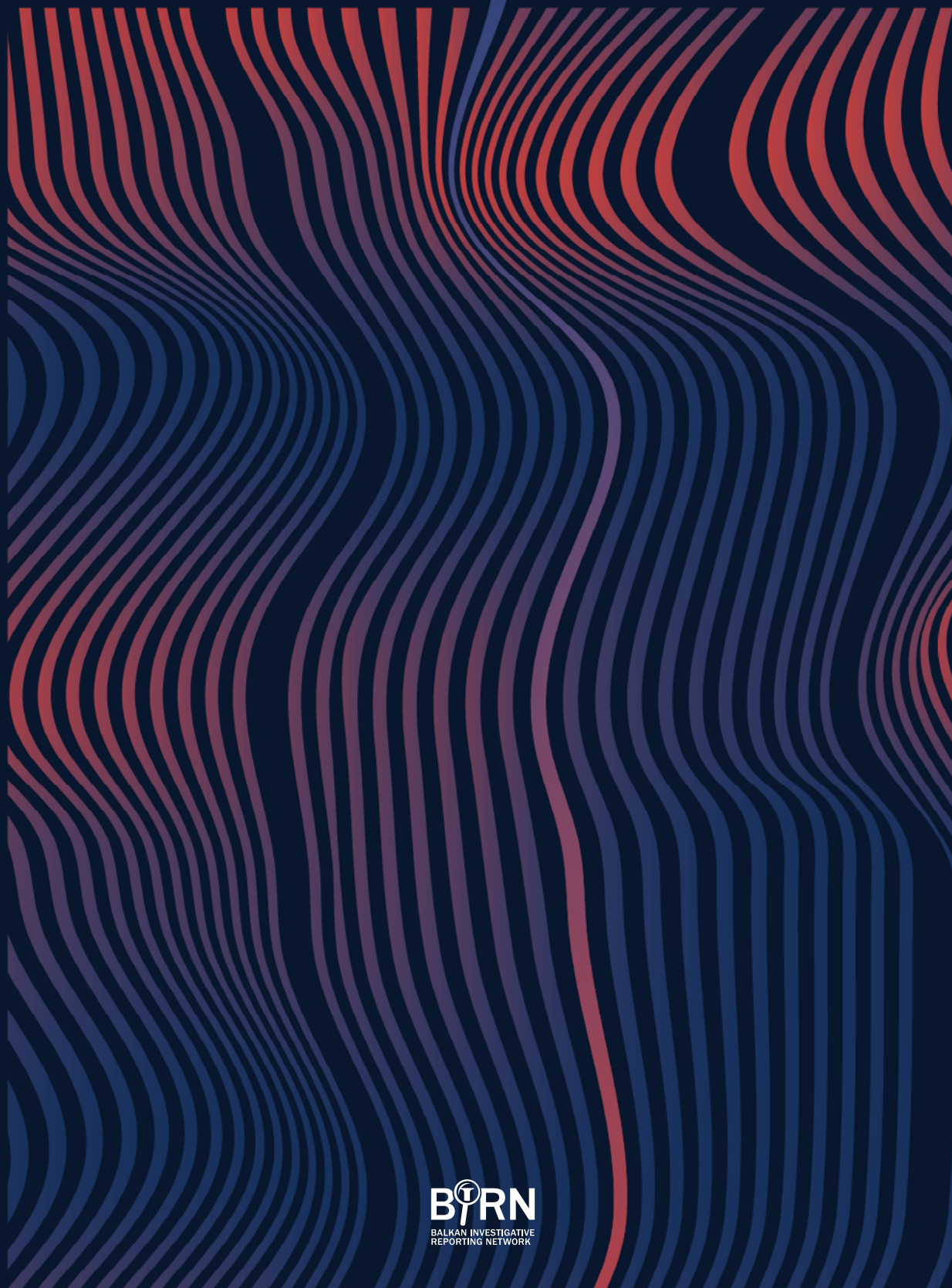


DISTORTING THE TRUTH: HATE SPEECH AND DISINFORMATION FUEL DIGITAL RIGHTS ABUSES IN THE BALKANS

Annual Digital Rights Report 2022



Contents

Acknowledgments	5
Glossary	6
Introduction	8
Data sources	9
Methodology and Definitions	10
Data capture	11
Executive Summary	12
Country reports	19
Bosnia and Herzegovina	19
Croatia	24
Hungary	28
Kosovo	32
Montenegro	36
North Macedonia	40
Romania	44
Serbia	48
Conclusion	53
Recommendations	54

Acknowledgments


The Balkan Investigative Reporting Network (BIRN) team that worked on this report includes Matteo Mastracci, Lead Researcher, Amina Mahović, Project Manager, and Miloš Ćirić, Digital Rights Programme Manager. The authors express their gratitude to BIRN's Regional Director, Milka Domanović, and Aida Ajanović, Head of Programmes, for providing vital support during the preparation of this report. The authors thank the SHARE Foundation for contributing to the Serbia country report and all journalist-monitors for providing critical insights and monitoring digital rights violations in the region.

The report was produced with the support of Greater Internet Freedom (GIF), a project funded by the United States Agency for International Development (USAID)¹ and implemented by Internews. The GIF project works through a coalition structure that brings together local, regional, and international civil society actors to deliver sustainable results. BIRN, as one of the eight regional partners, works in the Western Balkans region to preserve open, interoperable, reliable, and secure internet.

1 This report is made possible by the generous support of the American people through USAID. The contents are the responsibility of BIRN and do not necessarily reflect the views of USAID or the United States Government.

Glossary

Ad fraud	Using automated means to artificially inflate advertising metrics or generate revenue through fake clicks.
Case/incident	Any digital rights violations.
Cybersecurity	The practice of protecting systems, networks, and programs from digital attacks.
Clickbait	Refers to misleading news story headlines that are sensationalised or promise more than the story delivers or merely redirect readers to advertisements.
<u>DDoS</u> attacks	Overwhelming a website or network with traffic to cause it to crash or become unavailable.
Digital Rights	BIRN defines digital rights and responsibilities as mirroring human rights in the offline world (see the Definitions section on page 10 of this report).
Disinformation	False or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm.
Fake News	Fake news refers to false or misleading information presented as real news and disseminated through traditional online and social media. Fake news can be considered a type of disinformation. The purpose of fake news may be to manipulate public opinion, push a political agenda, or profit through clicks and advertising revenue.
Hate speech	Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. See the UN definition of <u>hate speech</u> for further information.



Malware	Malicious software that can infect devices and steal sensitive information.
Misinformation	False or misleading content shared without harmful intent, though the effects can still be harmful.
Monitoring	This refers to the whole process of collecting and documenting cases/incidents.
Online scams	Fraudulent schemes that are perpetrated over the internet with the intention of tricking people into giving away their money, personal information or both.
Online Threats	Online threats of violence or harm refer to any explicit, credible statements made through digital communication (such as social media, email, instant messaging, or forums) that threaten to cause physical or emotional harm to an individual or a group of individuals.
Phishing	Fraudulent emails or websites that impersonate legitimate entities to steal personal information or login credentials.
Ransomware	A type of malware that encrypts a victim's files and demands payment in exchange for the decryption key.

Introduction

Human rights violations in fragile democracies such as those covered in this report differ in type, nature, scope, and target. This - in combination with rapidly-changing technology - has led to violations of human rights in digital environments. Journalists, public officials, human rights activists, and the public face different attacks online, including smear campaigns, trolling, and hate speech.

Ongoing political tensions and “culture wars” - of the kind invoked by right-wing leaders and their enablers within the media to further divide societies by presenting democratic values as weak, lacking legitimacy and even immoral - have continued to migrate from the physical world to the digital space, while the accountability of on-line actors, including government officials and big tech, is very limited.

This annual report provides a snapshot of digital rights and freedoms violations in the Western Balkans digital space. In collaboration with the SHARE Foundation, the Balkan Investigative Reporting Network (BIRN) produced this report based on data from the Digital Rights Monitoring [database](#). The reporting period covers 1 September 2021 to 31 August 2022.

BIRN’s Digital Rights Monitoring project is a part of BIRN’s broader efforts to protect human rights and promote safe, inclusive communications and the responsible exercise of freedom of speech in both the off- and online domains. This report covers the state of digital rights in Bosnia and Herzegovina, Croatia, Hungary, Kosovo, Montenegro, North Macedonia, Romania, and Serbia.

BIRN remains dedicated to systematically mapping and reporting on the (mis)use of technology and human rights violations in the Western Balkans. For this report, breaches of digital rights were identified with descriptions of the cases and corresponding sources to provide information about the violations and their impact on society. Through a review of country-specific reports, the report summarises key cases of digital rights violations and lessons learned.

Overall, the chapters in this report are intended to present key, indicative findings based on BIRN’s monitoring in the countries covered but also improve understanding of what kind of digital rights violations most frequently occur in the digital environment of the Western Balkans. The report offers recommendations aimed at policy-makers, regional regulators, organisations, and individuals in media and technology for better implementation of human rights protection norms, both online and offline.

To improve internet governance, BIRN will continue expanding its monitoring and increase policy and advocacy efforts, thereby equipping citizens and media with the skills to track and respond to digital rights incidents.

In addition, a [dedicated page](#) on BIRN's flagship website, Balkan Insight, offers information on digital rights and other online rights-related topics for the general public and organisations/individuals operating within the field. BIRN's monitoring and reporting aims to provide timely warnings, which could be critical in effectively promoting and protecting digital rights.

Finally, the report seeks to raise public awareness and stimulate further discussion about digital rights and freedom violations.

Data sources

BIRN uses a mix of internal and external monitors who proactively search for and identify potential breaches of digital rights. Once a possible violation is identified, monitors then secure evidence – such as screenshots, web page archives, or other digital content that document the nature and extent of the alleged violation. BIRN's digital rights researcher then verifies whether the content (social media posts, online text, images, video etc.) constitutes an infringement of digital rights.

BIRN monitors incidents in Bosnia and Herzegovina, Croatia, Hungary, Kosovo, Montenegro, North Macedonia, Romania and Serbia. The [SHARE Foundation](#) monitored Serbia's digital rights violation cases. In August 2022, BIRN engaged the [Macedonian Helsinki Committee](#) (MHC), an NGO dedicated to promoting human rights and monitoring violations in North Macedonia, to provide temporary support with monitoring services.

Once BIRN has established that a breach of rights has taken place, the incident is logged on the monitoring online database and published on the BIRN Investigative Resource Desk (BIRD). The team endeavours to identify, verify and log as many incidents of digital right's infringements as possible to provide meaningful insights into behaviours within the region's digital space.

