DIGITAL RIGHTS IN A TIME OF CRISIS: AUTHORITARIANISM, POLITICAL TENSION AND WEAK LEGISLATION BOOST VIOLATIONS

Digital Rights Violations Annual Report 2022-2023

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK

BIRN Network Regional Director

Milka Domanovic

Editors

Hamdi Firat Buyuk,

Journalist and Balkan Insight Turkey correspondent

Ivana Jeremic,

Editor at Balkan Insight

Milos Ciric,

Digital Rights Programme Manager,

BIRN Hub

Copyediting

Matthew Collin

Lead Researcher

Matteo Mastracci

Digital Rights Project Manager

Amina Mahovic, BIRN Hub

Design

Milica Novakovic

Authors of country reports

Albania: Nensi Bogdani, BIRN Albania

Bosnia and Herzegovina: Aida Trepanic, Semir Mujkic, BIRN Bosnia and Herzegovina; Azem Kurtic, BIRN Hub

Croatia: Matej Augustin

Hungary: Ákos Keller

Kosovo: Diedon Nixha, BIRN Kosovo

Montenegro: Djurdja Radulovic; Samir Kajosevic (BIRN Montenegro) contributed to monitoring

North Macedonia: Bojan Stojkovski, BIRN Hub; Goce Trpkovski, BIRN Macedonia

Romania: Adina Florea; Marian Chiriac (BIRN Romania) contributed to editing

Serbia: Tijana Uzelac, Kalina Simic, BIRN Serbia; Bojan Perkov (SHARE Foundation) contributed to monitoring

Turkey: Hamdi Firat Buyuk, BIRN Hub

This publication is co-funded by the European Union. Its contents are the sole responsibility of BIRN and do not necessarily reflect the views of the European Union. The publication is also made possible through support from the UN Democracy Fund.

Co-funded by the European Union

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK

Reporting Digital Rights & Freedoms

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BIRN's Digital Rights Violations Annual Report 2022-2023 provides extensive information about and analysis of digital rights violations in Albania, Bosnia and Herzegovina, Croatia, Hungary, Kosovo, Montenegro, North Macedonia, Romania, Serbia and Turkey. From September 1, 2022, to August 31, 2023, BIRN registered cases of digital rights violations and added them to its database, which has been established in 2020 in partnership with the SHARE Foundation.

During this reporting period, there has been an increase in the number of cases registered in the BIRN database compared to the last reporting period. The total number of documented violations rose from 782 to 1,427, underscoring how challenges in the digital sphere have also increased. Hate speech and discrimination, digital manipulation and computer fraud were the most common categories of digital rights violations registered by BIRN.

Montenegro, Kosovo, Bosnia and Herzegovina and Croatia saw rises of 112, 102, 80 and 64 cases in this reporting period, respectively. Domestic political developments, as well as regional and international tensions, greatly contributed to the increase in rights violations in the digital sphere. Elections and intense polarisation within society shaped the digital landscape in Bosnia and Herzegovina, Montenegro, Turkey and Hungary. Regional and international crises such as the tensions between Kosovo and Serbia and Russia's war against

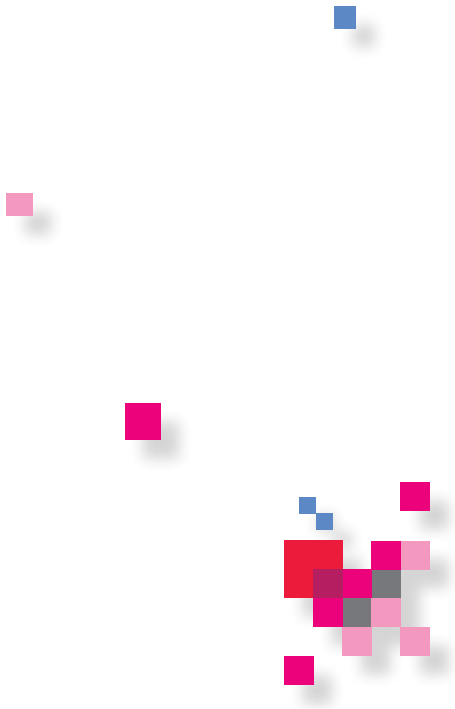
Ukraine only fuelled digital rights violations in the region, which is susceptible to malign influences.

Such an environment allowed online hate speech and discriminatory rhetoric to flourish across the region, especially against vulnerable groups including the LGBT community, women and ethnic minorities. The governments in Albania, Hungary, Serbia and Turkey continued to abuse digital rights using various tactics and methods including takeovers of independent outlets by pro-government businesspeople, paid online propagandists, intervention by government agencies and court action. Such governments often used legislation to increase their control over the internet and impose censorship, causing alarm among rights groups. Almost all the countries monitored by BIRN are preparing new legislation to counter digital threats, particularly disinformation campaigns. However, new measures should not be taken at a cost to digital rights and freedoms, as has already happened in Hungary and Turkey. Meanwhile journalists and online media continued to be the major victims of digital rights violations in the countries monitored, where existing legislation offers little or no protection for journalists who face digital violence.

Technological infrastructure in most of the countries BIRN monitored remains weak and has proved to provide inadequate defence against cyberattacks. In Montenegro, North Macedonia and Albania, government agencies and services were repeatedly targeted by cyberattackers throughout the reporting period. In these three Western Balkan countries, but also in other countries like Croatia, Kosovo, Turkey and Serbia, citizens' private data was reportedly leaked due to cyberattacks, scams and phishing activities, as well as because of mismanagement by the relevant authorities. Under these circumstances, new technological advancements present new digital challenges, particularly the malicious use of artificial intelligence, which has the potential to become a major digital rights and security issue in the coming years.

The introduction to this report shows the similarities and differences in the digital challenges being faced by the countries monitored. The introduction

is followed by detailed country reports based on violations registered in BIRN's database over the reporting period, experts' opinions and BIRN's own insights. At the end of the report, BIRN offers a set of recommendations for stakeholders including decision-makers, international organisations and governments, the private sector, media outlets, civil society groups and the public.



INTRODUCTION

In all the countries monitored by BIRN, there were multiple digital rights challenges during the reporting period from September 1, 2022, to August, 31, 2023. Notably, we observed an increased number of documented violations from 782 to 1,427. This rise may be attributed to BIRN's heightened monitoring efforts introduced in 2023, including the implementation of a monthly submission quota for BIRN's monitors. While most digital rights violation trends are prevalent across multiple countries, issues unique to specific countries also emerged.

BIRN documented concerning trends, noting a range of digital rights violations across all the monitored countries. Kosovo led with 191 cases, closely followed by Montenegro with 177 incidents, indicating the seriousness of the situation. BIRN logged 169 and 154 violations from Romania and Hungary, respectively, providing clear evidence of the rise in reported incidents. North Macedonia and Croatia reported 144 and 134 incidents, illustrating a rising challenge in the region. Bosnia contributed 157 cases to this pattern. Albania's disclosure of 156 violations recorded by BIRN signifies its scrutiny under BIRN's observation. 103 violations that BIRN logged from Serbia emphasises ongoing challenges requiring continuous attention. Additionally, BIRN's documentation of 42 violations in Turkey, in period July 2023-September 2023, adds to the growing concerns highlighted in the report.

The predominant areas for digital rights violations were hate speech and discrimination, digital manipulation and com-

puter fraud. Domestic, regional and international political developments made a direct impact on digital rights violations. During domestic crises and elections, digital rights violations spiked, as they did at times of regional and international tensions. The governments across the region remained major digital rights abusers. In patriarchal, politically polarised and ethnically-divided countries, vulnerable groups, particularly the LGBT community, minorities and women are often targeted online using hate speech and discriminatory rhetoric.

Legislation in most of the countries BIRN monitored remained weak and ineffective in countering digital rights violations. In some countries, new legislation was used to target critics and independent media by autocratic regimes. Proposed legislation that is in the planning stages also alarmed rights groups due to fears that it would allow governments to increase control over the digital arena. In most of the countries monitored, citizens' private data remained unprotected, with little effort or willingness shown by governments to ensure its security. There was also a lack of government effort to tackle online fraudsters, with perpetrators often going unidentified and unpunished. Cyberattacks paralysed some countries' government agencies and most countries' capacities to counter cyber threats remained low. In parallel with global trends, technological advancements in areas like artificial intelligence, as well as autocratic governments' deployment of advanced technological tools, present new challenges such as the malicious use of AI and digital censorship.

Digital Abuses by Autocratic Governments

During the reporting period, countries with autocratic governments remained the major abusers of digital rights, using courts, government agencies, pro-government media owners, teams of paid online propagandists and other tools to exert influence. In Turkey, President Recep Tayyip Erdogan's government increased its control over digital spaces during a major natural disaster and during elections. Following complaints about the slow official response to twin earthquakes in February 2023, the

government blocked most access to X (formerly Twitter) – a main source of communication for relatives of victims, survivors and aid campaigners. The government said it made the decision to counter disinformation and fake news, using the authority granted by a new law adopted in 2022. Turkish courts also ordered the removal of tens of thousands of online articles and blocked access to social media posts. Most of the content that was taken down or blocked was critical of government policies or was about people linked to the government, **President Erdogan's family** or influential leaders of organised criminal groups.

In Hungary, Viktor Orban's government dominates the media and internet with its apparatchiks. According to watchdog group Reporters Without Borders' annual World Press Freedom Index, Hungary **ranks 72nd** out of 180 countries worldwide in terms of media liberties, whereas in 2010, it was 23rd. Meanwhile, Freedom House labels Hungary **partly free** in terms of internet freedom. The reason for the decline in liberties is that under Orban's government, which has been in power since 2010, several independent media outlets, like Nepszabadsag, were forced to close down or were taken over, like Index or Origo, by allies of the ruling Fidesz party.

In Serbia, a **list** of over 14,000 suspected propaganda accounts on social media allegedly associated with Serbia's ruling Serbian Progressive Party was posted on X. The list, complete with names and locations of the people allegedly behind the accounts, implicates individuals from the public sector across the country, raising serious questions about their involvement in political activities during work hours. According to the list published by **Fake News Tragac**, ("FakeNews Seeker"), a specialised platform that fights disinformation in Serbia by tracking and fact-checking the news in the country, there were 3,162 individuals engaged in online propaganda activity on behalf of the Serbian Progressive Party. As new elections loom in Turkey, Serbia and Hungary, experts fear that these countries' governments will increase their violations to further tilt the online environment in their favour.

Regional and International Crises Increase Digital Violations

Digital rights violations were affected by regional and international crises as the Balkan region and Europe faced multiple security crises. Russia's war against Ukraine continued to have a malign influence, causing the spread of misinformation.

Bosnia and Herzegovina still represents fertile ground for Russian influence. The Russian Federation's embassy in Sarajevo often expresses its views on social networks, spreading disinformation and denying the crimes committed by Russia during its invasion of Ukraine, such as promoting the **view** that the massacre in Bucha was staged. In tandem, the website of Radio-Television Republika Srpska, the Serb-run entity-level public broadcaster, also promoted **Russian disinformation** about the war. There were also **public gatherings** supporting the Russian invasion of Ukraine, which were reported by mainstream media and then amplified online.

Since the beginning of Russia's full-scale invasion of Ukraine, many countries have seen an increase in disinformation campaigns. In Romania, an unexpected target was been the army, traditionally one of the most trusted institutions in the country, according to **Bertelsmann's 2022 Transformation Index**. **In March 2023**, the Romanian Defence Ministry warned the public to be wary of posts about an alleged general mobilisation, which had gone viral on TikTok and Instagram. This also happened in **February 2023** and in **October 2022**, as well as in the first two months of the Russian invasion of Ukraine.

Regional tensions also added to digital rights violations. Ethnically-charged incidents in the summer of 2023 in the Serb-majority north of Kosovo led to a tense political atmosphere in which the number of **attacks on journalists** and activists **increased** particularly against those who criticised Serbia's ruling party or the **Orthodox Church.** Violent confrontations erupted between local Serbs in northern Kosovo and peacekeepers from NATO's Kosovo force, KFOR. Such incidents not only heightened tensions but also fuelled the spread of misinformation, **hate speech and fake news**

on digital platforms, as evidenced by BIRN's monitoring.

Online Attacks on LGBT People, Women and Minorities

As domestic, regional and international politics remain tense and societies in the countries monitored by BIRN remain patriarchal and highly polarised, vulnerable groups such as women, the LGBT community and minorities have been targeted in the digital arena across the region. In Albania, LGBT activists and civil society organisations were targets of several online hate speech attacks on Instagram and Facebook, such as the case in March 2023 of **Zhakline Lekatari**, an LGBT activist, journalist and blogger on sex education and identity, who said that she had to undergo psychotherapy due to the continuous online attacks on her on social networks because of her activism for LGBT rights and sex education.

Online attacks against LGBT people also represent a major concern in Hungary. The government is believed to be fuelling this campaign, mainly **targeting transgender people** and claiming that LGBT people direct propaganda at children. Hungarian government officials have continuously targeted the LGBT community online, **intentionally conflating** LGBT people with paedophiles.

In Turkey, LGBT groups, Pride events and supporters of LGBT rights are often targeted by Islamist and nationalist groups associated with President Erdogan and his allies. Turkey's world and European championship-winning women's volleyball team was also targeted for online bullying and hate speech. Ebrar Karakurt and Melissa Vargas, two of the players who contributed greatly to the championship victories, came under attack from Islamist groups in Turkey due to their sexual orientation. In an organised social media smear **campaign**, which involved senior members of Erdogan's ruling party, Islamists targeted the two players with homophobic comments and condemned the team for wearing uniforms that they said were unacceptable under Islam.

In Bosnia, on August 11, 2023, Nermin Sulejmanovic, a man from Gradacac, livestreamed the murder of **his wife**, **broadcasting the murder on In-**

stagram. Sulejmanovic also killed two other people and wounded a further three that day. It took more than three hours for Instagram to react, **leaving** the video available for all users to watch in the meantime.

