who died from the virus was more than double the official death toll and that the number of infections reported at official briefings was significantly lower than the actual number of cases.

Mainstream media ignored the revelations - which were only reported by a few independent media outlets and on social media. Instead of responding to requests for an explanation of why government figures were much lower for COVID-19 infections and deaths, state officials and pro-government tabloids chose instead to target journalists and media organisations that ran the story, painting them out to be traitors in the pay of foreign powers, opposition parties or even warring criminal gangs.

Opposition stifled

In early May, an unofficial victory over the virus was proclaimed by the pro-government tabloid press, the state of emergency was lifted and the campaign resumed with the election date set for 21 June 2020 – giving candidates just one day more than the legal minimum of 45 days to start campaigning while complying with social distancing requirements and other COVID-19 restrictions.

The ruling party continued to dominate media coverage during campaigning and the OSCE Office for Democratic Institutions and Human Rights (ODIHR) Special Election

Assessment Mission [final report](#) noted a “blurring of the line between the [ruling party] campaign and media coverage of the president and government, including in response to the COVID-19 crisis”.

The vote was further marred by alleged fraud and voter intimidation, with the [same ODIHR report](#) citing numerous complaints from citizen observers of pressure – especially among public-sector employees – to support the government, parallel voter lists being used to track voters during the poll, vote buying and the casting of multiple ballots.

While social media platforms are indeed plagued by fake news and abusive content, the primary source of disinformation and hate speech are the tabloid press and broadcast and cable TV, financed by the state through [project subsidies](#).

International organisations have voiced concern about non-transparent media ownership and the allocation of public funds.

“The [ruling party] has expanded its influence over the media through both state-owned enterprises and an array of private outlets that are dependent on government funding, and has harnessed this influence to strengthen its political position and discredit its rivals, further reducing opposition parties’ competitiveness. Opposition figures have also faced escalating harassment and violence in recent years,” a 2021 [Freedom House](#) report warns.

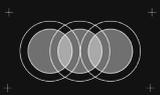
Beyond party-political infighting, the mainstream media vilification of refugees using the Balkan route to Europe continues. The first major incident happened in May when a man livestreamed himself on Facebook as he drove his car through the gates of a centre for migrants on the outskirts of Belgrade.

Fake news stories alleging migrants have committed crimes against Serbs garnered considerable attention on social media and in the tabloid press and anti-migrant rhetoric has been adopted by right-wing movements and parties.

Vucic’s SNS party [won the election with just over 60 per cent](#) of the vote but voter turnout was the lowest since 1990 at just 48.8 per cent – meaning the SNS can [press ahead with its agenda](#) of political and economic reforms that many regard as merely strengthening their grip on power by dismantling institutions.

Meanwhile, the government is pressing ahead with the controversial installation - in partnership with Chinese tech firm Huawei - of 8,000 “smart” street cameras and police car/body cams in Belgrade to enable continental Europe’s first mass, indiscriminate biometric surveillance system.

Critics are alarmed not only by the mass surveillance but also by the fact the cost and terms of the deal, including how personal biometric data will be protected, have not yet been made public.



SHARE
FOUNDATION