Naturally, our findings are indicative in nature as we investigate a sample of regional online activity. That said, BIRN verifies around 800 cases across the region each year and this enables us to identify significant trends and assess how these violations negatively impact access to reliable, fact-checked information, freedom of speech and

expression, the exchange of ideas in the eight monitored countries which - according to the [Nations in Transit 2022](#) report by Freedom House, a US-based non-profit monitoring global democracy - all belong to the growing category of hybrid regimes.

From 1 September 2021 to 31 August 2022, BIRN recorded a total of 782 digital rights violations in our database as follows: Bosnia and Herzegovina (77 cases), Croatia (70 cases), Hungary (146 cases), Kosovo (89 cases), North Macedonia (83 cases), Montenegro (65 cases), Romania (128 cases), along with 124 cases from Serbia recorded by the SHARE Foundation.

Definitions

In conducting our research and compiling this report, BIRN defines digital rights and responsibilities as mirroring human rights in the offline world and – as we become ever more dependent on the internet and increasingly exercise our freedoms online – BIRN believes that these online rights should be protected in the same manner.

BIRN has, in considering what constitutes digital rights, referred to the European Union’s work on defining and protecting these rights. The [European Declaration on Digital Rights and Principles](#) describes the importance of these rights and the difficulties in protecting them:

“The digital transformation also presents challenges for our democratic societies, our economies and for individuals. With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment. The digital transformation should not entail the regression of rights. What is illegal offline, is illegal online.”

Methodology

BIRN and our partner organisation, the SHARE Foundation, collect the data on digital rights and how they are abused in the region. Once violations of digital rights have been identified (see Data Sources section earlier in this report) – they are classified within the database. Through our [monitoring methodology](#), we have classified violations of those rights into seven broad categories as listed earlier in the report. To better understand how digital rights are being undermined, we have created seven, broad categories of violations:

Information security breaches - including unauthorised accesses, DDoS (Distributed Denial-of-Service) attacks, theft and destruction of data, and other security breaches.

Information privacy and personal data breaches - including data leaking, illegal data processing or interception of communications, etc.

Pressures because of expression and activities on the internet - including all breaches related to reputation, endangering security, discrimination and hatred, and pressures on individuals because of publishing information on the internet, among others.

Manipulation and propaganda in the digital environment – including the dissemination of fake news, creation of bogus social media accounts, the production of misleading or doctored images and videos, and the placement of commercial content as news, among other related digital rights violations.

Holding intermediaries liable - including digital rights violations related to pressures on internet service providers, such as hosting providers, to remove content or block access to websites or services, often through legal measures or threats of punishment.

Blocking and filtering of content - including cases of technical blocking or filtering of content at the national or organisational level or through algorithmic processes by online platforms.

Other breaches - referring to other digital rights violations not expressly included in all the other categories.

Bearing in mind that technology and online information sharing is constantly and rapidly evolving, BIRN continues to keep the methodology used under review.

Data capture

BIRN recognises that the data its monitors capture in order to produce this series of reports only provides a partial snapshot of the situation and indicative findings.

Going forward, BIRN will be increasing, revising and fine-tuning its methodology, data capture, classification and analysis to provide more reliable and robust data, which in turn will yield a more comprehensive picture of the incident rate of violations combined with greater insight into the subsequent impact on digital rights, society and democracy at large.

Executive Summary

The findings of this report are based on 782 cases of digital rights violation that BIRN monitors logged and verified between 1 September 2021 and 31 August 2022 in eight countries: Bosnia and Herzegovina, Croatia, Hungary, Kosovo, Montenegro, North Macedonia, Romania, and Serbia.²

This report does not analyse all recorded cases but focuses on the most paradigmatic incidents while providing a total number of violations classified by categories, attackers, and affected parties. The report also identifies significant trends to paint a picture of digital rights violations in each monitored country.

Cases logged in our database indicate there has been an overall rise in digital rights violations connected to country-specific topics compared to [last year's report](#), "Online Intimidation: Controlling the Narrative in the Balkans." This suggests that national authorities have not yet begun to address the problem of digital rights violations adequately or consistently.

Common trends

Our researchers have extrapolated common trends in online rights abuses by reviewing data captured during monitoring. These illustrate the interconnectivity between tensions and conflicts in the "offline world" across the region and rights abuses in the digital sphere.

Moscow's Ukraine disinformation campaign

Since its outbreak in February 2022, the war in Ukraine has been at the centre of large-scale online disinformation and propaganda campaigns across the Balkans, which is reflected in the number of incidents of digital rights violations BIRN has verified (60+ cases). The highest number of cases were recorded in Hungary and Romania, followed by Serbia.

In Hungary, fake news about the war in Ukraine has led to political clashes and concerns that the pro-government media is supporting a pro-Russia narrative. In one case, false claims that Ukrainian President Volodymyr Zelensky was on the run reached approximately 1.2 million Facebook users.

Moscow also continues to use fake news and propaganda to shore up support in Serbia, where Russian influence makes many Serbs feel culturally far closer to Russia than to Western Europe. In addition, Moscow's refusal to recognise Kosovo as an independent state – it declared independence in 2008 – has further endeared Russia to those Serbs who refuse to accept Kosovo's independent status.

However, while many Serbs might view Vladimir Putin as willing and able to return Kosovo to Serbia, Belgrade is, in reality, negotiating a trickier path. Serbian President Aleksandar Vucic is pursuing relations with both the West (notably EU-membership) and Russia. It is this balancing act that has seen Belgrade reject imposing sanctions against Moscow while at the same time stop short of recognising Crimea (annexed by Russia in 2014) as Russian territory, claiming that could create problems regarding Kosovo's status.

Just one day after Russia attacked Ukraine, the Twitter account of Youth of Jazas, a Serbian HIV/AIDS support and prevention NGO, was hacked. The hacker(s) – who remains unknown – tweeted that "Ukraine is AIDS" and described Russia as "the cure". After regaining control of its Twitter account, Youth of Jazas tweeted an apology for the incident.

Exploiting disquiet in Bosnia and Herzegovina, Kosovo

Russia's supporters have published denials of war crimes allegedly committed by Russian troops in Ukraine and disseminated a slew of sometimes contradictory fake news and social media posts in bitterly-divided Bosnia and Herzegovina – where power, since the 1995 Dayton Peace Accords, has been divided between two entities: the majority Bosniak (Muslim) and Croat Federation of Bosnia and Herzegovina and the Serb-dominated Republika Srpska.

Observers warn that Moscow is trying to scare Bosnia off joining the NATO military alliance by raising the spectre of renewed violent conflict in order to frustrate its EU-accession progress. They caution that Russia uses misinformation and conflicting fake news stories to sow discord and keep Bosnians in a state of anxiety and confusion.

The day after Russia invaded Ukraine, Dusanka Majkic, a Bosnian MP and member of the main Bosnian Serb party, the Alliance of Independent Social Democrats (SNSD), tweeted: "In March 2021, Moscow promised to react if Bosnia takes any further steps towards NATO. Don't say you haven't been warned."

The SNSD president and the leader of Republika Srpska, Milorad Dodik, has been a staunch supporter of Putin's Russia and an opponent of NATO. Dodik is actively advocating the break-up of Bosnia and Herzegovina and Republika Srpska's independence, and he has been a frequent guest in Serbia, whose presidents and prime ministers have shown him strong support in previous years. He is also backed by many Serbian right-wing groups and ultra-nationalistic opposition parties, such as the Dveri movement.

A few days after the Majkic incident, Serbian MP and Dveri leader Bosko Obradovic [told](#) TV Prva, a Belgrade-based television channel, that it would be "justified for the Serbian Army to get involved" in Bosnia and Herzegovina "to protect Serbs in Republika Srpska, if aggression is launched against them". He said that Serbian military intervention would be "an obligation in every kind of sense, both moral and historical". The video went viral and was covered by numerous media outlets.

In Kosovo, Moscow's supporters have also used widely-shared fake news to exploit deep-seated divisions and tensions between ethnic groups and generate fear among people that the violent conflicts between Kosovo Serbs and Albanians could erupt again. Long-standing tensions between the Kosovo government and ethnic Serbs who maintain close ties with Belgrade regularly spill over into violence in the Serb-dominated north of the country. Russia, a long-time supporter of Serbia, is viewed as a potential threat among the ethnic Albanian majority.

On 27 February 2022, several media outlet's Facebook pages [published](#) an article with the headline Vladimir Putin Goes Insane, Releases 2,000 Rockets in a Minute Toward Ukraine. However, the accompanying video has been widely available online since at least 2020 and does not depict the recent war in Ukraine. The story's publication looks to be a highly irresponsible exercise in clickbait given the significant tensions and unease in the country.

Journalists face threats and intimidation

The intimidation of journalists remains one of the greatest [challenges](#) to media freedom in the Balkans. According to the [2022 Reporters Without Borders World Press Freedom Index](#), media freedom remains a major concern in many Balkan states, with journalists working in highly polarised political environments and facing threats from criminal groups. It also noted the information chaos is a result of "a globalised and unregulated online information space that encourages fake news and propaganda".

Independent media and investigative journalists who expose abuse of office and seek to hold those in power to account are routinely threatened and targeted by media outlets that support President Aleksandar Vucic and his SNS party, which has ruled Serbia since 2012.

Of cases relating to threats against journalists, BIRN logged the most in Serbia (50 cases). This echoes the indicative findings in BIRN's [previous report](#) on digital rights abuses, which suggested Serbian journalists were the most frequently targeted party online (38 of 111 cases verified by BIRN). In addition, public figures who have been the subject of critical media coverage or have been investigated or charged by the police with offences related to corruption have launched legal actions against independent journalists/outlets in what are widely regarded as attempts to silence critical voices and stifle public debate.

There is growing concern over the development of a chilling effect on independent, critical reporting across the region due to the apparent impunity for those making on- and offline threats against journalists.

Political smears threaten democratic process

Smear campaigns have become commonplace across the region and pose a serious threat to democratic values where many of the monitored countries have hybrid regimes in power that combine elections with elements of authoritarian rule. Election campaigns held in 2022 in Bosnia and Herzegovina, Hungary and Serbia spawned a torrent of online attacks among political rivals.

In May 2022, the president of the Women of the SDA (Party of Democratic Action) Sarajevo, Alma Omerovic, insulted the vice president of the Social Democratic Party (SDP), Denis Becirovic in a [Facebook post](#). She called him a traitor, adding: "Get smart Bosniaks, this [the election] is the jihad of our time". After the post went viral and drew criticism from many media outlets, Omerovic defended her characterisation of the elections with: "Jihad, you bet! Because we truly need it!".