In Romania, there was a trend towards sex-related crimes perpetrated using digital methods. The victims used to create pornographic content were often children and women whose explicit images were distributed online without consent. **A significant incident** happened in October 2022 in northern Albania, highlighting how digital harassment can cost lives. According to media reports, it all began with a threat on social media and ended with a double murder and a suicide.

The European Institute for Gender Equality said in **a report** that cyber violence against women remains a prevalent issue in the Western Balkans and Turkey. "Numerous legal gaps persist, including those related to the Istanbul Convention, which is a treaty designed to combat violence against women and domestic violence. Additionally, there are significant shortcomings in data collection, making it difficult to gain a comprehensive understanding of the extent and nature of this problem," the report said.

As well as LGBT people and women, minorities were often victims of digital rights abuses. Ethnically-motivated hate speech persisted in North Macedonia as well as discriminatory rhetoric against LGBT people, as in previous years. In one instance, controversial TV host Milenko Nedelkovski used Facebook to **propagate hate speech** about a journalist of Albanian descent.

In Montenegro, minority groups were targeted in more than half of the 26 cases registered by BIRN under the category of "online hate speech and discrimination". In 11 incidents, **Serbs** and members of the **Serbian Orthodox Church** were the targets. In three cases, **Bosniaks** and **Muslims** were the targets. In these cases of ethnic intolerance, the perpetrators were mostly members of the public, but also included media outlets and public figures.

Journalists Remain Major Targets of Online Attacks

Journalists across the region were regular victims of digital rights violations. In Albania, journalists were often targets of online attacks or smear campaigns. Both journalists and media owners face restrictions of their activities and freedom of expression due to attacks aimed at damaging their reputations. In July 2023, the mayor of Tirana, Erion Veliaj, **called** investigative journalist Ola Xama a "militant" and a "contract killer" in WhatsApp messages after her **investigation** for BIRN about disputed waste concession contracts was published.

In Turkey, RTUK, the government agency to monitor media, imposed a series of fines on independent media platforms. The European Centre for Press and Media Freedoms, ECPMF and its partners **accused** RTUK of having become a government tool to silence media and online critics of President Erdogan. A **report** published by Germany's Friedrich Naumann Foundation for Freedom claimed that Turkey is copying the Russian 'playbook', using the judiciary to silence critical journalism and freedom of expression.

Hate speech in Serbia, particularly directed at activists, **journalists**, and public figures because of their views, is not uncommon. Serbia has witnessed at least 16 cases of hate recorded by BIRN,, but no substantial action has been taken by the authorities to prevent such incidents in the future. This has created an atmosphere in which it is considered normal to direct insults and threats at activists and journalists. Journalists' Safety in the Digital Environment, a **report** published by BIRN Serbia and the Independent Journalists Association of Serbia, IJAS, took a closer look at the growing online security threats faced by journalists in Serbia. It said that in recent years, there's been a troubling rise in the number of attacks and incidents of pressure exerted on journalists in the digital sphere. The report noted that in 2020, there were 53 online attacks, with 51 in 2021 and 52 in 2022.

In Turkey, **according** to the Media and Law Studies Association, more than 79 percent of journalists have been attacked online at least once. In Monte-

negro, journalists were also victims of online insults, threats, hate speech and falsehoods aimed at damaging their reputations, BIRN found. There were around 30 cases of digital violations aimed at journalists and online media in the country; half of the perpetrators were people writing in the comment sections of online media outlets.

In Hungary, journalists and online media also became victims of online attacks. DDoS attacks on independent media outlets increased in frequency. In the previous reporting period (2021-2022), BIRN documented just two cases, whereas in the current (2022-2023), the number rose to 20. During the attacks, the websites that were targeted were inaccessible to readers for hours or **even days,** and caused the outlets financial losses.

Cyberattacks, Phishing and Scams

State institutions and members of the public were targeted by cyberattacks and online fraudsters in the countries monitored by BIRN, as well as media outlets. In Montenegro, consequences of the August 2022 **cyberattack** on the country's public administration persisted throughout 2023, causing significant damage. Despite assistance from abroad, Montenegro did not manage to discover who was behind the attack, nor to resolve problems it caused for several months.

In North Macedonia, cyberattacks also targeted state institutions. The country witnessed a **significant rise** in cyberattacks, with various hacking incidents registered. One **prominent example** was when the BlackByte ransomware hacking group allegedly targeted the nation's agriculture ministry. The consequences of this **severe attack** were far-reaching, as ministry employees endured a complete loss of internet access within the ministry premises for more than a month. In Albania, a series of continuous cyberattacks started in September 2022, in which Albanian governmental servers and databases became the target of 32 hacker attacks. The government has linked the attackers to Iran, although the perpetrators remain **unknown.**

Online fraudsters targeted the public and often went unpunished due to gov-

ernments' lack of capacity or legislative measures to address the problem. Online scams became a frequent occurrence in Kosovo, according to BIRN's monitoring, with perpetrators using social media posts to direct users to non-secure websites. In parallel, certain Facebook pages offered apparently enticing loan deals with **favourable conditions**, targeting would-be entrepreneurs or those in financial need. The purported deals lured victims with low interest rates for various purchases, from appliances to real estate. A concerning aspect involved the use of names of real people from outside Kosovo, connected to questionable addresses and phone numbers for communication via WhatsApp.

In North Macedonia, unknown perpetrators used stolen data to apply for quick loans online without the knowledge or consent of the victims. The victims, who included a **person with disabilities**, a hospital **nurse** and a **farmer**, found themselves indebted to quick loan companies operating within the country. The Macedonian Ombudsman **called** on state institutions to address the issue and take robust measures to prevent future scams. A series of online scams and fraud attempts were also registered in Albania over the past year. The first months of 2023 saw 17 attempts by scammers to deceive the public by using fake identities on social networks to steal considerable amounts of money.

The EU's so-called **Tirana Declaration** in December 2022 recognised the lack of capacities and strategies in Western Balkan countries to deal properly with cybersecurity issues. In the declaration, the EU said the European Cybersecurity Agency and EU member states will support governments in the region to tackle their problems. In an effort to respond to recent large-scale cyber-attacks in the region, the EU launched a five-million-euro programme in early 2023.

Citizens' Private Data Inadequately Protected

State institutions and citizens in several countries were targeted by cyberattacks and scams, and citizens' data was stolen in various incidents, mostly due to governments' inability to protect it properly. Governments' responses to these

incidents were often ineffective and the attackers were not identified.

The Albanian authorities' rapid digitalisation programme moved forwards as 95 percent of public sector services that were previously provided in person at offices were made accessible online through the e-Albania platform in May 2022. While this transition promises efficiency, it also presents challenges, particularly for older people and other vulnerable groups who may struggle with using the digital interface. Privately owned 'service points' have been providing paid assistance with using the e-Albania platform for those who need it. However, they operate without regulatory oversight, **raising concerns** about data handling and accountability, such as third-party access to citizens' private data, passwords and accounts, and the need to pay extra costs for the services.

In June 2023, Turkey **recorded** the worst online data breach in its history. A website called sorgupaneli[dot]org offered to provide Turkish citizens' private data that had been stolen from the e-Devlet government services website, even claiming to be able to offer President Erdogan's personal information. The hacked information being offered for free by the website in return for a membership signup included ID numbers, phone numbers and information about people's family members. More sensitive information, including full addresses, real estate deeds and education details, was offered with a paid premium membership.

In Croatia, BIRN recorded two major personal data breaches. In March 2023, EOS Matrix, a debt collection company, faced accusations that it had leaked its databases, compromising over 181,000 personal records, including minors. This followed a personal data breach at debt collection company B2 Kapital, which was discovered in December 2022. The Personal Data Protection Agency **imposed a fine** of 2.26 million euros on B2 Kapital.

In Serbia, lives were put at risk due to personal information leaks. A mass shooting at the Vladislav Ribnikar school in Belgrade in May 2023 was the **trigger** for privacy and personal data breaches, data leaking and **illegal data processing**. After the school shooting, the chief

of the City of Belgrade Police Department revealed the first and last name of the underage perpetrator and showed a list of children that he had intended to kill. On the same day, Serbian President Aleksandar Vucic also revealed private information about the teenage shooter. In the aftermath of the shooting, police took action against people who glorified the teenage murderer, resulting in **several arrests.** Twenty-nine elementary school students were arrested for copycat attacks (mostly without weapons) or for celebrating the murders online. Criminal charges were filed against 82 **individuals** within a month of the mass shootings.

AI Presents New Digital Challenges

As the use of artificial intelligence tools increases, new challenges are being posed for digital rights and security. The Bosnian digital environment reflects the divisions within society, and AI-generated content becomes more and more prominent. Russian sympathisers or allies frequently use new technologies and social networks to promote pro-Russian propaganda in the Balkans.

Another recent example of unethical usage of the AI was a news piece about Serbia **purportedly ordering** 20,000 Shahed drones from Iran, which was entirely generated by AI. It was then republished by other media outlets despite being incorrect. The rise of fake accounts and fabricated content made using AI was also notable in Serbia, with 12 cases documented during 2022-2023. Despite the government's **2020-2025 AI Development Strategy** and associated **Ethical Standards**, which it adopted in March 2023, no regulations specifically address AI-generated media content. This regulatory gap leaves **the field unchecked.**

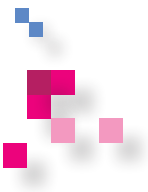
Unlike most countries covered by BIRN monitoring, the Romanian government decided to address the misuse of new technologies, including AI. In June 2023, the Romanian parliament's upper house voted in favour of a **bill** meant to outlaw the "malicious use of technology" by restricting the use of deepfakes. After it is approved by the upper house, it will become the first legislation in Romania to address the responsible use of AI, one of the last countries in the EU lacking

a national strategy on AI **according to the government**. Lawbreakers will face a fine of 2,000 to 20,000 euros from the National Audiovisual Council, with a maximum fine of 40,000 euros being given to repeat offenders.

Artificial intelligence and digital surveillance were not major issues in Turkey in 2023, but several developments suggested that they could posed threats to digital rights and freedoms in future. In May 2023, four former executives from the Munich-based FinFisher company, which develops spyware, were **charged** with illegally selling software to Turkey's secret service so it could spy on the country's opposition. Turkey also announced in September 2022 that it is developing its own digital surveillance system that will obtain, process and store data from digital media to transmit it quickly to **state authorities**.

The Need for Effective Legislation

In the majority of the countries monitored by BIRN, governments have yet to introduce effective legislation to counter digital threats including cyberattacks, the use of AI, private data security breaches, disinformation and online scams. 2024, politicians are likely to consider new legislation in Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro, Romania and Serbia as countries seek to counter multiple digital challenges. However, rights groups remain worried as governments often aim to use new legislation to increase their control over digital platforms, social networks and online media, as exemplified by the cases of **Hungary** and **Turkey**. For instance, in Croatia, **a proposed new Media Law** have caused controversy among journalists who see it as a potential threat to media freedom. The Croatian Journalists' Association argues that the draft law legalises censorship, granting publishers the right to refuse to publish journalistic pieces without giving an explanation, and that it represents unprecedented state interference in journalistic freedoms and self-regulation.



METHODOLOGY

In 2020, BIRN partnered with SHARE Foundation to expand the usage of SHARE's monitoring **methodology** to other countries besides Serbia. The methodology defines data collection and the categorisation of online incidents that amount to digital rights violations. To effectively capture the diverse landscape of digital rights violations, our monitoring process is based on a structured data collection framework. Our country monitors are tasked with filling out detailed fields, each designed to encapsulate the nuances of each case. These fields encompass various dimensions, including the actors involved, the affected parties, methods used in online attacks, the geographical context, and more. Once violations of digital rights have been identified, they are added to the database.

To better understand how digital rights are being undermined, we have created seven, broad categories of violations:

- **Information Security Breaches**: Encompassing unauthorised access, Distributed Denial-of-Service (DDoS) attacks, data theft and other breaches that jeopardise information security.
- **Information Privacy and Personal Data Breaches**: Covering violations such as data leaks, illegal data processing and interception of communications, threatening information privacy and personal data.
- **Pressures Because of Expression and Activities on the Internet**: This category addresses all violations related to reputation damage, threats

to personal security, discrimination, hate speech, and pressures on individuals due to their online activities and expression.

- **Manipulation and Propaganda in the Digital Environment**: Involves violations such as the spread of fake news, the creation of fraudulent social media accounts, the production of misleading images and videos, and the presentation of commercial content as news.

- **Holding Intermediaries Liable**: Digital rights violations related to pressures on internet service providers, hosting providers and other intermediaries to remove content or block access to websites or services, often enforced through legal measures or threats of punishment.

- **Blocking and Filtering of Content**: Cases of technical content blocking or filtering at the national, organisational or algorithmic level on online platforms.

- **Other Breaches**: A broad category to include digital rights violations that do not explicitly fit into the preceding categories.

Data sources

BIRN's commitment to providing reliable reports on digital rights violations extends to its rigorous monitoring processes, which draw from a variety of sources that include online media, social networks, official documents, academic research, and information shared by local NGOs, activists and experts. Our monitors actively scan these primary sources to identify potential cases of digital rights violations and update our extensive database.

The primary sources for data capture include:

- **Online Media**: Monitors actively engage with online news websites and outlets to stay informed about emerging cases of digital rights violations.

- **Social Networks**: Social media platforms are invaluable for detecting instances of digital rights violations.

- **Official Documents**: Monitors also review official documents, such as government reports, legal filings and official statements that may contain information on digital rights violations.
- **Academic Research**: Academic research papers, studies and publications are another crucial source of information on digital rights issues.

BIRN also maintains a commitment to reliable reporting on digital rights violations by regularly tracking research, publications and monitoring outcomes from respected organisations and institutions. This practice not only bolsters the accuracy of our reports but also assists us in recognising trends and developments in the field, both at the regional and global levels.

Some of our key sources include:

- **Access Now** - Monitors internet shutdowns and digital rights violations globally.
- **Article 19** - Documents threats to freedom of expression worldwide.
- **Ranking Digital Rights** - Assesses internet and telecommunications companies' commitments to human rights.
- **Electronic Frontier Foundation** - Advocates for digital privacy, free expression and innovation.
- **European Digital Rights (EDRi)** - A network defending digital rights in Europe.
- **Freedom House** - Conducts research on democracy, political freedom and human rights.
- **Privacy International** - Investigates and exposes issues of personal data.

BIRN also consults work from partners in the **SEE Digital Rights Network** to ensure a comprehensive understanding of the challenges to digital rights in South-East Europe.

Data capture

BIRN's data on digital rights violations is collected directly by monitors from media reports, social media, official doc-

uments, academic research and information from local NGOs, activists and experts, among other sources.

Monitors search for relevant cases on social media platforms and news websites. They track hashtags, keywords and locations to identify potential violations related to issues like online harassment, censorship and misinformation.

To enhance the information verification process and ensure data integrity, monitors go through a cross-referencing procedure involving multiple sources. Any data that appears questionable or unconfirmed is prominently labelled as such to maintain transparency and accuracy. Monitors use a standardised monitoring form for recording cases. This form includes essential details such as the date, descriptions, the parties involved (perpetrator and subject of the violation), category, and, when applicable, the means of attack.

Monitors also take steps to secure evidence and sources. They add links to the original sources in their records. When there's a risk that the original sources may become unavailable, monitors proactively use online archival services like Archive.li or the Wayback Machine to create snapshots or archives of the sources collected. These time-capsule websites preserve the content as it appeared at a specific point in time, ensuring that critical information remains accessible even if the original sources are at risk of being lost or altered.

Collected cases undergo review by the research team to ensure accuracy. Accepted cases are translated and logged into BIRN's **monitoring database**.

Data Comparison

Over the course of two years, from September 2021 to August 2023, the digital rights landscape in the countries monitored by BIRN has witnessed significant fluctuations. The data in this report reveals a substantial increase in online violations compared to the **previous** reporting period. The total number of documented violations increased from 782 to 1,427, underscoring the intensification of challenges in the digital sphere.

However, it's crucial to note that this apparent increase may not necessari-

ly indicate an overall rise in violations. During this period, BIRN applied a more consistent and rigorous monitoring process to find and document digital rights violations. This heightened vigilance and proactive approach may have contributed to the larger number of reported cases. These statistics reflect the ever-changing digital landscape, with each country's unique challenges and developments contributing to the complex mosaic of digital rights issues in our region.

Hate speech and discriminatory rhetoric have remained a major problem in online discourse. Bosnia reported 63 cases, Albania 30, Serbia 16, Turkey 6 cases and Montenegro 26.

Digital deception is another major issue, encompassing the dissemination of false information, the creation of deceptive social media profiles, the production of misleading images and videos, and the presentation of promotional content as genuine news. A total of 131 such cases were registered in Kosovo, while 55 and 32 cases were registered in North Macedonia and Hungary respectively.

Serious challenges continued to be posed by **computer fraud** and associated cybercrimes. A total of 69 were registered in Hungary, 62 in Croatia, and 32 and 16 cases in Albania and North Macedonia, respectively. Such crimes encompass offences ranging from identity theft to financial scams, underlining the pressing need for robust cybersecurity measures to safeguard personal data and information integrity.

GLOSSARY

This glossary serves as a valuable reference, providing concise explanations of some of the key digital rights terms used throughout the report. In a dynamic digital world, we take our commitment seriously – this glossary isn't set in stone. It's a living, breathing resource we continually refine and expand. As the digital landscape shifts and transforms, BIRN remains dedicated to ensuring that our language remains in tune with the times.

ANONYMITY	The ability to communicate, access, or share information online without revealing one's identity or personal information.
ARTIFICIAL INTELLIGENCE (AI)	The development of computer systems and software that can perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making.
CONTENT MODERATION	The process of reviewing, filtering, and managing user-generated content on digital platforms to ensure compliance with community guidelines, legal requirements, or other standards.
CYBERATTACK	Any intentional effort to steal, expose, alter, disable, or destroy data, applications or other discriminatory language with reference to a Using digital platforms, such as social media, email, or messaging apps, to harass, threaten, or intimidate an individual or group.

CYBERBULLYING	Using digital platforms, such as social media, email, or messaging apps, to harass, threaten, or intimidate an individual or group.
CYBERVIOLENCE	The use of computer systems to cause, facilitate, or threaten violence against individuals, which results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities.
DATA BREACH	An unauthorized access, disclosure, or theft of sensitive or confidential data, often involving personal or financial information.
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS	The targeting of websites and servers by disrupting network services.
DIGITAL RIGHTS	The fundamental human rights applicable in the online realm, including the rights to freedom of expression, privacy, and access to information.
DIGITAL SECURITY	The security of digital systems and the protection of personal and private data.
DISINFORMATION	The deliberate spread of false or misleading information, often with the intent to manipulate public opinion, create confusion, or undermine trust in institutions.
E-GOVERNMENT	Using digital technologies to improve the efficiency, accessibility, and transparency of government services, communication, and decision-making.

ENCRYPTION The process of encoding data or communications so that only authorized parties can access and understand the information.

FAKE NEWS False or misleading information presented as news, often spread through social media and other digital platforms to deceive or manipulate public opinion.

FREEDOM OF EXPRESSION The right to express one's opinions, ideas, and beliefs without interference, censorship, or punishment from governments or other entities.

HACKING The unauthorized user attempts to or gains access to an information system.

HACKTIVISM The use of hacking, digital disruption, or other cyber activities to promote a political or social cause, often targeting governments, corporations, or other organizations.

MISINFORMATION Refers to false or inaccurate information that is unintentionally spread, often due to misunderstandings, mistakes, or errors. It can take many forms, including rumors, hoaxes, conspiracy theories, and propaganda.

ONLINE HARASSMENT Using digital platforms to engage in hostile or offensive behavior, such as stalking, bullying, or threatening an individual or group.

PHISHING A cyberattack in which an attacker attempts to obtain sensitive information, such as login credentials or financial data, by posing as a trustworthy entity in electronic communications, such as email or instant messaging.

PRIVACY

The right to control one's personal information and communications, free from unauthorized surveillance, monitoring, or intrusion.

RANSOMWARE

A type of malicious software that encrypts a user's data and demands a ransom payment for its release, often targeting individuals, businesses, or public institutions.

SOCIAL MEDIA MANIPULATION

The use of social media platforms to spread disinformation, amplify specific narratives, or influence public opinion, often through the use of automated accounts, fake profiles, or coordinated campaigns.

SPYWARE

Malicious software that covertly gathers information about users' activities, habits, or personal data, often without their knowledge or consent.

SURVEILLANCE

The systematic monitoring of individuals or groups, often by governments or organizations, using digital technologies such as internet tracking, social media monitoring, or electronic eavesdropping.

TROLL

An individual who engages in disruptive or provocative behavior on digital platforms, often to provoke a reaction or cause conflict.


COUNTRY REPORTS
ALBANIA
MONTENEGRO
BOSNIA AND HERZEGOVINA
CROATIA
NORTH MACEDONIA
HUNGARY
TURKEY
KOSOVO
SERBIA
ROMANIA

DIGITAL TRANSITION CREATES NEW CHALLENGES IN ALBANIA'S ONLINE ENVIRONMENT

More than a dozen cases of intimidation of journalists were registered during the reporting period, while a wave of cyber-attacks put people's data at risk and dozens of individuals were exposed to online threats and scams. Breaches of the Electoral Code and attempted political manipulation of the public also followed the last local elections.

TOTAL NUMBER OF VIOLATIONS 156

MOST RECURRENT VIOLATIONS

Computer Fraud	32
Destruction and theft of data and programs	32
Hate speech and discrimination	30

VICTIMS

Citizens	87
Public Persons	22
State Institutions	20

PERPETRATORS

Unknown	55
Online Media	43
Citizens	35

During 2022-2023, Albania has grappled with a surge in digital rights infringements in an evolving landscape of online threats with 156 cases intercepted by our monitors. Of these incidents, 17 involved attempted computer fraud and attempted scams by malicious actors, as well as 32 cases of cyberattacks.

However, it's important to note that numerous cases of digital rights violations in Albania go unreported. Often, the gravity of these violations remains unrecognized by the public until they escalate into real-world threats or receive attention from mainstream media. Journalists have faced a troubling wave of attacks in Albania, underscoring

the continuing challenges to press freedom in the digital arena, with 12 cases of attacks against journalists, logged in BIRN's database, including online smear campaigns, hate speech and threats.

In 2022, Albania's ranking in the Reporters Without Borders World Press Freedom Index **fell** by 20 places, from 83 to 103 (out of a total of 180 countries).

Although there was a **slight improvement** in 2023, with the country moving to the 96th position, press freedom remains threatened. Partisan regulation poses a significant challenge to editorial independence, and journalists continue to be vulnerable to organised crime and, at times, police violence, often exacerbated by inadequate government protection. The head of the Albanian Media Council, Koloreto Cukali, told BIRN that "Instead of hiring 'monitors' for online public behaviour at the Media and Information Agency [a governmental body that has **attracted criticism**, Albania would do better to hire multiple officers to deal with the violence that happens in the online sphere".

Journalists also face harassment, threats and censorship due to political influence from politicians and media owners using their platforms for political agendas, Freedom House's Nations in Transit 2023 **report noted**.

A community app called Aktiv1sti, which was used to increase interactions on the Facebook and Instagram pages of ruling Socialist Party officials, **exploited** the public sector for the electoral benefit of the ruling party. This resulted in a breach of the Electoral Code.

Similar activity was registered in April and May 2023, coinciding with Albania's local elections held on May 14, 2023. Candidates used official municipality pages on the internet and social media to advertise their work and run their electoral campaigns in more than 20 instances, violating the Electoral Code. Facebook posts by online media outlets and articles published by websites also contained hate speech and derogatory terms about mayoral candidates.

Massive Data Blights Digitalisation Process

Albania's rapid digitalisation continued as 95 percent of the public sector services that were previously offered by desk staff at centres operated by the Agency for the Delivery of Integrated Services Albania were transferred to the **e-Albania** platform in May 2022, providing the services electronically rather than in person. While this transition promises efficiency, it also presents challenges, particularly for older people and other vulnerable groups who may struggle with using its digital interface. Privately-owned print or Xerox shops have been providing paid assistance with using the e-Albania platform for those who need it. However, these 'service points' operate without regulatory oversight, **raising concerns**, about data handling and accountability such as third-party access to citizens' private data, passwords and accounts, and the need to pay extra costs for the services.

Albania has experienced a surge in cyberattacks, prompting the government to increase its cybersecurity efforts. Collaborating with the Estonian e-Governance Academy and Cyberex Technologies, a '**live fire cyber drill exercise**' was conducted. Albania also expanded its **cybersecurity agreement** with Microsoft Corporation in December 2022. It signed a **new** cybersecurity agreement with the United Arab Emirates in April 2023, reflecting a commitment to strengthening cybersecurity measures.

However, Albanian IT expert Gent Progni questioned the choice of the UAE as a partner. "The United Arab Emirates isn't well-placed in terms of global technology, except the fact that they have an app, Bees, which is like Patronazhisti and Aktiv1sti in Albania, through which they manipulate the algorithms of social networks in their country to boost state propaganda and weaken protests. There are other states which have 'e-governments' and are way more technologically developed," Progni told BIRN.

In 2022 and early 2023, confidential government files were **hacked** and made public on Telegram. In response, Tirana's prosecution issued an **order** on September 19, 2022, prohibiting the media from republishing the hacked data. This sparked debate, with some viewing it as

censorship and others as necessary to protect data confidentiality.

IT expert Progni called the measure "total nonsense" because, as the files are already public, it makes no difference if the media publishes them or not. "This is just an attempt to lower citizens' awareness regarding this scandal and to pressurise media and journalists [by saying] that they can be imprisoned if they publish the data," Progni said.

Albania's digitalisation efforts offer opportunities for efficiency and accessibility but also raise concerns about data security, particularly at unofficial service points. Meanwhile, challenges to press freedom persist, with journalists **facing** online threats from known or unknown individuals as well as politically-motivated censorship. Strengthening cybersecurity measures is crucial, given also the increase in **cyberattacks** from unidentified hackers.

Balancing data security and freedom of information remains a complex issue, as seen in the response to the hacked government files. These developments underscore the need for Albania to address digital rights comprehensively.

Citizens' Data and Government Files Leaked in Cyberattacks

In the series of cyberattacks that started in September 2022, Albanian governmental servers and databases became the target of 32 hacker attacks. The government has **linked** many of them to Iranian cyber actors, although the perpetrators **remain still unknown.**

Dozens of files, including private data from ministries, **police directorates**, **Tirana municipality**, the **TIMS travel system**, the Albanian **parliament**, **the prime minister** and **president's mailboxes**, **citizens' phone numbers**, **Albanian State Intelligence Service employees** and other state officials was published by the Homeland Justice hacker group on Telegram over the course of nine months. Moreover, Albanian citizens' data **were sold** on the 'dark web'. "Nowadays, citizens' data is very precious, you can make a fortune out of them through selling them on the 'dark web'," IT expert Progni told BIRN, adding that "black hackers" target states undergo-

ing technological optimisations, such as Albania.

In the same period, private second-tier banks became targets of **repeated cyberattacks** in which case customers' data and financial details were put at risk. An FBI **report** and a Microsoft Detection and Response Team (DART) **investigation** found that Iran-linked hackers were behind these attacks, but the Albanian prosecution failed to identify them. After these attacks, Albania expelled all the Iranian embassy's staff on national security grounds.

Online Intimidation of Journalists Continues

Over the past year, Albanian journalists were targets of repeated online attacks or smear campaigns. Both journalists and media owners faced restrictions on their work and freedom of expression due to attacks aimed at damaging their reputations.