There are also ongoing concerns over censorship, particularly when it comes to media outlets that support ruling parties. In March 2022, Serbia's Happy TV removed a video from its YouTube channel which featured a heated debate involving political analyst Boban Stojanović, who criticised the government's economic policy and noted that salaries in Serbia are now the lowest they have been since the fall of former strongman leader Slobodan Milosevic in October 2000.

Viktor Orban secured another term as prime minister in Hungary following general elections. He used his victory speech to [criticise](#) European Union “bureaucrats” and Ukraine’s President Volodymyr Zelensky, calling them “opponents”. Zelensky has criticised Hungary’s refusal to unequivocally condemn Russia’s invasion of Ukraine or allow weapons intended for Ukraine through Hungary. Orban’s Fidesz party launched numerous smear campaigns and attacks against political opponents in the run-up to the elections.

Homophobia remains endemic online

Pride parades in Bosnia and Herzegovina and North Macedonia were met with incidents of online hate speech and incitement to violence against the LGBTQ+ community. In Sarajevo and Skopje on 25 June 2022, numerous digital rights violations occurred, including comments calling for violence against the Pride parade participants and other members of the LGBTQ+ community.

During the build-up to the October 2022 general elections in Bosnia and Herzegovina and North Macedonia, some politicians [utilised](#) the controversy surrounding the Pride parades to appeal to voters. This involved making [discriminatory statements](#) and [comparing](#) the parade to the siege of Sarajevo during the Bosnian War. These statements have left members of the LGBTQ+ community concerned about their future rights.

In Serbia, thousands protested the event while insults and homophobic content were shared on social media. In Hungary, several pro-government media started sharing [homophobic articles](#) targeting the newly appointed Deputy Assistant Secretary at the US Department of Energy, Sam Brinton, who identifies as non-binary. Some articles called Brinton a “dog fetish drag queen” with a “deviant” personality.

In Romania on 10 August 2022, MozaiQ, one of the most active gay rights NGOs in the country, denounced what it called a worrying [increase in hate speech against the LGBTQ+ community](#). In the following weeks, some members of the organisation received death threats and were on the receiving end of online attacks, said Vlad Viski, executive director of MozaiQ.ms.

Scams, phishing and data breaches

Online scams, fraud, data breaches and cybercrime are commonplace across the

region including hacking attacks targeting websites belonging to public and government institutions. BIRN monitors recorded serious attacks in North Macedonia and Romania involving cyber-attacks and computer fraud targeting public systems. On 4 July 2022, one of North Macedonia's most popular IT websites, IT.mk, fell victim to a series of devastating [DDoS attacks](#). The hackers demanded a ransom in bitcoin. IT.mk refused to pay and was [targeted again](#) on 17 August 2022, by another DDoS attack.

Meanwhile in Romania, websites of several key public institutions were also hit by [DDoS attacks](#). The attacks were claimed on Telegram by Killnet, a hacking group based in Russia. The hackers justified the attacks by blaming Marcel Ciolacu, the Chamber of Deputies' President, for promising "maximum assistance" to Ukraine. For about seven hours, users couldn't access online government services including the defence and border police websites.



COUNTRY REPORTS

FACT SHEET

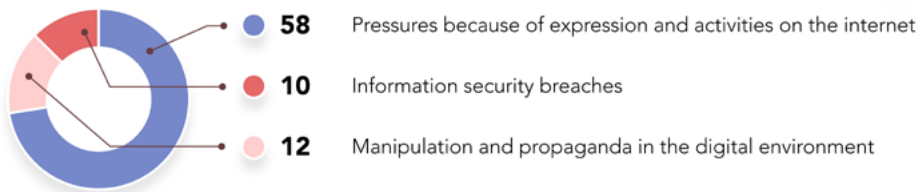
BOSNIA AND HERZEGOVINA

TOTAL NUMBER OF CASES VERIFIED BY BIRN

77* CASES

Between September 1, 2021 and August 31, 2022

THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
7	5	4	5

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
11	7	7	4	7	6	8	6

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

Most cases of digital rights violations verified by BIRN in Bosnia and Herzegovina were classified as “pressures because of expression and activities on the internet”. These breaches mainly refer to threatening content and endangering security (33 out of a total of 77 cases), followed by hate speech and discrimination (30 cases).

Calls for war and violence, expressions of ethnic hatred, threats posted via social media aimed at politicians, media outlets, and journalists, as well as sexist insults against female politicians and journalists, are just some of the most significant violations recorded in our database.

Similar to previous years, [Sarajevo’s Pride Parade](#) triggered incidents of hate speech including homophobic remarks made by politicians. The [commemoration of the 1995 Srebrenica genocide](#) also sparked numerous incidents of hate speech and genocide denial.

Finally, the war in Ukraine has been the subject of several dangerous narratives that have been widely shared, various propaganda and heightened unease among the citizens of Bosnia and Herzegovina.

Online intimidation of journalists and public figures

BIRN recorded several cases of politicians receiving death threats via social media. For example, in January 2022 the Bosniak vice-president of Republika Srpska, Ramiz Salkic, received [death threats](#) via his Facebook profile. Salkić said: “The threats are the product of the activities of separatist-oriented Bosnian Serbs led by Bosnia and Herzegovina Presidency member Milorad Dodik, who gives false hope to Bosnian Serbs that they will have a new Serbian state.”

In March 2022, attempts to reform legislation governing elections led to death threats being posted on the Facebook page of the Croatian Democratic Union (HDZ) Bosnia and Herzegovina Cantonal Committee of the Zenica-Doboj Canton, targeting Dragan Covic, the president of the HDZ, and Ivo Tadic, president of the Cantonal Board.

During the same month, Dodik, Republika Srpska vice-president, the Serbian member of Bosnia and Herzegovina’s tripartite presidency and head of the main Bosnian Serb party, the Independent Social Democrats (SNSD), was also the [target of death threats](#). A video in which a masked man offers a million euros for Dodik’s murder was

published on TikTok. The mayor of Republika Srpska's largest city Banja Luka, Drasko Stanivukovic, also received a [death threat on Viber](#), which featured a photograph of a man holding a gun with the caption "Drasko, I will kill you."

In November 2021, a journalist from direkt-portal.com received [threatening text messages](#) after she published an investigative story concerning the Hydroelectric Power Plant in Trebinje. The messages were allegedly sent from the phone of Ljubo Vukovic, one of the Hydroelectric Power Plant's executives and a member of the SNSD party. Vukovic denied sending messages to the journalist.

In December 2021, journalist Dragan Bursac and his wife received [death threats](#) via Messenger and other social media channels. Bursac has received numerous threats over the years for his work which deals with war crimes committed by Bosnian Serbs during the 1992-5 war.

Sarajevo film director Jasmila Zbanic reported receiving [death threats](#) to the Sarajevo Canton Interior Ministry in May 2022. She received the threats after publicly saying that the number of children killed during the siege of Sarajevo in the 1990s was much higher than officially recognised.

A further episode involved Rajko Vasic, a high official of the SNSD party, commenting on Twitter about the [difficult financial situation of Bosnian-Herzegovinian Radio Television \(BHRT\)](#) and saying that he would "blow up" the building of BHRT "if others were uncomfortable doing so."

Ethnic tensions and calls for violence

In October 2021, the online portal Istraga showed [videos](#) featuring members of Republika Srpska's police who participated in an exercise overseen by Minister of Interior Dragan Lukac. The way Lukac greeted the special unit went viral, as it was widely interpreted as a follow-up to previous [secessionist threats](#) made by Bosnian Serb leader Dodik. The videos led to online users sharing hate speech and comments promoting war.

The newly established gendarmerie unit in Bosnia's Republika Srpska [sparked criticism](#) from Bosniak politicians amid concern it will escalate existing inter-ethnic tensions. The unit's creation followed controversy surrounding a proposed reservist police force. The proposal was dropped in June but later endorsed by the entity's most powerful politician, Dodik. The reservist force was met with opposition from war victims' groups because of the alleged involvement of some Bosnian Serb police

officers in war crimes committed during the 1992-5 war in Bosnia.

The leader of the Party of Democratic Action (SDA), Bakir Izetbegovic, [attracted sharp criticism](#) after delivering a speech at a party meeting in Bosnia and Herzegovina. Izetbegovic told his audience that if others were wondering “if we [the Bosniaks] have enough military power for the worst-case scenario”, his answer was: “We do.” These comments were perceived as warmongering by Bosnian Serb politicians, who called for Izetbegovic to be removed from political life.

Cases of anti-Bosniak hatred were also recorded during last year's Republika Srpska Day celebration. Gorica Dodik, daughter of Bosnian Serb leader Dodik, posted numerous war-mongering messages. Twitter later [blocked](#) her account after many users logged complaints about her tweets.

Pride Parade in Sarajevo

Under the slogan “Family Gathering”, around 2,000 people took part in the Sarajevo Pride Parade to demand better rights for the LGBTQ+ community. Although the event was peaceful it led to numerous incidents of homophobic comments, insults and discriminatory remarks being posted and shared online. Mirza Halilcevic, a member of the organising committee for the event, was subjected to [homophobic and discriminatory comments](#) on the Bosnian portal Byka, following an interview he gave.

[Faruk Kapidzic](#), a former minister in the Sarajevo Canton and member of the Party for Democratic Action (SDA), compared the LBTIQ+ community with Eugen of Savoy, the Austrian general who torched Sarajevo in 1697, and Radovan Karadzic, the former Bosnian Serb leader convicted of genocide. Minister of Economy of Sarajevo Canton Adnan Delić [shared anti-LBTIQ+ views](#) on the official Facebook page of the Ministry.

Misogyny and sexism

On 22 September 2021, Lana Prlic, a member of the House of Representatives of the Federation entity parliament, was subjected to many [sexist threats and insults](#) after she called for people to get vaccinated against COVID-19. On 27 July 2022, MP and vice-president of the socio-liberal political party “Nasa stranka” (“Our party”) Sabina Cudic and Aleksandra Nikolic, Minister of Science, Higher Education and Youth of the Sarajevo Canton, were recipients [of insults](#) from representatives at the working sessions of the Assembly of the Canton of Sarajevo.

One day later, a representative of Our Party, Vildana Beslija, who condemned the sexism and misogyny in the Federation parliament, received [sexist and misogynist insults](#) via messenger after speaking out on social media. In January 2022, a public debate in Mostar's City Hall about small hydropower plants was marred by an [incident](#) when one of the participants used derogatory and sexist language against an activist from the environmentalist group Aarhus. The incident was recorded and went viral, with many users condemning the man's behaviour on social networks.

Moscow's Ukraine war disinformation campaign

The war in Ukraine has led to the spread of dangerous narratives as well as disinformation in Bosnia and Herzegovina.