"In the current circumstances, it is practically impossible to avoid such attacks because most of them are organised by powerful groups from politics, business or even crime, or sometimes all of them at once," Koloreto Cukali, head of the Albanian Media Council, told BIRN.

Online media smeared several journalists through derogatory posts, such as the cases of **Alfred Lela**, founder of news portal Politiko.al, **Sonila Meco**, journalist and TV host at Syri TV, **Anila Basha,** journalist and founder of news portal Newsbomb.al, who were all targets of hate speech and defamation through articles posted about their private life or that of their family members from March-July 2023 by the tabloid online media outlet Prapaskena[dot]com.

In July 2023, the mayor of Tirana, Erion Veliaj **called** investigative journalist Ola Xama a "militant" and a "contract killer" in some WhatsApp messages after she wrote a **BIRN investigation** about disputed waste concession contracts. The European Federation of Journalists and the European Centre for Press and Media Freedom **condemned** the insults and defended Xama and her work.

The targeting of journalists has led them to **practice self-censorship** to avoid online smear campaigns, pressure in the

newsroom and harassment by other actors. Albanian Media Council chairman Cukali told BIRN that "there is no reason to hope the trend of journalists being intimidated by other interest groups will stop". Despite rising concerns and increasing violations in the digital space, Albania still does not have a body dedicated to dealing with this type of attack on media workers or others.

Elections Disrupted by Violation of the Electoral Code

The most recent local elections in Albania held on May 14, 2023, were accompanied by a wave of derogatory articles and comments against candidates for mayoralties throughout Albania. The opposition Democratic Party candidate for the mayor of Tirana municipality was **insulted and targeted** by discriminatory rhetoric several times in online media posts, while some online media outlets, using discriminatory language, claimed he belonged to the Roma community. Breaches in the Electoral Code also accompanied the elections; more than 15 officials used their official channels to run and advertise their electoral campaigns. **Article 91 of the Albanian Electoral Code** prohibits the usage of public resources for electoral campaign purposes. The Albanian Complaints and Sanctions Commission fined **15 mayors from the ruling Socialist Party** and five other **ministry secretaries** for using their official Facebook pages to reach the public for electoral purposes, particularly from April-May 2023.

General Public Targeted by Online Scams

Albania registered a series of online scams and fraud attempts over the past year. The first months of 2023 saw 17 attempts of fraud in which scammers tried to con citizens by presenting fake identities on social networks to steal considerable amounts of money.

One case involved an email sent to several Albanian citizens on June 23, 2023, which at first sight appeared to be sent by the director of the Criminal Police Department. The sender used the Criminal Police Department director's name, but the email address was obviously not related to the police, so it immediately raised concerns.

After members of the public reported the suspicious email to the Albanian Police, it was discovered that it was actually a scam. The email had an attached PDF court order and said that if the recipients failed to answer within a 24-hour timeframe, they would face penalties. Immediately after it was reported to the police, the Directorate for the Investigation of Cybercrimes in the Albanian State Police posted a public announcement, warning the public to watch out for the scam email that was an attempt to steal money and urging them to report it to the cybercrime department.

Social Media Conflicts Escalate into Real-Life Threats

Social networks have become a battlefield for many young people in Albania. In some cases, after young people have sent each other offensive or threatening messages via TikTok, Instagram or other platforms, an online conflict has escalated into a physical fight between different groups and individuals. One of the most **violent cases** was the stabbing to death of a 15-year-old boy from Gramshi after a conflict initiated on TikTok, even though he hadn't been directly involved in it.

Two groups of boys engaged in verbal abuse on TikTok, which later escalated into a physical altercation near Asllan Shahini School in Gramshi. The 15-year-old victim, who died on his way to the hospital, was a relative of one of the boys involved in the fight and had intervened to stop the violence and save his cousin. After the police arrested four perpetrators, it was discovered that before the attack, one of them **had contacted** his friend, via TikTok, sending him a message with a photo of the knives and brass knuckledusters they would use to attack their "enemies." The police seized three knives and two brass knuckledusters during their arrest.

Another horrific incident happened in October 2022. According to media reports, it began with a threat on social media and ended with a double murder and a suicide. Local media further reported that a girl from the town of received online threats from a boy she had been talking to on Instagram, who threatened to publish nude photos of her. Based on the available public infor-

mation, when the girl's father found out, he killed the boy and the boy's father. The girl's father then killed himself as well, local media reported.

LGBT and Rights Groups Increasingly Attacked Online

LGBT activists and civil society organisations have been targets of several online hate speech attacks on Instagram and Facebook. One case in March 2023 concerned **Zhakline Lekatari**, an LGBT activist, journalist and blogger on sexual education and identity, who mentioned in one public appearance that she had to undergo regular psychotherapy sessions due to continuous online attacks that she received on social networks because of her LGBT rights and sexual education activism.

Another concern is the spread of online disinformation about the LGBT community. A trans activist's **account was restricted** on Facebook after an organised campaign was launched to report the account in the wake of a TV interview he gave, talking about the LGBT's community rights.

There was another major incident involving disinformation after a **TV debate** between LGBT activists and Albanian pastor Akil Pano in 2021. The pastor is the founder of a campaign group called "Pro Family and Life", and he and his wife have repeatedly claimed in TV appearances and other public forums that LGBT rights are immoral and anti-family and should be illegal. In November 2022, the pastor's wife, Linda Pano, again publicly spread disinformation by criticising what she called the "gay agenda" on Facebook and a TV programme, **claiming** that a men's gay choir in Los Angeles had been singing "We are coming for your children". However, LGBT activists said this was disinformation, as the song calls for tolerance, respect and understanding for LGBT community members.

Lack of Legal Sanctions Likely to Increase Digital Violations

The digital sphere in Albania is constantly increasing its influence on Albanian society. However, the security of personal information is steadily decreasing, and the Albanian government is failing to protect its citizens' data. IT expert Gent

Progni said Albania could face even larger-scale attacks in the future, particularly in light of the changing geopolitical situation and the technological changes that the country is undergoing.

"The Albanian government's reaction [to the hacker attacks] was zero in terms of technical reaction, meaning that we have not made any change in relation to protecting cyberspace. Nothing has changed," said Progni.

The role of social media in spreading harmful and threatening content online also seems to be on the rise, as there are no measures or regulations to prevent it in Albania. Online platforms have become powerful tools to spread sensationalist videos, which often include **extreme violence against people** and sometimes **animals**.

On the other hand, the online intimidation of journalists is expected to continue next year due to ties between media, politics and other groups of interest as well as control of information by public authorities. Public officials seem eager to continue with their **2022 practice** of avoiding direct engagement with journalists and thus limiting opportunities for in-depth reporting and critical questioning. Journalists report that Prime Minister Edi Rama is further **curbing press freedom** by insisting their questions be confined to government-predetermined themes.

Due to media owners' political and economic interests, journalists often face censorship and self-censorship, leading to less reliable coverage of digital topics and broader social and political issues. Cukali, the head of the Albanian Media Council and founder of the Alliance for Ethical Media in Albania, said that this pressure drives journalists towards self-censorship or even leaving the profession altogether. This poses a serious threat to objective journalism in Albanian society, and therefore to the functioning of the country's democracy.

Recommendations

The proliferation of digital rights violations in Albania underscores the need for comprehensive reforms to protect individuals in the online sphere. While the government has taken some steps, such as cybersecurity agreements with

Microsoft and the UAE, there are systemic problems. To safeguard digital rights and inclusion as technology advances, policymakers, the Albanian government and other relevant authorities should take broader action across three key areas: data protection, press freedom and digital literacy.

- Strengthen data protection laws and cybersecurity measures. Albania's should commit itself to ensuring robust data protection and upholding citizens' data privacy rights, as emphasised in the **2022 Report** on Albania by the European Commission, calls for the prompt enactment of comprehensive data protection legislation that aligns with EU standards, particularly the GDPR. Technical cybersecurity measures, staff training programs, and collaboration with international partners like NATO can help mitigate future cyber threats.

- Increase press freedom protections for journalists. The government should strengthen legal protections for press freedom and freedom of expression, while ensuring an independent media regulatory authority not beholden to partisan interests. Anti-SLAPP laws and better enforcement of laws prohibiting online threats/harassment could help deter attacks on journalists.

- Promote digital literacy and inclusion nationwide. As Albania rapidly digitises services through platforms like e-Albania, the government must ensure that digitally-illiterate and marginalised groups are not left behind. Digital literacy courses, public access programmes in rural areas and user-friendly e-government interfaces can improve equitable digital access. Civil society organisations should monitor inclusion gaps and develop targeted outreach for vulnerable groups.

BOSNIA AND HERZEGOVINA

REAL-LIFE EVENTS KEEP FUELLING DIGITAL RIGHTS VIOLATIONS

People in Bosnia and Herzegovina were shocked by a livestreamed femicide, which raised many questions as the country saw a continuation of digital rights violations fuelled by real-life events such as war crimes anniversaries or the Sarajevo Pride march. The country has also seen a rise in cybersecurity incidents, highlighting the need for strengthening its human and technical capacities to respond, as well as its legal framework.

TOTAL NUMBER OF VIOLATIONS 157

MOST RECURRENT VIOLATIONS

Hate speech and discrimination	63
Threatening content and endangering of security	34
Other manipulations in the digital environment	33

VICTIMS

Citizens	118
Public Persons	26
State Officials / Online Media	8

PERPETRATORS

Citizens	64
Unknown	52
Online Media	24

During this reporting period, Bosnia and Herzegovina witnessed a notable surge in digital rights violations compared to the previous one. The tally reached 157 cases, marking a substantial increase of over 50 percent from the previous reporting period, during which 77 cases were recorded. The most common violations fell under the BIRN reporting categories of "Threatening content and endangering security" and "Hate speech and discrimination".

This reflects a post-conflict society where inter-ethnic tensions are an everyday reality, particularly on the internet. In the examples registered in the BIRN database, the affected parties were mostly

citizens (118 cases). Other significant issues in Bosnia were computer fraud with 17 cases, and the publishing of falsehoods and unverified information with 19 cases.

As in previous years, digital rights violations especially increase in May, June and July. This coincides with the annual Sarajevo Pride event, the latest was organized in May 2023, and on and around July 11, when the annual commemoration for the victims of the Srebrenica Genocide takes place. The violations in these periods range from the propagation of homophobic sentiments, threats targeting the LGBT community and the dissemination of hate speech to calls for harm to both individuals and communities. Denials of the Srebrenica genocide and of war crimes were also an issue again on social media.

Turbulent Political, Ethnic and Social Situation Shapes Digital Space

In general, the number of cases of genocide denial that BIRN recorded in Bosnia decreased compared to 2021-2022. However, BIRN monitoring still registered eight significant cases of denial in the country's media outlets. In the last two years, the numbers have **decreased** after a decision in 2021 by the international overseer of the country's peace agreement, the then High Representative Valentin Inzko, **to impose amendments** to the country's criminal code to ban the denial of genocide and the glorification of war crimes, although prosecutors have yet to bring anyone to court.

In August 2023, the country was shaken by an **unprecedented case** of livestreamed femicide, in addition to various attacks on women both offline and online. The **case** of a teenager from Bijeljina who posted videos on TikTok threatening his Bosniak neighbours also attracted a lot of public attention, as did **the case** of two female students in Sarajevo who glorified convicted war criminal Ratko Mladic. These cases provoked a large amount of hate speech online and resulted in police action in Bijeljina and the expulsion of the two students from the University of Sarajevo.

BIRN registered a noticeable number of online violence cases against the LGBT

community, female journalists and politicians who are often exposed to insults and threats because of their work. The country has experienced a series of serious cybersecurity incidents, such as a hacker attack on the state-level parliament. During the monitoring timeframe, BIRN has identified and documented 15 major incidents, many of which involved Distributed Denial of Service (DDoS) attacks targeting independent media outlets.

In March 2023, a **legislative change** to the Criminal Code of Republika Srpska was **adopted** and there is now a penalty for the **misuse** of photographs and recordings of sexually explicit content. In the Federation of Bosnia and Herzegovina, there is a proposal to amend the law to recognise this kind of behaviour as a criminal offence. The police in Sarajevo Canton, one of ten in Bosnia's entity, proposed **legal solutions** to fight against hate speech and the spread of fake news on the internet. However, **experts** warned that the draft law accepted by the Cantonal government, enables abuse and narrows the freedom of speech. For the first time, the draft law on misdemeanours gives a legal basis for violence on the internet to be punishable by law. However, experts **claimed** the text leaves a lot of space for interpretation, enabling the censoring of the media, and could limit media freedoms, as a result of loose definitions and lack of oversight over the process. The draft law has yet to be adopted.

In October 2022, Bosnia's state-level government endorsed the Ministry of Human Rights and Refugees' **proposal** to map responses to hate speech in Bosnia. According to **a ministry document**, it will monitor the activities of public institutions and will prepare a comprehensive report on freedom of speech, freedom of access to information and the prevention of hate speech by the end of 2024.

Teens' Hate Speech on Tiktok Exposes Media Ethics Gaps

In August 2023, **a teenager from Bijeljina** threatened his Bosniak neighbours on TikTok. He created and shared videos containing insults to Islam and Muslims, including calls for a "reduction" of the Muslim population and their expulsion

from areas inhabited by Serbs. After facing public criticism, he **told BIRN he regretted it** and claimed he wouldn't repeat his actions, yet he continued to publish similar content on TikTok.

In August 2023, the Public Prosecutor's Office in Bijeljina said it was collecting data and information to see if there were elements of a criminal offence in his actions. Replying to BIRN's query, the prosecution said that the Mental Health Centre in Bijeljina "referred the young man for treatment after a suggestion from the prosecutor." However, in September 2023, he **posted more offensive material**. While reporting on this case, most media outlets in Bosnia and Herzegovina disclosed the **minor's identity**, clearly disregarding the media code of ethics. This exposure of a minor's identity during media coverage was not an isolated incident.