On 25 February 2022, Dusanka Majkic, a parliamentarian in Bosnia and Herzegovina's House of Peoples and a member of the SNSD, commented on the [war in Ukraine on Twitter](#), emphasising that a Ukrainian scenario could happen in Bosnia.

On the same day, a video circulated on the internet that [appeared](#) to show a military plane being targeted by Ukrainian air defence. The accompanying post suggested that the video was from the conflict in Ukraine. However, this was debunked by the Raskrinkavanje fact-checking portal, which clarified that the video was from the video game Arma 3. This game, released in September 2013, is known for its realistic simulation of military conflicts.

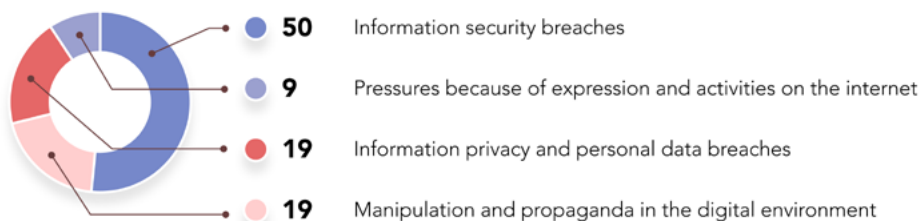
CROATIA

TOTAL NUMBER OF CASES VERIFIED BY BIRN

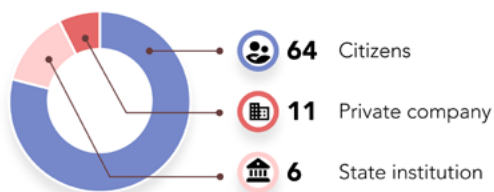
70* CASES

Between September 1, 2021 and August 31, 2022

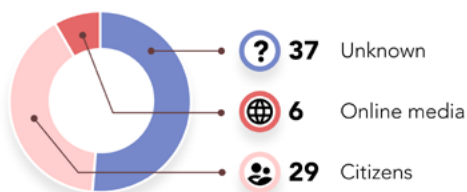
THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
3	4	4	4

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
11	13	13	4	2	4	4	4

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

In Croatia, digital rights violations logged by BIRN monitors have predominantly involved information security and personal data breaches. Of 70 cases recorded, 50 fall into the category of information security breaches, with 19 cases being information privacy and personal data breaches. BIRN also logged 19 incidents classified as manipulation and propaganda in the digital environment. The least common category of violations logged by BIRN in Croatia were cases of pressure because of expression and activities on the internet (9 cases verified). Fake news and disinformation about the war in Ukraine and online hate speech have been significant issues in Croatia, along with various marginalised groups - including minors - targeted through online posts, comments, and messages.

Ukraine war disinformation

Fake news, misinformation, and disinformation about the war in Ukraine have also circulated widely in Croatia. Several Croatian media outlets published [fake news](#) about the so-called Ghost of Kyiv, a story celebrating a Ukrainian fighter pilot for shooting down as many as 40 Russian planes, a claim that was later described as “highly exaggerated” by German news outlet [Deutsche Welle](#).

On 7 March 2022, many Croatian social network users [shared a still image](#) taken from a popular Serbian film *Lepa sela lepo gore*, that was incorrectly described as showing soldiers in Ukraine. The still was shown with the caption: “Russian occupation soldiers drink beer after burning a village. European civilisation is disappearing in flames.” This appeared on a Twitter account that is now suspended. On the same day, [fake news](#) claiming the COVID-19 vaccination had caused thousands of deaths was circulated in Croatia. The fake news story also claimed that the war in Ukraine was being used as a “cover-up” to distract the public from the “facts” relating to deaths from COVID-19 vaccines.

Hate speech drives digital rights violations

Hate speech continues to be a significant problem in Croatia on social media platforms, websites, and other online spaces.

On 1 December 2021, Bernarda Jug, a Croatian teacher and one of the most promi-

ment figures of the anti-vaccination movement in Croatia, [asked](#) her followers to make additions to “the list of traitors” published on the website “Croatian traitors”, so that “the people could put them [those on the list] on trial.” The logo used on the page was a hanging noose. On the home page, people were asked to enter the personal information of the “traitor” with their phone numbers and emails, as well as the names and surnames of people closely related to them. Another incident saw a scientist who had been vocal during the pandemic about the dangers of COVID-19 fall victim to [hate speech and death threats](#) on 3 February 2022.

On 8 May 2022, a teenage schoolboy from Zagreb was taking a stroll through the city when he was approached by a photographer who wanted to capture his striking, alternative fashion sense. Pictures of him were later posted on the Style Seconds Facebook page, which has more than 91,000 followers. The schoolboy, who local media reported as being just 16 years old, was subjected to a [wave of cyberbullying](#). The abuse included death threats, insults based on nationality and homophobic messages.

An elementary school teacher from Pula posted a [homophobic comment](#) on Facebook on 10 June 2022 in response to an article aimed at raising awareness about homophobia in schools and preventing abuse and violence. The teacher wrote sarcastically: “I believe that we lag behind organised European countries in terms of the number of gays in one class, so children and parents should be further educated so that there are at least 50 per cent of them per class, in order to be at the very top, advanced and modern!” The teacher then claimed that his comment was not homophobic. In response to the incident, the school's principal made it clear that she was against any hate speech, violence, degradation, or homophobic messages, and promised to talk to the teacher about what happened. The incident highlights the issue of how schools should address and prevent homophobic behaviour among staff and students.

Cybercrimes and online fraud remain endemic in the Croatian digital space

Cybercrimes and online fraud continue to be a major problem in the Croatian digital space. Reports of hacking, phishing attacks, and other forms of cybercrime are common, and individuals and businesses are vulnerable to these crimes. These crimes can result in significant financial losses for victims and damage their reputations and credibility. In addition, the perpetrators of cybercrimes often operate from outside the country, making it difficult for authorities to track and prosecute them. It is im-

portant for individuals and businesses to be aware of these risks and to take steps to protect themselves online, such as using strong passwords and being cautious when providing personal information or making financial transactions online.

Croatian telecommunications operator A1 was hacked and around 10 per cent of its user data was compromised. According to local news reports, the hacker demanded a \$500,000 ransom and threatened to sell the data on the dark web. A cryptocurrency fraud was reported to the Varaždin police after a Croatian citizen had been conned into giving their bank account details to someone he had interacted with on social media between September and November 2021.

BIRN monitors logged two cases of computer fraud on March 6, 2022. In the first case, Erste bank, the third largest bank in Croatia, notified its customers that scammers were circulating a fake internet page that closely resembled the bank's web pages and warned them against inputting any personal data on the page. Similarly, RBA bank warned of fake SMS messages, which were "trying to discredit the bank and its stability". The bank reported the case to the Interior Ministry.

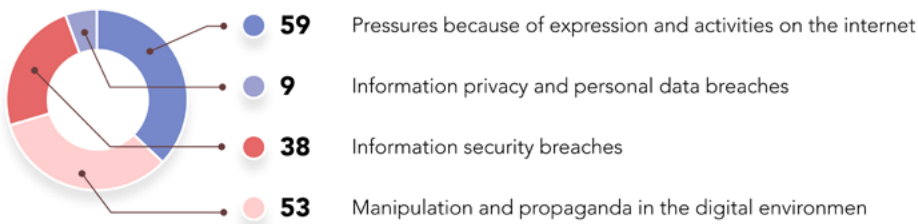
HUNGARY

TOTAL NUMBER OF CASES VERIFIED BY BIRN

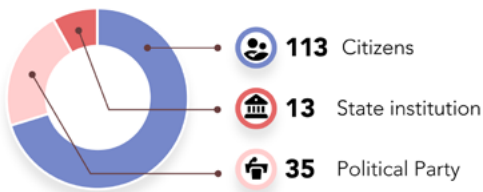
146* CASES

Between September 1, 2021 and August 31, 2022

THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
11	22	12	10

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
17	11	14	11	10	8	10	10

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

The majority of cases of digital rights violations in Hungary verified by BIRN monitors were classified as “pressures because of expression and activities on the internet” (59 incidents). The second most common category in the database is “manipulation and propaganda in the digital environment” (53 cases). Information security breaches, including hacking and cyberattacks, accounted for 38 cases, while information privacy and personal data breaches were less frequent (9 cases). Computer fraud was also a significant issue, with 28 cases verified by BIRN.

The April 2022 parliamentary election in Hungary was characterised by acrimonious campaigning. The Fidesz party, led by Prime Minister Viktor Orbán, sponsored [a referendum](#) on a proposed child-protection law banning making sexual orientation courses and gender reassignment information available to minors without parental consent, among other proposals. Although the referendum failed to attain binding status due to low voter turnout, it resulted in numerous incidents of online hate speech against members of the LGBTQ+ community.

Similar to all other monitored countries, Hungary recorded a spike in fake news and disinformation linked to the war in Ukraine. Following the April 2022 [episode of misinformation](#) where Ukrainian President Zelensky was falsely accused of using drugs, online attacks against Zelensky remain commonplace in Hungary’s digital environment.

Smear campaigns, acrimonious electioneering

As Hungary’s April election approached, Facebook became a major online arena for political conflict. A [joint investigation](#) by BIRN and Hungarian independent media outlet Telex, published in March 2022, discovered several Facebook pages that promote the Fidesz party line and feature paid advertisements that defame opposition candidates. The source of funding for these efforts is unclear.

Pro-government media have been involved in political attacks and disinformation to discredit Fidesz’s opponents. On 13 February 2022, pro-government media [launched a campaign](#) against Ferenc Gyurcsány, president of the liberal Democratic Coalition Party, claiming he did not know the name of his party’s candidate at an election event. To support this claim, they published a manipulated video in which Gyurcsány appeared not to know the candidate’s last name.

Homophobic attacks

On 11 January 2022, pro-government media outlets spread homophobic messages by presenting themselves as defenders of the "natural family" structure. Following a [case](#) in early March 2022, when the szentkoronaradio.hu website published a list of names and photos of teachers who have supported LGBTQ+ rights, similar cases followed. On March 23, 2022, CitizenGO Hungary, a local branch of a far-right group founded in Madrid, and the website vasarnap.hu, a portal linked to the junior ruling KDNP (Christian Democratic People's Party) in Orbán's government, [published homophobic articles](#) linking homosexuality with paedophilia. Vasarnap.hu also [published](#) a series of unverified allegations with the intention of boycotting the referendum, claiming, among others, that laws on the protection of children in Hungary were inadequate and that the demands of LGBTQ+ rights groups were unfounded.

Ukraine war disinformation

In Hungary, fake news about the war in Ukraine led to political clashes and smear campaigns targeting political opponents in a country where "state media still cannot seem to find a different narrative to their traditionally pro-Russian line" as Edit Inotai, Balkan Insight's correspondent from Hungary, [found in her analysis](#).

Pro-government news outlets reported untrue statements from the Kremlin about Ukraine, [including](#) that Ukrainian troops entered Russia and that the Ukrainian nation does not exist. Even after Russian attacks began, some media outlets still claimed Russia had no plans to attack Ukraine. Various Facebook pages supportive of the Fidesz party are still spreading Russian propaganda. Additionally, both government politicians and pro-government media outlets have [falsely claimed](#) that Hungarian opposition politicians want to send soldiers to Ukraine, plunging Hungary into war with Russia.

On 10 May 2022, an [incident](#) where a photograph of a weeping girl was incorrectly identified as Zelensky's daughter was posted on Facebook with the caption: "Zelensky's daughter hates her father, who is a fascist and murderer of the Ukrainian people". Another [case](#) of online image manipulation occurred on 16 May 2022, when Zelensky was shown holding a football jersey that displayed a swastika instead of a number. However, after Agence France-Presse fact-checkers [detected pixel discrepancies](#) and it was found that the picture had been digitally manipulated by adding a swastika to an [photo that Zelensky posted](#) in June 2021.

Online scams and fraud

On 8 March 2022, the National Cybersecurity Institute of Hungary warned that several organisations had received email requests that appeared to be from the European Commission that claimed to be about the “Situation at the EU’s borders with Ukraine”, which contained harmful links and malware file attachments.

It was reported on 26 April 2022 that phishing emails were being sent out by cyber-criminals posing as MKB, a Hungarian bank. The emails asked customers to log in to their internet banking accounts using a link provided in the email, which looked very similar to the official MKB login page. However, by entering their information through this link, individuals risked giving fraudsters access to their online banking details, potentially enabling unauthorised transactions.

In May 2022, three other incidents of fraud in Hungary were logged by monitors. The first involved scammers posing as private investigators on a professional advertising site, joszaki.hu, and cheating victims. The second incident involved phishing emails sent on behalf of DHL that aimed to obtain users' data by guiding them through the process of submitting their data through automated chatbots. Lastly, a fake online education programme was offered with promises of official graduation certificates and vocational training, resulting in the swindling of over 70 million forints (around 177,000 euros) from victims over several years. On 25 June 2022, Gergely Karacsony, Mayor of Budapest, announced that he was scammed by someone who falsely claimed to be Vitalij Klitschko, Mayor of Kyiv.

On 4 July 2022, a Facebook page mimicking a Hungarian Post page offered to give away unclaimed parcels at a bargain price. The link led to a phishing website that asked for users’ personal information and bank details. One day later, in a separate incident, a Hungarian couple conned 139 users into buying products that were not supplied. Following this, prosecutors filed a charge against the couple for conspiracy, misdemeanour and online fraud. On 9 August, another Hungarian couple conned users of a dating website out of around 15 million Hungarian forints (approximately 38,000 euros).

FACT SHEET

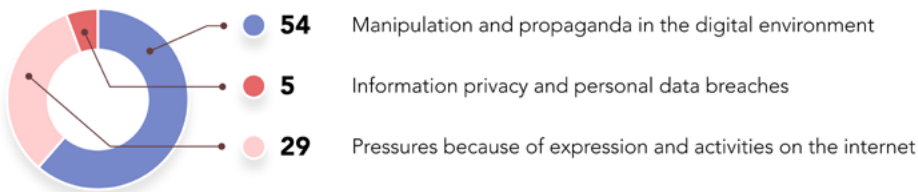
KOSOVO

TOTAL NUMBER OF CASES VERIFIED BY BIRN

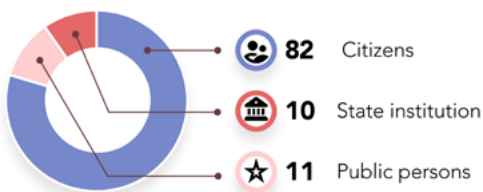
89* CASES

Between September 1, 2021 and August 31, 2022

THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
8	7	7	2

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
4	17	8	5	3	7	16	5

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

In Kosovo, the most frequently reported digital rights violations recorded by BIRN were classified as manipulation and propaganda (54 incidents). Twenty-nine incidents listed as pressure because of online expression/activities were also recorded, in addition to five incidents of information privacy and personal data breaches.

Fake news continues to flourish online, with false information frequently circulated on social media and other platforms. As with the other monitored countries, the war in Ukraine was the focus of many inaccurate/fake news stories that make it difficult for citizens to discern fact from fiction, [as reported by BIRN's publication Prishtina Insight](#). Cybernetics expert Driart Elshani warned in the article that the spread of false news for specific purposes, such as propaganda or profit, can be dangerous in terms of manipulating public opinion.

In addition, a [report](#) released last July 2022 by the Press Council of Kosovo confirmed that online media do not have access to fact-checking specialists or enough editors and sub-editors to deal with disinformation and fake news.

Other digital rights violations have been recorded in Kosovo, including the publishing of fake news related to the dispute between Kosovo and Serbia over vehicle licence plates and several instances of cyberviolence against women.

Ukraine war fake news

News outlet Periskopi [published](#) on 24 February 2022 a photo that it claimed showed a Russian military plane being destroyed by Ukrainian forces. The article cited Ukrainian media without naming media outlets and it was later discovered that the photo had first been published online sometime in 2017 or 2018 and had been taken in Russia. Other Kosovo online portals, such as Gazeta Plisi, Vatra, and KosovaLive, published a [video](#) of military planes that they claimed were Russian planes in Donbas, Ukraine. However, the video was first published on social media in May 2020, before the current conflict in Ukraine started. Media outlets like Gazeta Infokus, Prishtina News, Gazeta Shekulli, and Gazeta Newborn shared a [video](#) titled Vladimir Putin Goes Insane, Releases 2,000 Rockets in a Minute Towards Ukraine. However, the accompanying video has been circulating online since at least 2020 and is not related to the war in Ukraine.

In April 2022, Gazeta Korrekte's Facebook page [shared a link](#) to a news article (Airplanes cover the sky/NATO has given Putin a fatal blow) claiming that NATO had intervened in the war in Ukraine. The page has over 530,000 likes. Despite the title, the article only describes NATO exercises near the Ukrainian border.

Kosovo online media outlet Insajderi.org shared [a photo](#) on Facebook in February 2022 of two children greeting soldiers, claiming that the photo was taken in Ukraine after the Russian invasion and that the children were greeting Ukrainian soldiers. However, this photo was taken in 2016 by Ukrainian photographer Dmitry Muravsky. The post has since been deleted.

Other cases of disinformation recorded in Kosovo include [publishing](#) photos of the Ukrainian capital, Kyiv, by Gazeta Prishtina, Lipjan City, 02 Press, Gazeta Neutral, Desk.al, and Gazeta Stop claiming they were taken before and after the outbreak of the Russian invasion. The "after" photo shows the destroyed centre of Kyiv. However, the photo was taken during the 2014 protests that toppled President Viktor Yanukovich.

Tensions with neighbouring Serbia

As [reported by Balkan Insight](#), the 2021 dispute over Kosovo's insistence that vehicles with Serbian licence plates switch to temporary Kosovo ones when in the country - which Kosovar vehicles must do when entering Serbia - led to many digital rights violations.

On September 2021, several Kosovo media, such as broadcaster TV Dukagjini, newsbomb.al and balkani.info, but also websites in Albania, such as broadcaster Top Channel, [published videos](#) of Serbian military tanks, claiming they were going toward the Serb-dominated north of Kosovo where local Serbs had blocked the roads to the border in a protest about the licence plate rules implemented by Prishtina. The videos of the tanks came from Serbian tabloid media outlets, but they were not headed to the Kosovo border.

On 18 October 2021, the Gazeta Aktive Facebook page [shared an article](#) with a headline falsely claiming that Kosovo had closed the border with Serbia. This was shared a day after there was shooting at the Kosovo-Serbia border police cabin.

Women targeted by scammers

Despite Kosovo's efforts in its [National Strategy](#) on the Protection against Domestic Violence and Violence against Women and its Action Plan for the period 2022-2026, it is believed that many cases of gender-based violence - including online incidents – still go underreported. Online gender-based violence in the Balkans is often rooted, as Balkan Insight has reported, in [patriarchal norms and frequently goes unpunished](#). Failing to tackle online violent misogyny can lead to offline violence, discrimination against vulnerable individuals, and the exclusion of women and girls from public life.

On 13 December 2021, Kosovo feminist media outlet Grazeta [published a news](#) story warning about a website selling “sex pills” to facilitate the sexual abuse of women. In the Instagram advertisement for the pills, the sellers claim that “women who are under their influence can be abused more easily.”

FACT SHEET

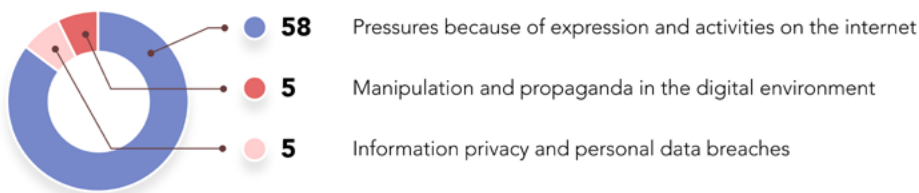
MONTENEGRO

TOTAL NUMBER OF CASES VERIFIED BY BIRN

65* CASES

Between September 1, 2021 and August 31, 2022

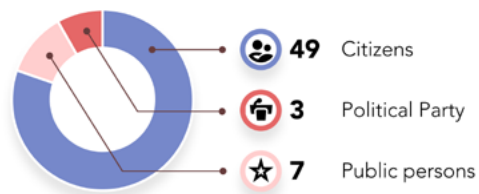
THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
6	7	6	6

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
4	5	6	6	5	4	6	4

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

In Montenegro, the majority of digital rights violations were logged by BIRN as pressure because of online expression/activities (58 incidents). Five incidents each were recorded for manipulation/propaganda and privacy and personal data breaches.

Journalists and political figures in Montenegro have received online threats, highlighting the deep political and ideological divisions in the country. In September 2022, the government of Montenegro [requested](#) assistance from foreign experts, including the FBI, in solving old cases of attacks on journalists in the country.

The European Affairs Minister emphasised the importance of solving these attacks to ensure media freedom in the country in the 2022 [report](#) on monitoring the actions of competent authorities in investigations of cases of threats and violence against journalists, murders of journalists and attacks on media property from 23 June to 5 December 2022, adopted by the Commission for Monitoring Violence against Media. The European Commission [has called](#) for more concerted efforts to protect journalists from attacks.