During the same month, **an urgent call** for help for a child from the northern Bosnian town of Gradacac began circulating on social media. The child, whose mother Nizama Hecimovic was brutally murdered in a **live-streamed femicide** ten days earlier, was under the care of social services at the time the appeal gained attention on social media. The posts included the girl's full name, a bank account for donations, and an image of the child cradled in the arms of her late mother. However, according to the local Centre for Social Work, the appeal was false and constituted an act of abuse, as the child was already receiving appropriate care. The Centre for Social Work in Gradacac stated that the "announcements about the collection of aid for the daughter of the murdered Nizama Hecimovic are false" and warned that revealing the child's identity "constitutes a criminal offence".

The Bosnian authorities have yet to reveal who was behind the fake appeal, which spread quickly through Bosnian media. Such digital rights violations, as well as being possible criminal offences, also contravene the Code of Media Ethics, which clearly states how media should operate when reporting on incidents involving minors. After a **school shooting** in June 2023, in north-east Bosnia, the pupil's identity was revealed by the media even before the police con-

firmed that the child had opened fire and wounded a teacher.

Russia Finds New Ways to Spread Disinformation

After Russia launched its full-scale invasion of Ukraine in February **2022**, the Russian disinformation campaign in Bosnia intensified when RT (Russia Today), a Kremlin-controlled international news channel, **streamed a documentary** that claimed that there were, and still are, aspirations to establish an Islamic caliphate in Bosnia, since the 1990s war. It also denied facts established by International Criminal Tribunal for the Former Yugoslavia (ICTY) verdicts about massacres during the siege of Sarajevo and the Srebrenica genocide. In the documentary, interviewees drew a parallel between Bosnia and Ukraine.

The Russian embassy in Sarajevo often expresses its views on social networks, spreading disinformation and denying the crimes committed by Russia during the invasion of Ukraine. One of its false **claims** was that the massacre in Bucha was staged. In tandem, the website of Radio-Television Republika Srpska, the Serb-run entity-level public broadcaster, has also promoted **disinformation** about the war against Ukraine. Public gatherings supporting the Russian invasion of Ukraine and comments by Bosnian Serb politicians justifying Moscow's actions were reported by mainstream media in articles that were then circulated and amplified online.

After a year and a half of full-scale war in Ukraine, Russia's methods of spreading disinformation **are changing**, with the use of artificial intelligence techniques to create and share fake content faster.

Bosnia and Herzegovina is still fertile ground for the spread of Russian influence as the Bosnian digital environment reflects the divisions within society. Russian actors frequently use emerging technologies and social networks to promote their **propaganda**. They disseminate misinformation about Russia's invasion of Ukraine through various news sources. They also employ artificial intelligence to generate and circulate fabricated news and disinformation content. These narratives are then widely picked up by media outlets in Bosnia and Herzegovina and Serbia.

Russian state media operating in Serbia further boost the dissemination of these **narratives**.

Meta's Algorithm Failed to Prevent Livestreaming of Femicide

On August 11, 2023, people from Bosnia, as well as outside the country, witnessed a livestreamed murder. Nermin Sulejmanovic, a man from Gradacac, killed three people and wounded another three. He started his killing spree by murdering **his wife**, and **broadcasted it on Instagram**.

It took more than three hours for Instagram to react, leaving the video **available for all users**. By the time it was removed, more than 70,000 people seen it. Meta's delayed response allowed the video to circulate on other social media platforms and be reposted by various users before it was eventually removed.

Bojana Kostic, a human rights and tech researcher and advocate at the Pen to Paper, a media development consulting firm, said the key question is why they did not react even after many people reported the video and sent requests for its removal. "We know that these content removal systems, which rely on both automatic removal and human intervention after reporting violations of the community rules, are ineffective, and certainly even less effective for our language group and region," Kostic told BIRN. "Even more extraordinary is the fact that the content was taken down via the intervention of a person from another continent who had the opportunity to communicate directly with company representatives and escalate the case, despite the fact that there is a trusted flagger organisation in Bosnia and very minimal cooperation with the representative for the Western Balkans at Meta.", Kostic concluded.

In Kostic's opinion, this incident illustrated that only those who have established consistent partnerships with social media companies and hold the status of 'trusted contacts', such as organisations, experts and activists, can react swiftly to deal with such situations. "We all depend on them," she said. Surprisingly, many people 'liked' the video or left comments **in support** of the killer, causing the Bosnian author-

ities to announce an investigation into his online supporters.

High-Profile Women Targeted with Insults and Threats

BIRN recorded 14 cases of online violence against the LGBT population, female journalists and politicians, who are often exposed to insults and threats because of their work. **Dalija Konakovic**, Al Jazeera Balkans journalist and wife of the Bosnian Foreign Minister Elmedin Konakovic, was targeted because of her high public profile and complained several times that she received insulting and threatening messages. In March 2023, she published on X (formerly Twitter) the content of offensive and threatening messages that she received directly and via comments on her posts.

Miomirka Melank, a representative of Nasa Stranka party, **was labelled** an 'Islamophobe' and 'fascist' on X (formerly Twitter), after she shared a tweet from Fadil Novalic, a former prime minister of the Federation of Bosnia and Herzegovina, in which he quoted a verse from the Koran offering forgiveness to believers and "destruction to the infidels".

Various other disturbing messages have been posted by social media users in Bosnia. One written by the ex-husband of a woman who was murdered **said** she may have deserved what happened to her. In another incident, social media subjected a woman to **chauvinistic insults** after she shared a video online documenting a violent altercation with her husband.

At the recent Internet Governance Forum, co-organised by BIRN Bosnia and Herzegovina, **a panel discussed** the absence of adequate legal measures and protective systems, leaving online violence victims feeling betrayed. Panellists stressed the need for law enforcement training and international cooperation due to the international nature of the problem and the jurisdictional limits in Bosnia regarding social networks.

According to Bojana Kostic, the digital arena only reflects what's going on in the physical world in Bosnia and Herzegovina. She said online violence against women is only part of a set of methods to silence, target and belittle people who are "other and different". "What is especially terrible is that the consequences

- physical, mental, emotional, economic, professional and intersectional differences - of violence against women through technology - are ignored, belittled and erased," she said. She argued that more needs to be known about the experiences of female politicians who are targeted by the media and how they perceive their situation.

Genocide Denial Continues Without Repercussions

The denial of genocide has been banned since 2021, but Bosnian state prosecutors office had not filed any indictments by **October 2023**. This left some people feeling encouraged that they could continue denying the genocide and not be afraid of being prosecuted. BIRN **analysed** prosecutors' documents about the suspension of investigations into genocide denial under the Law on Access to Information, and discovered that the explanations given were flawed.

In the reporting period, BIRN recorded eight cases of genocide denials and/or the glorification of people convicted of genocide. However, it should be noted that these were mostly cases that attracted the attention of the public and caused a significant reaction.

One was **the case** of two female students in their early twenties at the University of Sarajevo, who wrote on Instagram that Sarajevo is a city of 157,000 missing Serbs, and after a comment by a Bosniak student, one of them replied: "Good that we killed you." The same day, the other student wrote a comment on Instagram that glorified convicted war criminal Ratko Mladic. In response, some students held a protest, while the Disciplinary Commission of the Faculty of Criminalistics, Criminology and Security Studies investigated and found the incident had damaged the reputation of the University of Sarajevo and the faculty, **imposed the strictest penalty** and expelled the two students, explaining that it wanted to send a message that genocide denial is not acceptable at the faculty.

The president of Republika Srpska, Milorad Dodik, also defied the judiciary and publicly denied the Srebrenica genocide on several occasions. At the beginning of 2023, he told a press conference that **"genocide did not happen"** and that "we

all know that." His comment **sparked** hate speech on social networks, where anonymous users reacted with fury. Some of the comments included: "Dodik is genocidal and dreams of killing women and children", Republika Srpska is "based on genocide", and "Serbs are a genocidal nation".

Apart from public officials, there has also been genocide denial on Radio-Television Republika Srpska. An **article** on the website of the entity-level public broadcaster described the Srebrenica genocide as 'so-called'. Every July, when the anniversary of the genocide is commemorated, the amount of hate speech, denial of genocide and glorification of people convicted of war crimes increases on social networks. However, **such posts** are not removed from social networks, even though they upset the victims who survived and family members of those who were killed. At the same time, professional journalists **have problems with promoting** their fact-checked content on genocide as Facebook's algorithms identify it as negative coverage. Meta has **said** it will impose strict regulation on genocide-related content after it was banned in Bosnia but journalists' current experiences suggest that the regulation is still not being implemented adequately.

Critical Infrastructure at Risk Amid DDos Attacks and Hoax Alerts

The country has seen an increase in cybersecurity incidents; 17 were registered by BIRN in this reporting period. These often-included DDoS attacks on critical media, but also computer fraud. One of the most notable cases **happened** on September 9, 2022, when the website and servers of Bosnia and Herzegovina's parliament were attacked by **CryptoLocker** malware. The attack came a few days after the state Intelligence and Security Agency, OSA, issued **a warning** about the potential for such attacks and called for additional security measures to be implemented.

Sasa Mrdovic, an IT expert teaching computer networks and security at Sarajevo University, told BIRN that the attack was successful for two reasons. "First is a human mistake, where someone had to let that virus in," Mrdovic said.

He continued, "But you can't blame the human if you didn't teach them how to use the network properly. The second thing that helped is that the system was not able to stop the further spread [of the virus] through the network, which means it was poorly constructed."

According to cybersecurity company **Group-IB's** Threat Intelligence report, the attack was carried out by a group called Dark Pink. However, its intentions remain unknown, as no ransom request ever came. Media outlets, mostly in Bosnia's Serb-dominated Republika Srpska entity, which are often critical towards the government, have also seen an increase in DDoS attacks in the monitored period. **Online magazine Buka**, **Nezavisne Novine** and **BN Television** were the target of **simultaneous** attacks in April 2023.

Mrdovic said the motives for such attacks don't have to be just political. "Today you can rent, let's say, 100,000 addresses [to use in an attack] just because you don't like what some media wrote," he said. DDoS attacks flood a web domain with continued attempts to access the homepage, overloading the servers, which eventually can't take any more traffic, effectively taking the site offline. "Hackers don't have to use computers or mobile phones for such attacks anymore, but anything that can be connected to the internet, such as baby monitors, cameras, doorbells," Mrdovic explained. "Then they program those devices to access your website constantly," he added, noting that fighting to stop such attacks is "extremely hard".

Although these attacks do not cause direct infrastructure damage, they lower media ad revenue while reducing the public's access to information. Attacks on critical infrastructure via **hoax bomb alerts** have been common in the Balkans in the reporting period this report covers. In the Bosnian capital, hoax emails were sent, claiming that explosive devices had been planted in various places. The Bosnian branch of Raiffeisen Bank had to evacuate all the employees and customers in all of its banks in Sarajevo due to one **such threat**, which the bank received via email. As the email did not specify which bank exactly had been targeted, the police had to evacuate all of them in the capital. Such

threats, which are easy to send using anonymous emails, cause significant cost to the authorities to determine that they are fake.

Surge in Digital Threats Undermines Hope for Future

Due to the long-running divisions in the country that were cemented by the 1992-95 war and subsequently perpetuated by politicians for electoral gain, the digital space in Bosnia and Herzegovina also remains divided. According to BIRN's monitoring, digital rights violations are often fuelled by real-life events such as war crimes anniversaries, the Srebrenica genocide commemoration or events such as disputed Day of Republika Srpska on January 9, 2023, and the Sarajevo Pride March, usually held in June – a phenomenon that BIRN monitors have noted every year. Among the most common violations are hate speech directed towards other ethnic groups, genocide denial and hate speech based on sexual orientation or gender identity.

Incidents of gender-based violence and femicides have shocked the country, but also encouraged some to glorify the perpetrators, while women are noticeably more subjected to digital rights violations. The consequences of online violence against women are often downplayed, despite their profound physical, mental, emotional, economic and professional impacts. In addition to already existing real-life problems spilling over into the digital space, the use of AI for digital propaganda also affected Bosnia. Adding to this the significant rise in cybersecurity incidents and attacks on critical infrastructure, the situation shows that the country is far from prepared to face these challenges. It is imperative to develop robust legal measures and protective systems to address online violence and digital rights abuses. This necessitates effective law enforcement training and international cooperation, given the cross-border nature of the issues.

Although some levels of the very complicated governance system in the country have recognised the need to regulate the digital space, introducing sanctions for online shaming, spreading fake news, unauthorised recording and privacy protection, many experts think that those

regulations are actually a step back, limiting media freedoms and freedom of speech. Meanwhile the existence of a legal framework does not guarantee that digital rights violations will not happen if the law is not being implemented — as with the Genocide Denial Law, which resulted in a reduced number of cases but no indictments.

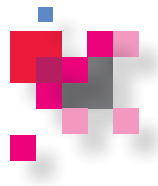
Recommendations

The pressing issue of digital rights violations in Bosnia and Herzegovina, exacerbated by ethnic tensions, underscores the urgent necessity for reforms aimed at promoting online inclusion, safety and accountability. Although the country has prohibited online genocide denial, enduring systemic problems enable the spread of hate speech, gender-based violence, disinformation and cyberattacks. To ensure the protection of digital rights in an era of advancing technology, it is imperative for law enforcement, authorities, and relevant organisations to take comprehensive action in three crucial domains: consistent law enforcement, enhanced user safeguards, and the modernisation of critical infrastructure.

- Rigorously enforce laws banning genocide denial and glorification of war criminals. Despite banning genocide denial in 2021, prosecutors have failed to file any indictments, emboldening many to continue this harmful behaviour without consequences. Prosecutors must uniformly apply the law by filing charges and setting a precedent that hate speech and genocide denial online will not be tolerated.

- Increase protections and support for victims of online gender-based violence. The livestreaming of the murder of a woman exposed shortcomings in protecting at-risk groups from online threats. Bosnia and Herzegovina should pass comprehensive laws criminalising cyber-violence and require social media platforms to promptly remove abusive content upon victim requests. Authorities must provide training to assist victims in documenting threats and pursuing justice.