In Montenegro, there has been some progress in safeguarding freedom of expression, but there is still concern over the lack of effective follow-up on important cases. While the legal framework for protecting journalists has been enhanced with stricter penalties against attacks and threats, revisions to the framework and a new media strategy are still pending (Montenegro 2022 Report, pg. 6). Finally, the US State Department in the 2021 Country Reports on Human Rights Practices [noted](#) (pp. 16-17) that unsolved attacks against journalists remain a significant problem in Montenegro. No significant progress has been made in addressing the issue of attacks against journalists in the country so far.

Hate speech remains widespread in the country while vulnerable groups, such as the LGBTQ+ community and national and religious minorities, are systematically attacked online. Fake news and disinformation, following a general trend in the region, have largely touched on the topic of the war in Ukraine.

Journalists and public figures targeted

Social networks have been used in the country to launch attacks, threats and insults directed at journalists and politicians. On 24 October 2021, Milka Devic, editor of the local television station Gradska TV from Podgorica, was [threatened](#) on social

networks after she commented on a robbery in Niksic. Devic was threatened after her comments on prime-time news in which she said that participants in an armed robbery were supporters of the Serbian Orthodox Church.

Multiple cases of online harassment and threats against journalists have been reported on Facebook. In one case, a Montenegrin citizen [insulted](#) journalist Dragan Bursac on Facebook, warning he will be beaten during his vacation. Bursac posted messages he received on Facebook which said: "You don't deserve to live" and "Beware of the dark on streets of Budva," referring to the well-known holiday resort town on 17 February 2022.

On 15 April 2022, journalist Vladan Micunovic was also [insulted](#) on Facebook after he accused the public broadcaster head Boris Raonic of mobbing. In the comments section of the daily newspaper Vijesti's Facebook page, he was called "scum" and "a coward".

On 17 December 2021, Marina Jovic, an official from the ruling Democratic Front party, [insulted](#) and used offensive language about Prime Minister Zdravko Krivokapic and the Minister of Ecology, Spatial Planning and Urbanism, Ratko Mitrovic, on Facebook, after Krivokapic dismissed Jelena Kljajevic as the national parks chief.

In another case the same month, a Twitter user [insulted](#) and used sexist terms about Democratic Party of Socialists officials Drita Llolla, Amina Brahic and Nina Perunovic. Another Twitter user [threatened](#) politicians Aleksa Becic and Momo Koprivica of the ruling Democratic Montenegro party on 3 February 2022 over their statements about the government crisis and threatened to cause them harm.

Hate speech, fake news and disinformation

Online hate speech is a persistent problem in Montenegro, with vulnerable groups such as the LGBTQ+ community and activists for LGBTQ+ rights systematically targeted. On 3 May 2022, a Montenegrin citizen [called](#) the LGBTQ+ community "scum" and "[the] garbage of humankind" adding that they shouldn't "poison the young population with their sickness" in comments posted on an LGBTQ+ activist press release published on news outlet Vijesti's Facebook page.

In Montenegro, monitors also logged incidents of disinformation and fake news. On 3 April 2022, Twitter users [manipulated photos](#) of anti-Ukraine war protesters with an image of a swastika superimposed on a Ukrainian flag. Similarly, on 6 June 2022, a Facebook user in Montenegro [posted](#) false information about the war in Ukraine,

stating that President Putin's goal was not to take control of Ukraine but to eliminate Nazis in the country. The user also claimed that those who support Ukraine are fascists.

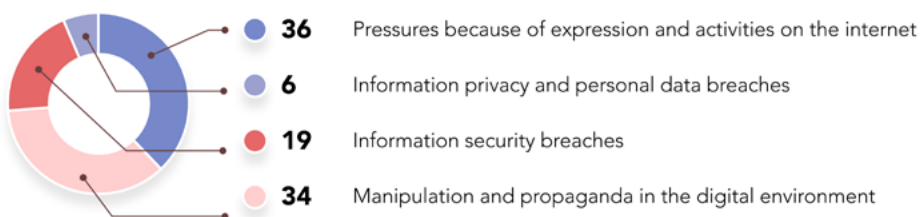
NORTH MACEDONIA

TOTAL NUMBER OF CASES VERIFIED BY BIRN

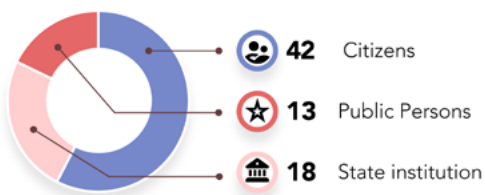
83* CASES

Between September 1, 2021 and August 31, 2022

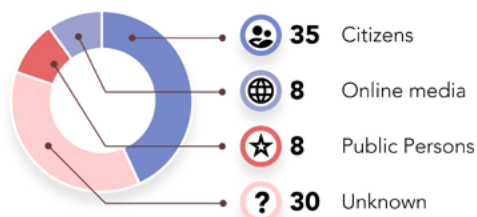
THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
4	5	4	4

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
4	4	5	4	5	8	10	31

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

In North Macedonia, the most frequently reported category of digital rights violations logged by BIRN were listed as "pressures because of expression and activities on the internet" (36 incidents) closely followed by manipulation and propaganda (34 incidents). Nineteen incidents of security breaches and 6 of privacy and personal data breaches were also recorded.

Following October 2022 [local elections](#) in North Macedonia and the subsequent resignation of Prime Minister Zoran Zaev, the political scene entered a new phase of [turmoil](#). Political and institutional instability dominated the post-election period. Since 11 November 2022, after the opposition's attempt to topple the centre-left government through a [no-confidence vote](#) failed, the political climate has [further deteriorated](#), prompting many politically-related digital rights violations.

Several violations targeted the ethnic Bulgarian minority in North Macedonia and the much larger Albanian minority, which further demonstrates how internal ethnic tensions are being exploited and exacerbated by online [far-right](#) propaganda. Our monitors recorded widespread usage of the highly derogatory and insulting term "[Ship-tar](#)" in reference to the Albanian minority on North Macedonian social networks. As Albanian commentator Butrim Gjonbalaj [explained](#), "Skiftar, Siptar, or Shiptar was a derogatory term used by Yugoslavians to insult Albanians and is basically the equivalent of calling [people of colour]... the N-word."

North Macedonian state websites were hacked despite government pledges to increase the security of institutional websites. The lack [of adequate training](#) of IT personnel to prevent hacking attacks and raise awareness of their effects is another issue.

Political tensions and ethnicity-based violations

Balkan Insight correspondent Sinisa Jakov Marusic [writes](#) that inter-ethnic hatred between large ethnic groups that finds expression online highlights that North Macedonia is a post-conflict society. Despite the great progress made toward achieving cohesion since the 2001 conflict between ethnic Albanian insurgents and the security forces, ethnic segregation and prejudice are still present.

On 6 November 2021, Shkodrane Dardishta, a member of the Board of Directors of Makedonski Telekom from the Democratic Union for Integration (DUI), an ethnic Albanian party and the third-largest party in North Macedonia, [posted](#) threats on Facebook of armed conflict if her party was forced into opposition. “We still have our combat boots in the attics of the old house – we can take off the white sneakers in a second. We are not orphans, we emerged after the war. Do not play with fire because, in the end, you will burn yourself”, she wrote. Both Makedonski Telekom and the DUI’s leader, Ali Ahmeti, [condemned](#) the statement.

In a [case](#) in January 2022, an anonymous Twitter user spread false claims about the contents of the North Macedonian dictionary, accusing its editors of allowing words and phrases deemed offensive to Macedonians, while throwing out words seen as offensive towards ethnic Albanian and Roma people. The tweet went viral and sparked an intense debate online.

In a [Facebook case](#) on 24 January 2022, administrators of a popular Facebook group posted pro-Bulgarian and anti-Macedonian content using the logo of well-known North Macedonian online media outlet SDK. SDK was similarly targeted by another Facebook group in 2018, ahead of that year’s referendum on EU and NATO membership.

On 25 August 2022, a Twitter user addressing the ethnic Albanian minority [wrote](#): “Why don't we too, like the Shiptars, start refusing to pay for electricity?” Similarly, a Twitter user [posted](#) that he “got into a fight with a ‘shipper’”, which was followed by several users also using derogatory words about ethnic Albanians in North Macedonia. On 23 August 2022, following a tweet published by a university professor who had criticised the government, a Twitter user [replied](#) that the large ethnic Albanian minority ought to be “removed from power”. The user said: “Only a general popular uprising can remove them from power.”

Online media outlet Plusinfo.mk [published an article](#) headline What awaits the Albanians? which targeted the Albanian minority: “They know their dream of a Greater Albania will never come true!” the article said, adding other derogatory phrases that claimed that the country’s ethnic Albanians are stateless and accused them of working against the country. Online media went on to say that Albanians are political spies whose sole aim is to destroy the Macedonian identity, state and culture.

Hacking and online fraud

In a [case](#) recorded on 4 February 2022, hackers calling themselves the “Powerful Greek Army” boasted that they had hacked the Ministry of Education and released footage that appeared to be from the ministry’s own video cameras. However, after [confirming that the attack happened](#), the ministry insisted the video footage published by the group was fake. Days later, scammers sent out mass phishing emails from a bogus email address similar to that of [North Macedonian Post](#). Many people reported receiving these suspicious messages, which asked them to make payments through a fake website. North Macedonian Post warned the public not to follow instructions given in these emails.

In one of the [most prominent cases](#) of digital rights violations in North Macedonia in the first half of May 2022, scammers targeted one of the biggest banks, NLB Bank and its customers, asking them for their personal data and accounts. The bank warned customers not to share any details with those asking for it, even if they said they were bank representatives.

On 26 August 2022, an online [raffle offering hundreds of fridges and cookers as prizes](#) appeared on Facebook under a fake profile called Technomarket Fans. The actual Technomarket, a Bulgarian retailer of consumer electronics, warned that the prize and the website were fake and an online scam.

FACT SHEET

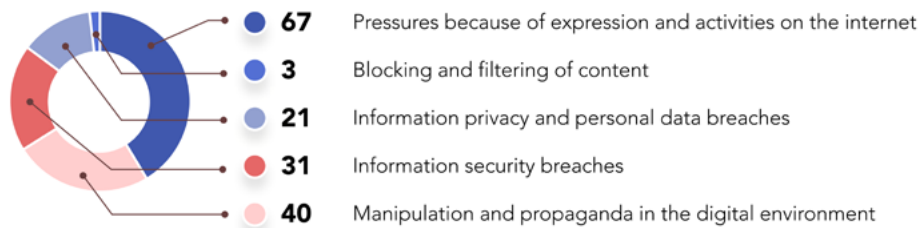
ROMANIA

TOTAL NUMBER OF CASES VERIFIED BY BIRN

128* CASES

Between September 1, 2021 and August 31, 2022

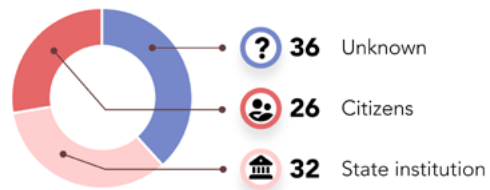
THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
9	12	8	10

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
10	13	13	10	12	13	9	9

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

The majority of recorded digital rights violations verified by BIRN in Romania were classified as pressures related to expression and internet activities (67 incidents), followed by manipulation and propaganda (40 incidents). Thirty-one incidents of information security breaches and 21 incidents of information privacy and personal data breaches were logged. The least frequently reported violation was "blocking and filtering of content," with only three incidents.