- Bolster cybersecurity capabilities and cooperation. The surge in cyber-attacks on critical infrastructure like media outlets demonstrates Bosnia and Herzegovina's vulnerability. The government should invest in advanced systems to thwart attacks and closely collaborate with global partners to identify threats early and share best practices. Drills, employee training programmes and new units focused on cybersecurity can help minimise future disruptions.



CROATIA

TOTAL NUMBER OF VIOLATIONS 134

MOST RECURRENT VIOLATIONS

Computer Fraud	62
Illegal personal data processing	46
Citizens' personal data breaches	45

VICTIMS

Citizens	103
Private Company	16
Public Persons	8

PERPETRATORS

Unknown	63
Online Media	13
Citizens	49

TOUGHER LAWS URGED AS CROATIA FACES A RISE IN CYBERCRIME AND DATA BREACHES

Croatia witnessed a series of significant human rights violations in the digital sphere. The government made moves to try to prevent such incidents in the future, but experts believe that this is not enough to prevent similar situations from recurring in the future.

There was an increase in digital rights violations in Croatia in the reporting period compared to the violations recorded in the previous annual report. BIRN recorded 62 computer fraud cases, representing an increase of around 38 percent compared to the previous year when 45 such cases were recorded.

Leaks of private data are of particular concern, and it is necessary to revise the current legislation in order to deter future potential perpetrators. Croatian journalist Goran Latkovic, who covers digital and human rights, told BIRN that the state needs to respond more quickly and adopt adequate regulations to protect people's privacy online. "The state is significantly lagging behind with legal regulations, mostly concerning the Law on Debt Collection Agencies. On October 5, 2023, the Personal Data Protec-

tion Agency fined one agency a record 5.4 million euros for disclosing the personal data of more than 180,000 debtors," Latkovic said.

Latkovic added the data breach, revealed by investigative journalists at the Index website, raised concerns about institutional effectiveness in responding to such problems. He argued that state institutions must act more proactively in order to avoid more serious consequences, as well as deal with other problems in the digital sphere.

"Stronger protection of citizens' personal data under questionable circumstances is necessary. Despite the increase in cases of child pornography, there has still not been a toughening of legal regulations. Croatia plans to introduce a comprehensive legislative framework by the end of 2023. The state's lagging behind in regulating causes significant concern, given the frequent leakage of data," he said.

The Croatian Government's Proposed Media Law Causes Concerns

In May 2023, Croatia **signed** a memorandum of understanding on dealing with transnational cybercrimes with the United States. The memorandum of understanding focuses on enhancing cooperation between law enforcement agencies. Justice Minister Ivan Malenica described this as a step in the right direction and said the authorities intend to adjust the legal framework and strengthen the country's capacities to fight cybercrime.

However, it remains questionable whether this kind of cooperation will yield any results. Rather, to bring about more robust change, Croatia needs to improve legislation and, if necessary, engage in more comprehensive international cooperation to detect and prevent cybercrime.

Croatia's **proposed Media Law**, criticised by the Croatian Journalists' Association, CJA, seems controversial. If the parliament passes the law, freedom of the press could be threatened, the CJA

said. The possibility of censorship, or more specifically, a publisher deciding on their own initiative to refuse to publish a specific article without a justified reason, has been pointed out as particularly problematic.

Members of CJA called the bill an unprecedented encroachment on media freedom in Croatia and expressed deep concern over the **lack of transparency** in drafting the law. CJA members complained about the potential censorship of publishers, requests to reveal journalists' sources, control of funding by the Council of Media Experts, and the creation of a state registry of journalists.

In addition, the register of journalists also represents another opportunity for the authorities to control the media and threaten the freedom of the press. Despite the criticism of the CJA, the government is moving forward with the proposed law.

In the past year, Croatia faced new challenges as well as already familiar issues when it comes to the protection of citizens' personal data. Although there is still much room for improvement, the government claims its 2015 National Cyber Security Strategy is "mostly implemented". However, Croatia, like many other nations, is facing the question of finding a balance between protecting its citizens from digital threats and not encroaching on their rights and freedoms at the same time. This issue has been particularly prominent with the proposed new Cybersecurity Law, which aims to centralise cybersecurity control putting it in the arms of the Security and Intelligence Agency. Journalist Latkovic expressed concern about the proposed legislation, highlighting the lack of transparency inherent in the powers granted to the Security and Intelligence Agency.

Arrests and Charges for Online Child Pornography and Abuse

One particularly serious form of human rights violation is the sexual exploitation of children — BIRN recorded two such cases in Croatia' online environment during 2022-2023. Changes to ensure the safety of the most vulnerable members of society are being discussed. Croatia is **considering** lifting the statute of limitations for pedophilia, which signals a

move in the right direction, but imposing new legislation is still in progress.

In the reporting period, Croatia faced the problem of the **exploitation of children** for online pornography. From September 2022 to the end of August 2023, BIRN recorded BIRN recorded three such cases. **One** case involved a 42-year-old man, identified only as V.S., who was accused of accessing and downloading 16,147 photographs and 270 videos of child pornography between March 2018 and March 2023. Another case was allegedly committed by a suspect identified as E.K., 29, who is accused of sexual abuse of a minor under the age of 15, exposing a child to harmful materials, and luring children to satisfy sexual needs. The government is considering abolishing the statute of limitations for pedophilia with the aim of deterring new violations of the most vulnerable members of society.

Pressure on Journalists and False Accusations

During 2022-2023, BIRN registered 16 cases of insults and unsubstantiated accusations in the digital space in Croatia. In one recorded **case**, online media outlet Narod accused the Croatian fact-checking site Faktograf of information censorship. Accusations of this type usually occur because of the widespread misconception that fact-checkers limit access to certain data they deem unreliable to prevent the spread of fake news.

In three instances, the situation escalated to the point where individuals received online death threats. Member of Parliament Sandra Bencic told media in February 2023 how she had **faced death and rape threats** during her mandate, while the mayor of Samobor, Petra Skrobot, was exposed to **sexist attacks** during her duties. The spread of **disinformation** was also registered in the case of Deputy Prime Minister Tomo Medved.

TV presenter Iva Sulentic **faced insults** on Instagram after hosting a celebration

for the Croatian national football team in Zagreb after the players returned from the World Cup in Qatar. YouTuber Ivan Rado **faced death threats** and accusations of religious bias after his video was manipulated and misrepresented on social media, sparking a wave of misinformation.

Phishing Fraudsters Impersonate Police Officers

BIRN also noted 62 online fraud cases in Croatia. BIRN identified at least three cases in which the perpetrators **falsely** presented themselves as bank employees via email, along with a **case** in which the scammers impersonated police officers. In **one** of the cases, the perpetrator sent an email asking the recipient to click on a link to a fake bank website in order to update their information, saying it was necessary for risk management and to prevent money laundering. In May 2023, police warned citizens to be careful with such emails, saying they received multiple criminal complaints about them. Although Croatia signed a Memorandum of Understanding with the United States in May 2023 in order to combat cybercrime more effectively, Latkovic questioned whether this was an adequate substitute for stricter legislation or "just good PR."

Citizens' Data Leaks from Debt Collection Agencies

One of the **most serious breach** cases of privacy involved EOS Matrix, a debt collection agency, when the private data of 181,000 users in their possession, including those of minors, leaked. The case of EOS Matrix is reported as the second in a row in the reporting period; in December 2022, a **similar incident** was reported about the company B2 Kapital

The Personal Data Protection Agency **imposed a fine** of 2.26 million euros on the B2 Kapital for violating the General Data Protection Regulation.

The EOS Matrix data leak became public after an investigative article by a journalist from the **Index** website in March 2023. It was reported that EOS Matrix was collecting or gathering data about minors, which they admitted, claiming that they were doing so based on valid

court rulings on inheritance, that is, for persons who have been determined to be the heirs of debtors. In October 2023, the Personal Data Protection Agency **fined** EOS Matrix 5.47 million euros due to violations of the General Data Protection Regulation. The agency concluded, among other things, that the company "did not take appropriate technical measures to protect personal data of the data subjects" and that they processed the personal data of data subjects who are not in a debtor-creditor relationship as well as health data without determining a legal basis from GDPR.

Online Fraud Still On the Rise

BIRN's monitoring recorded an increase in the number of computer frauds, signaling the need for more effective cybersecurity measures. Besides introducing new, more effective, and strengthening the existing legislative measures and their enforcement to tackle cybersecurity threats, key steps to reduce their prevalence and consequences would include better efforts by the authorities to educate the public about cybersecurity threats.

A case of a company in Rijeka that was defrauded of 183,200 euros, when an employee fell victim to fraudsters pretending to be the bank employees, underlines the need for more robust cybersecurity training for private and public entities. Current government measures that amount only to public warnings about cybersecurity threats are not proving to be sufficient.

Recommendations

Due to the growing number of cybercrime cases, leakage of citizens' personal data and threats to journalistic freedoms, it is evident that Croatia must address several key issues if it wants to reverse the negative trend of human rights violations in the digital world.

- Strengthen cyber security and train personnel. The government needs to invest more resources in developing the cybersecurity infrastructure and educating staff who will manage it so protecting citizens' private data is more effective. Cooperation between the government and private entities,

which are also often victims of cyber fraud, should also be a part of a wider strategy. In addition, the government should employ the knowledge of private companies with expertise in fighting cybercrime.

- Protect privacy and enforce strict measures from existing data protection laws and new regulations. Besides public institutions and bodies that proved fragile to the cyberattacks, the cases of leakage of citizens' personal data under private entities' care have highlighted shortcomings in the privacy protection system. Private and public entities should benefit from potential mutual cooperation in order to better safeguard the data under their protection.

- Preserve the independence of the media. By all accounts, the new draft law on media will not improve the freedom of the press; on the contrary, it could further restrict it. Members of the parliament and members of the working group that is developing the law must ensure that the drafting and implementation of the legislation are carried out transparently and with respect to professional bodies' recommendations. There should not be any abuse of authority resulting in media censorship, which could have long-term consequences for the public interest.

DIGITAL RIGHTS VIOLATIONS, DISINFORMATION AND REAL-WORLD CONSEQUENCES

Hungary has been witnessing a surge in digital violations, disinformation campaigns and real-world repercussions from these issues, amid ongoing concerns about media freedom and online security. The government of Viktor Orban is likely to continue to have a negative impact on internet and media freedoms as the 2024 European Parliamentary elections and local polls approach.

TOTAL NUMBER OF VIOLATIONS 154

MOST RECURRENT VIOLATIONS

Computer Fraud	69
Other Manipulation in the DR environment	32
Publishing falsehoods and unverified information with the intention to damage reputation	23

VICTIMS

Citizens	105
State Officials	26
State Institutions	24

PERPETRATORS

Unknown	92
Online Media	26
Political Party	13

BIRN detected 105 digital rights violations in Hungary during the reporting period. As 2023 unfolded, the country saw persistent threats to digital freedoms and the continuing presence of online disinformation. Although the number of disinformation cases that BIRN recorded saw a decrease from 47 in 2022 to 31 in 2023, the propagation of false or misleading claims by pro-government media outlets and influencers remained a pressing concern. Notably, these included instances of pro-Kremlin disinformation concerning the Russia's aggression in Ukraine, marking a continuation of patterns observed in 2022.

The digital realm also saw over a dozen instances in which government-affiliated figures and media entities resorted to insulting or verbally attacking opposition politicians, independent journalists and other public figures. Left-wing Szikra movement and its MP Andras Jambor **were falsely accused** of organising the beating of far-right demonstrators by pro-government media, **Fidesz politicians** and **the police**. The personal data of several left-wing activists has been published on Facebook and Telegram, and they have been threatened with physical violence.

The use of Distributed Denial of Service (DDoS) attacks to stifle digital freedoms was a continuation of trends from the previous year. DDoS attacks disrupted the websites of independent news sources, including **HVG**, **Atlatszo**, **Telex** and **Klubradio** among others. The digital sphere was also tainted by the persistence of hate speech and discrimination, with 15 incidents BIRN documented in 2022-2023 compared to 13 in 2021-2022. Among these were instances of homophobic rhetoric **disseminated by officials** and **media outlets**. Taken as a whole, the data gathered by BIRN illustrates that Hungary's digital arena and **civic space** continue to grapple with **increased pressures**, mirroring the landscape observed in 2021-2022. Technological attacks on media websites, the use of propaganda and the curtailing of freedom of speech have collectively impeded independent reporting and stifled opposition voices in the virtual realm.

Orban Government and Its Allies Dominate Media and Internet

According to Reporters Without Borders' World Press Freedom Index, Hungary currently **ranks 72nd** out of 180 countries worldwide in terms of media freedom, while in 2010, it was in 23rd place. In terms of internet freedoms, Freedom House has labelled Hungary **partly free**. The reason for this decline is that under Prime Minister Viktor Orban's government (in power since 2010), several independent media outlets, like Nepszabadsag, were forced to close down, or were taken over, like Index or Origo, by allies of the ruling Fidesz party. In 2021, Reporters Without Borders described Orban as a "**press freedom**

predator" for having "steadily and effectively undermined media pluralism and independence since being returned to power in 2010".

The Central European Press and Media Foundation, KESMA, owns the majority of about 500 media outlets, including all the local daily newspapers, important online news outlets, tabloids and weekly magazines. Public broadcasting service (including the only newswire in the country) is also under the government's strict control. The Megafon Centre, a government-controlled online influencer organisation, **spends hundreds of millions on** social media such as Facebook, Instagram, YouTube and TikTok to echo the government's messages. Megafon says that donations are its source of income. But independent media outlet Telex reported that Megafon could have received public money. Megafon sued Telex, claiming it hadn't received any public funds and that Telex lied. But Megafon lost the case in court.

Violations committed by online media turned out to be the pro-government media in most of the cases documented by BIRN. Getting access to information is getting more and more difficult for independent journalists. State institutions are reluctant to answer queries, and independent experts are afraid to be critical for fear of losing their jobs, becoming a **target of smear campaigns** or **suffering other disadvantages**. Independent media are also targets of **defamation campaigns**. "Fidesz has dominated public speech since 2006, because then, as an opposition party in that old media system, they had the opportunity to deliver their messages," said Gabor Polyak, a media expert and the leader of Mertek Media Monitor, a Hungarian NGO.

"After 2010 [when Fidesz came to power], they had all the tools to take over the media: foreign publishing houses were ready to leave, the government started to run expensive campaigns in the pro-government outlets, they bought up not only media outlets but printing and distribution companies as well. In addition, the independent media is also critical to the opposition parties, and that makes the opposition's situation even harder when they try to deliver their messages," Polyak added.

As a result, the government's agenda strongly dominates the Hungarian media landscape and public speech. Beyond these challenges, Hungary has had to contend with various other digital threats, including an increase in phishing scams employing the names of official bodies and companies to deceive and exploit individuals. The scale of computer fraud cases increased to 69 instances documented by BIRN in 2022-2023, over twice as many as the 28 reported in 2021-2022. Fraudsters orchestrated sham online **sweepstakes**, fabricated **dating profiles** and created deceptive **e-commerce listings** to ensnare unsuspecting victims — a continuation of the online scam trends witnessed in 2021-2022.

DDoS Attacks Hit Independent Media Outlets

Independent media outlets have been increasingly targeted by DDoS attacks. In 2021-2022, BIRN documented only two major cases,, whereas in 2022-2023, 20 were recorded. During the attacks, the websites were rendered inaccessible to readers for hours or **even days**, causing the media outlets financial losses.

In a **recent report**, the International Press Institute, IPI called these DDoS attacks "one of the broadest cyber-attacks against an independent media community within a European Union member state to date". IPI said that since April 2023, at least 40 different media websites have been attacked. (BIRN has recorded 20 cases in **Hungary's database**.) The victims of the attacks were independent outlets, including the most important news sites Telex, HVG, Atlatszo, 444, Magyar Narancs and Merce, and an online radio station, Klub Radio. Attackers also hit the website of **Budapest Pride**, making it inaccessible on the day of the Pride parade. Based on the targets and the methods, these attacks appear to be connected. In some cases, the attackers left messages in the code that they were being coordinated domestically, IPI said. After publishing its report, IPI itself **became a target** for attacks. Polyak told BIRN that "It is very difficult to investigate such cases, and it seems the Hungarian police don't see them as a high priority". However, he

added: “We cannot link these attacks to any political party. And these attacks were not so serious, it would have been serious if more major websites had been inaccessible at the same time for at least half a day.”

Rising Tide of Online Scams and Phishing in Hungary

According to BIRN’s findings, online scams and phishing attempts in Hungary became more frequent in 2022-2023 compared to 2021-2022. BIRN recorded 17 in 2021-2022, while the number of these violations jumped to 30 in 2022-2023.

Statistics from the Hungarian National Bank confirm this trend. BIRN observed various different types of phishing attempts in which fraudsters tried to get access to users’ bank card numbers and other personal details. There were **fake advertisements**, prize draws announced in the name of well-known **supermarket chains** and email campaigns started in the name of **service providers** or even of **the police**. Fraudsters made **copies of banks’ websites** almost identical to the original ones. In a new development, fraudsters sent text messages to their victims’ phones, seemingly from a delivery service. But the link in the message directed the victim to a phishing site or downloaded malware to the user’s smartphone. **According to experts**, these kinds of scams became more prevalent in Hungary because automatic online translators improved their translations in Hungarian, so foreign fraudsters can now deceive Hungarian users more effectively.

Experts think that the Hungarian Media Authority, NMHH should organise an awareness campaign. “These scams are more and more sophisticated. Teaching media and financial literacy should be part of general education, but the Hungarian system is very far from that,” Polyak said.

LGBT Community Faces Continuing Online Attacks

Online attacks against LGBT people represent a major concern in Hungary. The government is believed to fuel this campaign, alleging that LGBT people **target children with their propaganda**. “We will protect Hungarian children

from LGBT propaganda, even if we are pressured and attacked," said state secretary Tamas Menczer. Pro-government media outlets **denigrate transgender people** and **intentionally link** LGBT people with paedophiles.

In April 2023, the European Commission and 15 EU member states **backed legal action** against the Hungarian government over a 2021 law that discriminates against LBGT people. The law bans all content that "promotes or portrays'' what it refers to as "divergence from self-identity corresponding to sex at birth, sex change or homosexuality" to minors. Ahead of the 2023 Pride march in Budapest, the **embassies of 38 countries** released a statement urging the Hungarian government to protect the rights of LGBT people and scrap laws that discriminate against them.

Prominent pro-government pundits have described homosexuals as paedophiles. One pundit, Zsolt Bayer, even **labelled LGBT people** "ugly, disgusting, worms to be cleaned up". More alarming is that politicians participate in denigrating the LGBT community during election campaigns.

Bence Retvari, the state secretary at the Interior Ministry, **published an anti-LGBT post** on Facebook, claiming that the Labrisz Lesbian Association wants to "impose LGBT ideology on young children without the knowledge of parents, even against their will". In reality, the association and Amnesty International Hungary offer an out-of-school training programme for teachers on how to deal with children of LGBT parents. None of these anti-LGBT statements have had any legal consequences.

However, some media coverage has had a chilling effect. After a local pro-government outlet published **a homophobic article** saying that people planned to organise an LGBT party in Hodmezovasarhely, a city in south-east Hungary, the organisers had to cancel the event. "We do not want to be involved in political games," **said the organiser**, adding that people in Hadmezovasarhely are not very tolerant.

Media expert Polyak said that current media law and press regulation is outdated. "It was relevant when there were 15 to 20 major outlets and much less news so the corrections ordered by the

court could reach the readers. Now a smear campaign is quoted by all the pro-government outlets, reaching a lot of readers and viewers. In the meantime, an order to correct it affects one or two outlets, and you have to wait years for such a ruling. So, the current regulation is not effective in today's media system," Polyak said.

Online Attacks on the Judiciary: Disrupting the Rule of Law

The Hungarian government has been continuing its attempts to extend its power over the judiciary, which is the last remaining primarily independent branch of power in the country. The judiciary has been under constant attack in the online sphere, with the government trying to prove how politically biased some judges are. Government officials make statements criticising certain judges, as do pro-government online media and government-linked NGOs. Sometimes these attacks are **combined with anti-LGBT campaigns**. BIRN recorded a case in which a court ruled that a trans woman is entitled to a woman's early retirement pension. Gabriella Selmeczi, deputy leader of the ruling Fidesz's parliamentary group, **attacked the ruling in an interview** with pro-government daily newspaper Magyar Nemzet, which was also published online. "The case is a blatant provocation and a slap in the face of the legal system," Selmeczi said. She added that "the case also shows that LGBT propaganda exists" and that it is "outrageous that there is a judge in Hungary who can make such a ruling". The Centre for Fundamental Rights, a government-sponsored NGO (GONGO) supported Selmeczi **with a statement** saying that the ruling was "a dangerous, incomprehensible decision that runs counter to written law and common sense." Pro-government outlets also **attack certain judges by name**.

Inflammatory Online Activity Makes a Tangible Impact

BIRN documented two cases in 2022-2023 in which online activities resulted in significant real-life consequences. On May 19, 2023, a secondary school student **created and posted online** two memes of Robert Bibok, the principal of Tancsics Mihaly College, holding a ribbon with the colours of the Hungarian flag upside down. The student was expelled, even after deleting the memes at the request of a teacher.

In a second incident recorded on May 2, 2023, a participant in the Nyirmartonfalva public employment programme **was threatened with the sack** by Fidesz mayor Mihaly Filemon after she reacted to a friend's Facebook post about a controversial wooden canopy walkway without trees around it with an emoji of a laughing face. Filemon, who built the walkway with EU funding, threatened to fire the worker and changed her work schedule so that she could not take her child to school.

As Elections Loom, Orban's Assault on Internet Freedoms Continues

In the Hungarian media landscape, the online sector seems to have had the greatest degree of freedom. Local newspapers and radio stations are generally viewed as pro-government, although there is one daily and one major broadcaster that are not aligned with the government. There are also a few weeklies, but their influence is limited. In recent years meanwhile, the government and affiliated organisations have invested **tens of millions of euros** to establish dominance over social media and the digital sphere.

The government's campaigns have often targeted LGBT people and **migrants**. The government and its allies have also engaged in spreading **anti-Ukrainian, pro-Russian propaganda**. Sometimes, they spread false statements **about Ukraine**, but mostly just present events according to the Russian narrative, or publishing articles with **fear-mongering, clickbait titles** such as **'Announcement: WWIII has**

started' or **"Dramatic turn of events: Russia threatens nuclear strike"**.

A continuation of 2022-2023's trends into 2024 is expected, as Hungary will hold both local elections and European Parliamentary elections on June 9, 2024. If the government employs the same tactics as it did in the previous election cycle, a prolonged and intense campaign period that will have a significant impact on Hungary's digital sphere can be expected.

2024 will not be any different when it comes to digital rights, experts warn. "There will be very tough smear campaigns at the local level, and it doesn't necessarily have to be done in an organised way. Put simply, it has just become part of the Hungarian political culture that there are no boundaries, there's no respect and this is true for all political sides. But Fidesz has more tools and they will not risk losing," Polyak said. There has been a rise in cyberattacks against independent media outlets and in the number of online scams. But the Hungarian law enforcement authorities have not been effectively investigating these cases, experts say. "While some affected media have filed police reports, investigations have shown little progress," the IPI noted. "Police appear to be handling cases individually rather than as part of a coordinated national effort. There is also a lack of awareness campaigns regarding fraud prevention. While commercial banks occasionally send warning emails, there is no organised effort to educate a broad, general audience on how to avoid scams."

Recommendations

There are continuing concerns about media freedom and online security in Hungary, with the government of Viktor Orban at the centre of these issues. As the 2024 elections approach, it is imperative to address the digital violations, disinformation campaigns and real-world consequences faced by the country. To secure digital rights as technology advances, the authorities must take broader action across three key areas: strengthening media independence, enhancing online protections and combating disinformation.

- Ensure the independence and plurality of media. The media landscape in Hungary is currently characterised by a significant imbalance, with pro-government outlets dominating the scene. This situation has raised serious concerns about the impartiality of reporting and the health of media pluralism. Policymakers should implement reforms to diversify media ownership, increase funding for independent outlets and prevent political interference in state media. This involves setting limits on the percentage of media outlets that any single owner or entity can control, and applying these regulations consistently to print, broadcast and digital media. By diversifying media ownership, a more varied and balanced range of voices can be introduced into the media landscape, reducing the risk of undue political influence and promoting a wider array of perspectives and opinions.

- Enhance Cybersecurity Measures and Investigate DDoS Attacks. In light of the rising frequency of Distributed Denial of Service (DDoS) attacks against independent media outlets in Hungary, law enforcement bodies and the relevant authorities must prioritise cybersecurity measures and investigate these attacks rigorously. A coordinated national effort should be established to address these attacks, targeting not only the perpetrators but also the potential domestic coordination behind them. Collaboration with international organisations experienced in cybercrime investigations can aid in identifying and prosecuting those responsible. This effort should also include preventive measures to bolster the resilience of media outlets against future DDoS attacks.

- Safeguard LGBT rights and combat hate speech. The government of Hungary must take active steps to safeguard the rights of the LGBT community and combat hate speech, particularly online. The existing media law and press regulations should be updated to address the challenges posed by the

rapid dissemination of hate speech through various pro-government outlets. Legal sanctions for individuals and entities engaging in hate speech should be strengthened to ensure that such actions do not go unpunished. Prominent figures and politicians involved in such campaigns should be held accountable for their inflammatory rhetoric. To foster a more inclusive and tolerant society, government-backed campaigns against the LGBT community must be stopped, and legislation discriminating against this community should be repealed or revised.

KOSOVO

TOTAL NUMBER OF VIOLATIONS **191**

MOST RECURRENT VIOLATIONS

Other Manipulation in the DR environment **131**

Content manipulation and organized reporting on social media **115**

Publishing falsehood and unverified information with the intention to damage reputation **81**

VICTIMS

Citizens **162**

Public Persons **69**

State Official **52**

PERPETRATORS

Online Media **158**

Citizens **40**

State Official **1**

MISINFORMATION, PRIVACY BREACHES AND SCAMS TAKE CENTRE STAGE

There has been an increase in misinformation, privacy breaches and scams, deepening discord and mistrust in Kosovo. These issues are exacerbated by narratives driven by political events, leading to digital rights violations on various platforms. This situation reflects the country's complex social and political dynamics, impacting its digital landscape.

Manipulative misinformation campaigns, unauthorised sharing of personal data and a surge in marketing scams have dominated the scene in the reporting period. This marks a stark departure from **2022**, when the focus was primarily on fake news surrounding Russia's full-scale invasion of Ukraine, heightened digital tensions with Serbia, and scams targeting women.

As 2023 unfolded, the new trends signified that there has been a deliberate attempt to undermine trust and foster division among the Kosovo public. A

closer look reveals that many of these digital rights violations relate to content steeped in an 'us versus them' narrative — a narrative that is particularly evident in discussions involving political figures, journalists and significant events.

Digital rights violations have also revolved around narratives exploiting the troubled relationship between Kosovo and Serbia. This dynamic is evident on both Albanian- and Serbian-language social media channels. There's been a growing trend of targeting Kosovo's public figures by falsely associating them with Serbia, questioning their loyalties or intentions. The prevailing political tensions between the two countries have also led to malicious releases of personal data, particularly targeting individuals perceived to be aiding the 'adversary', such as Serb recruits to the Kosovo police force. The digital realm has now become a focal point where these tensions and discussions are amplified, capitalising on historical and ongoing disputes, fostering a climate of scepticism and mistrust among the population, as public figures and ordinary citizens alike have become the subjects of targeted violations.