During the reporting period, Romania saw an alarming increase in nationalistic rhetoric. The Alliance for the Union of Romanians (AUR), the ultranationalist right-wing party active in Romania and Moldova, inflamed political tensions and ethnic-racial hatred.

Women continue to be targeted online by cases of misogyny, sexism and other cases of gender hatred, as was [highlighted](#) by the findings of the GREVIO Baseline Evaluation Report.

Political tensions and far-right rhetoric

The AUR party organised a [protest](#) in front of the Romanian parliament against the possible introduction of mandatory COVID vaccination passes and [criticised](#) the teaching of Holocaust and sex education in schools. Madalin Necsutu, BIRN's Balkan Insight correspondent for Romania, said in [an analysis](#) that observers believe the AUR party in Romania "sees anti-Semitism as a way to pick up new voters". AUR also launched a [campaign on Facebook](#) in January 2022 as part of which it listed Romanian media outlets that it deemed hostile. Cristian Pantazi, editor-in-chief of G4 Media, [told BIRN](#) that "by making public blacklists, AUR intends to intimidate journalists who honestly report [on] this party's facts, intentions and positions."

In a [case](#) recorded on 8 February 2022, Energy Minister Popescu complained that a verbal attack by AUR leader George Simion in parliament led to him and his family receiving threats on Facebook. "Since this happened, I have been targeted by an avalanche of insults and threats on my personal Facebook account. These threats appeared even under pictures of my children. They went too far this time. Some of the accounts are fake, and the whole action seems organised," [he told news outlet Libertatea](#). On 9 February 2022, the government [proposed amendments](#) to the rules of the chamber that would limit MPs' rights to live stream and video-record events inside parliament. Six NGOs criticised the change. "The ban on displaying banners in

the parliament, as well as the ban on recording and broadcasting live, is, in our view, a restriction on freedom of expression, which is a fundamental right, all the more protected when it comes to political debate,” they told [news outlet Libertatea](#).

Women harassed and abused online

Romanian women remain subject to frequent online abuse. In one case, two female police officers were [attacked online](#) on 19 August 2022 after a photograph was taken of them without their consent and posted on Facebook. In the photo, the two women appear to drink coffee and smoke cigarettes in front of a police station in Bucharest and both are wearing make-up. “These girls are some strippers, caught while preparing for a stag party,” wrote one user on Facebook. Another assumed that the two police officers were uneducated and had not studied at the Police Academy. “Wearing jewellery instead of police equipment. Instead of safety and protection, they offer us style,” another commented.

Anti-vaxxers and COVID-19 disinformation

On 19 October 2021, Piatra Neamţ County Police opened a [criminal investigation](#) into the spread of false information after a woman streamed herself on Facebook in front of a critical care ward, where COVID patients were being treated in Piatra Neamţ, north-east Romania. The woman, filming from a distance, claimed that “no one” was inside the clinic, suggesting the pandemic was a hoax. The video also became known thanks to a [Facebook post](#) by Oana Gheorghiu, cofounder of the NGO [Dăruiește Viață](#), who exposed the video as a hoax and reported the case to the authorities.

Another illustrative case concerned [Florentina Golea](#), a schoolteacher who was [harassed](#) after posting photos on Facebook while teaching a class of 12-year-old girls about the importance of vaccination. On 5 October 2021, RO vaccinare, the official page of the National Committee for Vaccination shared photos from the teacher’s profile on Facebook. After that, the teacher received hundreds of insulting comments via Facebook, describing her as a “profiteer”, “monster” and “criminal”. Golea also received death threats from people who claimed to know where she lived and the address of her school in Tecuci, in Galați County. Sorin Cîmpeanu, the Minister of Education, [announced](#) that he would support the teacher if she sued those who had harassed her on Facebook.

Cyberattacks and online scams

Large public companies and institutions in Romania have been frequently targeted by hacker groups linked to Russia. In a [case](#) recorded on 30 April 2022, the Romanian National Cybersecurity Directorate said its own website was temporarily taken down by a DDoS attack one day after key public institutions in the country were hit by a wave of cyberattacks claimed by Killnet, a pro-Russia hacking group. Another [case](#) occurred on 1 May when Digi24.ro, the most-read news site in Romania, remained offline for several hours after a DDoS attack, later also claimed by Killnet.

The most populous country in the region seems particularly exposed to large-scale frauds involving thousands of citizens. On 11 January 2022, Bitdefender cybersecurity experts working for one of the leading technology companies in Romania warned that a [phishing scam](#), first detected in July 2021, was now targeting email users, mainly in Romania, Croatia and Hungary. Hackers sent emails that appeared to respond to emails the targets had previously sent in which they claimed to have obtained passwords and even intimate images before demanding 1,200 euros in Bitcoin as ransom. According to Bitdefender, more than half of emails addressed to Romanian users were sent from local IP addresses.

FACT SHEET

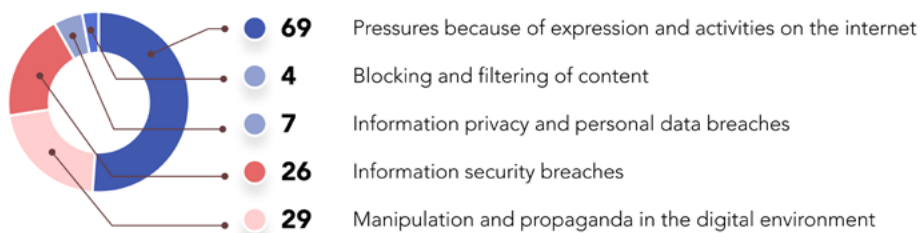
SERBIA

TOTAL NUMBER OF CASES VERIFIED BY BIRN

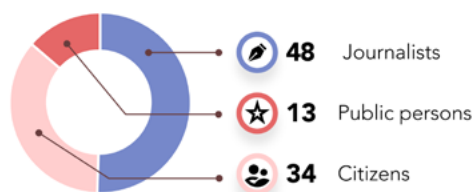
128* CASES

Between September 1, 2021 and August 31, 2022

THE MOST FREQUENT VIOLATIONS BY CATEGORY



THE MOST FREQUENTLY TARGETED PARTIES



THE MOST FREQUENT ATTACKERS



NUMBER OF VERIFIED INCIDENTS BY MONTH

2021

SEP	OCT	NOV	DEC
10	10	10	20

2022

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
6	11	12	13	5	6	9	12

* Some verified cases fall into multiple categories of digital rights violations. Similarly, more than one group of people and perpetrators may be included under the specific digital rights violation case.

Featured cases

The majority of digital rights violations recorded by BIRN in Serbia were classified as pressures because of online expression/activities (69 incidents), followed by online propaganda and manipulation (29 incidents) and information security breaches (26 incidents).

In Serbia, journalists' digital rights and freedoms are frequently violated. Almost 40 per cent of all digital rights violations logged were directed at journalists, including insults and death threats. The frequency with which journalists are targeted in Serbia has been noted by various country-based reports, such as the [2022 European Commission Report on Serbia](#), which reported: "Cases of threats and violence against journalists remain a concern and the overall environment for the exercise of freedom of expression without hindrance still needs to be further strengthened in practice".

Media outlets and individual journalists, especially women, reporting on political events in Serbia, including Kosovo-Serbia relations, were the target of many cases of online hate speech and threats. Aside from insults and threats to journalists, there were notable incidents of fake news, hacked accounts and personal data breaches. After Kosovo announced changes to Serbian-issued documents and vehicle licence plates, sparking tensions with Serbia, [numerous claims](#) that the two states were at war began to circulate on Twitter and other social platforms.

Fake information and conspiracy theories about the COVID-19 pandemic were widely shared in Serbia during this reporting period, including [claims](#) that those who were infected belong mainly to the LGBTQ+ community.

In addition, BIRN's database suggests many Serbian social media accounts are vulnerable to unauthorised access. In February 2022 the [Twitter account of Youth of JAZAS](#), a Serbian HIV prevention NGO was hacked. In July 2022, Women for Peace reported a [breach](#) of their email accounts and compromised correspondence.

Cyberattacks appear to have become more frequent, especially phishing campaigns, illegal data processing and personal data breaches. On 8 August 2022, scammers promoted a [fake online competition](#), falsely claiming that it was organised by the Post of Serbia. Users had to answer several questions and were told they had won a prize and to claim it they should forward the link to at least 20 friends and provide their email addresses and other personal information.

Journalists threatened and demeaned

Online intimidation, threats and insults are so commonplace as to be normal in Serbia. Journalists, as already noted, face [numerous online threats and insults](#) focused on discrediting their work. Journalists are also subject to online attacks by state officials and politicians. For example, the Serbian Prime Minister Ana Brnabic [tweeted](#) that journalists working for the daily Danas were “[eloquent liars](#)”.

Another attack came from SNS MP Lav Pajkić, who [compared](#) Danas daily’s journalists, N1 TV and Nova.rs to the Ustasha (the Fascist movement that ran Croatia under Nazi auspices during World War II) via his Instagram profile. In another instance, Simo Spasić, the president of the Association of Families of Kidnapped, Murdered, and Missing Persons from Kosovo, [threatened](#) the Južne Vesti journalist Aleksandar Stankov by sending him text messages filled with insults and vulgar language. Despite police warnings, Spasić continued to send messages, not only to Stankov but also to other media outlets and members of the prosecutor's office and police. All the messages were reported to the police and the Higher Public Prosecutor's Office in Niš, while the Prosecutor's Office has started the process of pursuing this as a criminal act of persecution.

In February 2022, Serbia-based journalist Nedim Sejdinovic [received threats and insults](#) via Facebook Messenger, which he reported to the Special Prosecution Office for High Tech Crime. Sejdinovic [was also insulted](#) via Twitter and called a “Serb-hater” by SNS MP Vladimir Djukanovic. This specific insult was made by Djukanovic after Sejdinovic wrote an article in which he criticised Djukanovic’s position in Serbian politics and law practice.

Environmental protesters and online threats

A controversial Rio Tinto lithium mining project in Serbia led to widespread [protests and criticism](#) over concerns the mines would cause significant environmental damage. Journalists (and their sources) faced serious threats - including death threats - for reporting on the protests. President Aleksandar Vucic criticised environmentalist NGOs and announced a potential referendum on the matter.

On the day of the protests, members of the Vranje police approached Dejan and Milena Dimic, editor and journalist at Vranje News. Milena Dimic said the police [warned](#) her not to appear at the environmental protest and that she would face criminal charges if she did.

Goran Jevremovic, the editor and owner of the Central Media online outlet from Jagodina, said that the police warned him that he would bear “legal consequences of violating public order and the peace” if he attended the protests.

The day before the environmental protests were held across Serbia, [serious threats](#) were sent to N1 TV staff and their families via email and social media. Public officials supporting the environmental protests in Serbia were not exempt from threats, including death threats.

War in Ukraine: Disinformation and hate speech

False information and propaganda can easily spread and gain traction online and this is particularly evident with regard to the conflict in Ukraine, where numerous Serbian online media [reported false claims](#) that US companies had bought up almost a third of the arable land in Ukraine. The claims originated on a website called Australian National Review and were spread widely via Facebook. In fact, Ukraine does not allow foreigners and foreign-owned companies to buy agricultural land.

In another case, the Twitter account of the Yugoslav Youth Association Against AIDS (Youth of JAZAS), an NGO committed to HIV support and prevention, was [hacked](#) by an unknown person on 25 February 2022. Tweets from the hacked account said that “Ukraine is AIDS” and claimed that Russia was “the cure”. The next day, after regaining control of the account, Youth of JAZAS [apologised](#) for the tweets. Also, Twitter [flagged](#) a picture tweeted by Serbia’s Eurovision song contest entrant Ana Duric Konstrakta. The image featured tables that were said to be arranged in the shape of the letter Z and was therefore interpreted as a sign of support for Russia’s invasion of Ukraine.

Phishing and cyberattacks

During the reporting period, the National Cybersecurity Emergency Response Team of Serbia warned of several phishing campaigns.

One relates to the [Digital Green Certificates](#) which record vaccination against COVID-19. Emails were sent out that contained a link to download an electronic document about their vaccination status. National CERT of Serbia advised that the only legitimate issuer of the Digital Green Certificate in Serbia is the Office for Information Technology and e-Government and that when citizens receive a message from

another alleged issuer of the Digital Green Certificate, they should disregard it. National CERT [also warned](#) Facebook users about a phishing campaign aimed at compromising their account credentials. Users were getting messages asking: "Are you in this video?" which also contained a link to malware that would enable scammers to obtain personal data.

Several well-known companies, such as the Serbian branch of Banca Intesa and the Post of Serbia, informed citizens about [phishing campaigns](#), [false ads](#) and [fraudulent emails](#) with malicious attachments which aim to collect citizens' personal data. Companies advised their clients not to open the fake links and not to follow instructions in these emails.

Finally, Serbian media also faced cyberattacks, including one against the Beta News Agency in April 2022, when Beta's website crashed due to a [DDoS attack](#), allegedly launched from abroad. It is not known who the attacker was.

Conclusion

BIRN's 2022 annual report on digital rights violations identified key trends in digital rights violations, including the spread of hate speech, disinformation and cyberbullying, which significantly threaten freedom of expression and access to information. The report emphasises the need for more robust accountability measures to address these issues and highlights the importance of raising public awareness and promoting the responsible exercise of freedom of speech in both online and offline domains. By bringing attention to these critical issues, BIRN aims to ensure that policymakers, civil society organisations and citizens are better equipped to protect and promote digital rights now and in future.

It seems inevitable that digital rights violations will constantly evolve. As such, it is not always easy to categorise or capture all of them with our current methodology and definitions. Therefore, our future work in the field should focus on refining our approach to better adapt to the changing landscape of digital rights violations and ensure we accurately capture the full range of violations in the region. This may involve developing new categories or criteria for identifying incidents and regularly updating our definitions and research methods to stay current with emerging trends and tactics used to undermine human rights and democracy online.

In addition, we will prioritise building partnerships and collaborations with local organisations and communities to ensure that our work is grounded in the perspectives and experiences of those most directly affected by digital rights violations. [The South East Europe Digital Rights Network](#) is part of these endeavours.

Recommendations

These recommendations are primarily aimed at policymakers and regional regulators, individuals and organisations working in media and technology. The purpose is to promote and protect digital rights in online media and journalism, including freedom of expression, access to information, and privacy.

The recommendations that BIRN has identified include: making all types of online aggression illegal; providing specific training and resources to law enforcement authorities and prosecutors; taking interim measures to combat hate speech; prioritising the development and implementation of robust cybersecurity measures; collaborating with local civil society players on content moderation and freedom of speech; and improving data collection to combat hate speech and hate crime.

BIRN believes that by following these recommendations, policymakers and regulators can help ensure that digital platforms and technologies are designed and used to respect users' rights and freedoms. However, we recognise a pressing need for a better legislative framework and implementation regarding online crimes, as many of these offences remain largely unregulated. Therefore, policymakers must prioritise the development of clear and compelling regulations to protect online journalists and ensure their safety while conducting fact-checking and ethical journalism activities.

Better legislation and effective implementation will help media professionals and organisations enhance the quality and credibility of their reporting, fostering greater public trust in the media. Ultimately, we hope these recommendations will contribute to a healthier, more vibrant digital public sphere where diverse voices can be heard and informed public debate can flourish.


1. We ask governments and lawmakers in the region to make all types of online aggression illegal, such as, but not limited to, cyberstalking, cyberbullying, doxing and non-consensual intimate image abuse. This would require clear and comprehensive legislation prohibiting internet abuse and the subsequent re-sharing of damaging information. For instance, in Bosnia and Herzegovina, the legislative framework for regulating hate speech needs to be more closely aligned with European standards. The report conducted by South East European Network for Professionalization of Media Youth revealed that despite evidence of an increase in hate speech in Bosnia and Herzegovina, only 12 convictions for hate speech were issued by courts from 2004 to 2019 (see p. 11 of [the report](#)). In February 2023, BIRN Bosnia and Herzegovina and the Centre for Judicial and Prosecutorial Training of Federation of Bosnia and Herzegovina [presented](#) the most recent

findings on processing hate crimes in Bosnia and Herzegovina based on data from BIRN's database [Mapping Hate](#), which was [launched in 2021](#) and documents hate speech, discriminatory rhetoric, the incitement of hatred and the denial of genocide and other war crimes in Bosnia and Herzegovina.

2. Law enforcement authorities and regional prosecutors should have access to specific training and resources, such as forensic tools and technical knowledge, to implement these laws. In this regard, a coordinated response across several agencies and groups, such as victim support organisations, mental health specialists, and technology corporations, is also required to give help and services to victims.
3. All relevant authorities in the region should implement interim measures to improve the prosecution of online offences. This includes the use of existing legal provisions, in particular discrimination laws, media laws and criminal law. For example in Serbia, a [Council of Europe \(CoE\) report on the use of hate speech in Serbian media](#) shows that despite a very solid legal framework to combat hate speech (pp. 23-29), existing laws do not seem to be properly implemented. Even though several laws regulating hate speech in Balkan countries do not contain provisions explicitly regulating online hate speech, relevant authorities should interpret and apply existing legislation considering contemporary trends and issues including, for example, tackling online gender-based violence and hate speech that women and girls face. It is essential the authorities proactively enforce these existing legal provisions to hold those who engage in online hate speech accountable and prevent further violations of digital rights.
4. Given the increasing number of cyberattacks in the Balkans, governments and institutions must prioritise developing and implementing robust cybersecurity measures. Cyberattacks across the region targeting state websites show the need for increased attention and investment. To address this challenge, governments should prioritise the [training of IT personnel](#) and raise awareness of the potential impacts of cyberattacks. Developing adequate prevention systems and response plans is also essential and should be regularly reviewed and updated. Additionally, governments should consider collaborating with neighbouring countries to share best practices and leverage collective expertise. In particular, the Budapest Cybercrime Convention provides a framework for international cooperation in the fight against cybercrime. Serbia's [ratification](#) of the Budapest Convention, along with its Additional Protocol on Xenophobia and Racism Committed through Computer Systems, is a positive example. However, practical implementation challenges persist, as shown by the difficulties of the Prosecution Office for Cybercrime in

Belgrade in keeping up with the increasing number of incidents and the growing backlog of cases.

5. The urgent need for regional governments to provide adequate resources to their respective cybercrime prosecution authorities is also highlighted by the situation in [Romania](#) where, although 1,335 cybercrime cases were closed in 2020, over 4,000 cases remain pending since 2018, highlighting the need for continued investment in cybercrime prevention and prosecution efforts. Overall, the threat of cyberattacks in the Balkans is a complex and evolving challenge that requires a coordinated and sustained effort from governments, institutions, and individuals alike. By prioritising cybersecurity and investing in necessary resources, the region can better protect its citizens and institutions.
6. Social media corporations should collaborate with local civil society players and form local coalitions on content moderation and freedom of speech to ensure fair and effective content moderation. By partnering with local civil society organisations, social media corporations can better understand the local cultural and social context and the nuances of local languages. This information can inform content moderation processes, allowing for more effective and culturally sensitive moderation. Furthermore, local coalitions can bridge the gap between social media corporations and local communities, which may have different perspectives on freedom of speech and what constitutes hate speech. By engaging with local coalitions, social media corporations can demonstrate their commitment to addressing hate speech and promoting freedom of speech in a way that respects local cultural values and norms. Local coalitions could provide necessary training and support to civil society activists affected by online hate speech.
7. Addressing hate speech through improving data collection is also crucial to combating hate speech and hate crime in the Balkans. To achieve this, governments and relevant institutions should prioritise developing and implementing robust data collection systems that enable the collection of comprehensive and reliable data on hate speech and crime. This data should include information on the nature and frequency of hate speech and hate crime, as well as the groups and individuals who are most affected. To ensure the effectiveness of these data collection systems, governments and institutions should also prioritise training relevant personnel on data collection, analysis, and interpretation. Additionally, the collected data should be regularly reviewed and analysed to identify trends and patterns and to inform the development of evidence-based policies and interventions to combat hate speech and crime.



It is vital that governments and institutions in the Balkans collaborate and also work with international stakeholders such as the European Union and the Council of Europe, to share best practice, exchange information and leverage collective expertise in the area of hate speech and hate crime data collection. The collaborative network of equality bodies combating hate speech provides an excellent example of this type of collaboration and exchange.



March, 2023