Startling findings from BIRN's latest monitoring report show a significant spike in reported digital rights violations. During 2022-2023 BIRN documented 191 cases, a stark contrast to the 89 recorded in last monitoring period. State officials were targeted in 52 cases, and public persons in 69. The rest of the violations primarily affected the general public, primarily via distorted and misleading news. These manipulated narratives **intentionally twist information**, take it out of context or present it in a misleading manner, spreading confusion and misinformation.

Even more concerning is the fact that 158 incidents originate from articles published by online media (the other great majority were generated by members of the public and officials). Such narratives are then disseminated via social media platforms like Facebook and TikTok. Over half of the cases involve the dissemination of unverified, damaging information, particularly targeting state officials, journalists and public figures. Such incidents, whether involving doctored images or false statements, erode trust in institutions and public figures,

which is evident by the heated social media responses they ignite.

Another alarming trend revolves around the unauthorised disclosure of personal information. Of particular concern are attempts to expose the identities of protected witnesses in trials, potentially jeopardising their safety. Platforms such as Facebook and, notably, Telegram have been central to these breaches. Specifically, Serbian-language Telegram channels operating in Kosovo frequently post unauthorised names and images, including those of **Kosovo police recruits** of Serb ethnicity. Tanzer Abazi, the chairman of the Albanian Cyber Association in Pristina outlined aspects of Telegram's appeal to BIRN: "Its early promotion of anonymity and end-to-end encryption — a feature only its secret chats fully utilise. Coupled with easily obtainable international phone numbers via cryptocurrency, users maintain a level of anonymity, making tracing them challenging. Furthermore, Telegram's reputation for limited support in cases of breaches exacerbates the issue. The lack of entities monitoring personal data on the platform allows for the free exchange of such data, either between individuals or within groups."

Although both Albanian and Serbian users are present on Telegram, Abazi noted the prevalence of groups and channels, primarily in the Serbian language, that "are utilising this platform to incite hatred and potentially engage in unlawful activities in Kosovo". These actions not only compromise personal security but also exacerbate divisions in an environment already strained by political differences within Kosovo and its relations with Serbia.

Kosovo's digital sphere has also witnessed an increase in marketing scams, targeting unsuspecting members of the public. The operators of these scams, ranging from false financial offers to deceptive health products, often masquerade as legitimate entities in order to collect personal data from their unsuspecting targets.

Kosovo Faces Increased Digital Rights and Information Integrity Challenges

Kosovo's media landscape has undergone significant change in recent years and the country has seen a rise from 78th in 2018 to 56th in 2023 in the **global press freedom index** published by Reporters Without Borders, which surveys 180 countries worldwide.

According to the **World Bank** and the **Kosovo Economy Ministry**, Kosovo achieved 100 percent internet penetration in 2023, and the digital realm has expanded as a medium for expression. However, after further verification via the Kosovo Statistical Agency, data pertaining to internet penetration in the north of Kosovo is absent, as it does not cover this area. Consequently, the assertion of a 100 percent penetration rate may not provide a comprehensive representation of the entire country.

This widespread accessibility has amplified the internet's role in shaping public discourse and enabling communication. However, it is also a medium where digital rights violations have increased. Partisan content and biased campaigns fill the digital realm, aiming to sway public sentiment using inherent biases. These range from instances like a manipulated photo of the Minister of Industry, Entrepreneurship and Trade disseminated on a popular Facebook page, **insinuating** that she admitted to misappropriating state reserves, to misleading attributions on another Facebook page that falsely claimed the president of Croatia accused opponents of Kosovo's government of being funded by the Serbian president.

Young people in Kosovo are mainly active on platforms like TikTok, Snapchat and Instagram, and digital rights violations and misinformation go largely unchecked on these platforms. In contrast, Telegram was more popular in the Serb-majority regions of Kosovo. Given the increase in digital engagement and the potential pitfalls, the significance of reliable fact-checking entities has grown immensely. BIRN's Krypometer platform and Hibrid.info are some of the International Fact-Checking Network (**IFCN**), actively fact-checking disinformation and digital rights violations affecting

Kosovo citizens. Other platforms like Sbunker and Kosovo 2.0 also address digital rights violations and disinformation. Their monitoring, reporting and research has indicated similar trends in terms of violations.

The proposed Association of Serb-Majority Municipalities in Kosovo relations has added complexity to the Pristina-Belgrade dialogue, straining ties further, especially in northern Kosovo. Contested elections in the north, recognised by the Kosovo government and those of the United States, France, Germany, Italy and the United Kingdom, also known as the **QUINT countries**, but boycotted by Kosovo Serbs, led to Kosovo Albanian officials taking key positions. This **sparked clashes**, such as the incident in Zvecan municipality where violent confrontations occurred between local Serbs and peacekeepers from NATO's Kosovo force KFOR. Such incidents not only heightened tensions but also fuelled the spread of misinformation, **hate speech** and **fake news** on digital platforms, as evidenced by our monitoring. Tensions persisted throughout the summer, **culminating in EU-mediated talks** between Serbia and Kosovo's leaders in September 2023.

Journalists, Politicians and Diplomats Hit by Barrage of Online Attacks

The digital landscape in Kosovo in 2023 saw a rise in rights violations, mainly driven by fake images, **altered photos** and **deep fakes**. These campaigns frequently aim to inaccurately associate individuals with controversial people, policies or political views, thereby harming their reputation, in order to create divisions.

Notably, political figures and prominent journalists have been the primary targets of these misinformation campaigns. Over 30 instances have been registered in which manipulated content has supported false narratives and has spread across online platforms. A significant **example** of this is the multiple Facebook accounts circulating unfounded claims associating Kosovo Prime Minister Albin Kurti with the Serbian state. The tactics also include **videos** suggesting Kurti's ties with Serbian intelligence agencies.

Journalists in Kosovo are increasingly facing misinformation campaigns, with some encountering false associations with opposing political entities or foreign governments. These instances often utilise manipulated images and false claims to misrepresent their affiliation and viewpoints. Such efforts are part of a larger trend where deep-rooted cultural stigmas are exploited to label public figures, echoing the evolution of political discourse over the years.

This phenomenon is particularly pronounced in today's environment of open dialogue, where unchecked and provocative language is rampant in public discussions. These tactics, employed across the political spectrum, target journalists and opinion leaders who may express views contrary to certain policies or politicians. The culture of creating, emphasising, and amplifying cultural stigmas can be traced back to the language used in politics and among political establishments. Social media platforms are the main grounds where individuals often pin events or trends on specific individuals, by presenting baseless accusations and without facing repercussions. There is a growing concern over the tangible threats posed by the online campaigns, especially given the significant portion of the public that readily accepts and acts upon these narratives. The danger lies in the potential for misguided individuals to act on such beliefs, potentially causing harm to those targeted. Alarmingly, these campaigns, rooted in perceptions of betrayal, have become increasingly common, amplifying their impact within the realm of social media and contributing to a charged and adversarial online discourse. For many victims, these attacks are perceived as an inevitable aspect of modern digital conversation, highlighting the need for greater awareness and stronger measures to combat misinformation and protect the integrity of public discourse in Kosovo's digital landscape.

Privacy violations: A Growing Threat in Kosovo's Digital Sphere

After **the arrest of a Kosovo Serb**, Milun Milenkovic, a leader of the Civil Protection organisation, tensions heightened in the north of Kosovo. Arrested

for allegedly initiating attacks on NATO peacekeepers in May 2023, his capture sparked local disturbances. Additionally, another individual, identified only as N.O., faced detention on accusations of violence against KFOR soldiers in Zvecan.

Throughout these developments, digital platforms became tools for provocation. Serbian Telegram channels active in Kosovo distributed controversial images and assertions. Specifically, a channel named "БУНТ је стање духа" ("Rebellion is a State of Mind") **posted photos** suggesting two 'unknown' individuals had been seen in North Mitrovica right after Milenkovic's arrest, without evidence that they were connected to the case in any way. Considering the tense atmosphere during those days, such exposure could have **endangered** the safety of the individuals pictured. Another channel, BUNKER, **revealed** the names and pictures of Kosovo Serb recruits to the Kosovo Police who live in Serb-majority areas while hinting that they 'betrayed' the Serb community. In 2018, **similar** intimidation tactics caused many Serb members of the Kosovo Security Force to resign.

In March 2023, a video re-emerged in which a publicly known individual **offered** a financial reward for identifying protected witnesses testifying against former Kosovo Liberation Army leaders in court in The Hague. This endangered witness safety and constituted a severe violation of digital rights as well as being a criminal offence. The Specialist Prosecutor's Office in The Hague **cited** this case when denying early release to two defendants. However, the Prosecutor's Office took no legal action against the perpetrator.

Scams and Phishing Continue to Plague Kosovo's Online Ecosystem

During 2022-2023, online scams emerged as a significant issue in Kosovo according to BIRN's monitoring. Such scams were particularly evident in social media posts directing users to unsecure websites. A multitude of misleading Facebook pages appeared, **imitating** advertisements from legitimate financial institutions, potentially

convincing users of their authenticity through offers of swift loan approvals. Alarmingly, many lack contact information and redirect users to insecure websites that prompt the input of personal data, indicating potential phishing attempts for personal details.

In parallel, certain Facebook pages **offered** enticing loan deals with favourable conditions, targeting potential entrepreneurs or those in financial need. They attract individuals with low interest rates for various purchases, from appliances to real-estate. A concerning aspect involved using the real names of people not from Kosovo, connected to questionable addresses and phone numbers for WhatsApp communication. This could be an attempt to get individuals to divulge personal information, possibly for phishing or even illegal loan-sharking, a significant problem in Kosovo.

In the health sector, scams also thrived, with pages advertising products with lofty promises, like oils **promising** dramatic height increases. These products often lead users to unsafe payment sites, putting their financial data at risk. In response to BIRN's inquiries regarding the extent of these issues, the Information and Privacy Agency of Kosovo clarified that it did not register any complaints or reports related to such activities in 2023.

This absence of official reports does not necessarily reflect the reality on the ground but rather suggests a potential underreporting or unawareness among victims. It is important to note that instances leading to the theft of personal information are considered criminal offences, which would bypass the agency's purview and fall under the jurisdiction of law enforcement institutions. When asked about collaborations with social media companies to protect personal data and prevent potential unauthorised access to information, the Information Privacy Agency of Kosovo provided details of its recent discussions with TikTok. The discussions revolved around ensuring the clarity of privacy policies, upholding age restrictions in line with Kosovo's Personal Data Protection Law and appointing a local representative for effective communication.

Safer Digital Space Needed in Kosovo

In 2023, Kosovo observed a marginal advancement in internet coverage, achieving near-complete internet penetration, according to the authorities. Concurrently, there was a discernible increase in monitored digital rights violations, underscoring the imperative to address and enhance digital rights safeguards. Three primary trends were evident: manipulative misinformation campaigns, unauthorised dissemination of personal data, and the emergence of marketing scams. Prominent platforms, such as Facebook and TikTok, became significant vectors for the spread of manipulated content. Many of these violations were traced to influential social media accounts, with a considerable number also originating from recognised media outlets. State officials, journalists and public figures often found themselves at the receiving end of this manipulated content, which sought to undermine their credibility and reputation.

Another concern in 2023 was digital privacy breaches. Platforms like Facebook and Telegram played a role in the unauthorised release of personal data. Among the notable incidents was the online solicitation of identities of protected witnesses in exchange for financial rewards and the publication of personal information of Kosovo police recruits.

Such intrusions had tangible repercussions, as illustrated by decisions by certain members of the Kosovo Police to resign and the Kosovo Specialist Prosecutor's Office's decisions on witness protection matters.

Scammers used diverse tactics, often involving the impersonation of reputable institutions or advertising seemingly beneficial deals, with the primary aim of collecting personal data. While Kosovo possesses the necessary legislation and infrastructure to counter these digital challenges, its actual monitoring capacity is somewhat limited. The Information and Privacy Agency of Kosovo reported a notable absence of complaints related to online data breaches in 2023, indicating potential underreporting or a general lack of awareness among the public.

Considering the trends observed and the minimal reporting from the public, it's likely that these patterns will continue into 2024. Strengthening the digital environment requires rigorous enforcement of existing guidelines, enhanced public awareness efforts and proactive partnerships with digital platforms to uphold the digital rights of Kosovo's citizens.

Recommendations

The growing challenges related to digital rights in Kosovo demand a multifaceted approach to ensure the protection of citizens' online rights and privacy. While Kosovo has taken significant steps in establishing a legal framework for digital governance, the persistent issues in the digital landscape call for targeted and comprehensive action. To safeguard digital rights as technology continues to evolve, Kosovo's policymakers must focus its efforts on three critical areas: strengthening online privacy safeguards, combating disinformation, and expanding digital literacy initiatives.

- Establish a specialised task force to investigate online privacy violations. The unauthorised disclosure of protected witness identities and personal information of police recruits indicates a need for more rigorous enforcement. Kosovo should create a dedicated task force of cybersecurity experts within law enforcement to swiftly identify perpetrators and bring them to justice. Strict penalties for unlawful data sharing will deter future violations. The task force can also provide guidance to the public on reporting privacy breaches.
- Work with platforms to promptly remove manipulated content targeting public figures. The expansion of deep fakes and doctored images to falsely portray journalists and officials is highly damaging. Kosovo should pressure major platforms like Facebook through legal channels or financial penalties to rapidly take down verifiably false content, especially that which harms reputations or incites violence. Setting

clear policies will limit the spread of manipulated media.

- Implement digital literacy programs targeting vulnerable groups. With nearly ubiquitous connectivity, focused efforts are needed to close digital divides. The government should fund and support civil society organisations in providing digital literacy training and resources for marginalised communities, including seniors, rural citizens and minority groups. Tailored programmes addressing data privacy, online safety and media literacy could empower at-risk populations.

ETHNIC TENSIONS AND ELECTIONS BOOST DIGITAL RIGHTS VIOLATIONS IN MONTENEGRO

Elections fuelled the ethnically and politically divided country's multiple crises, resulting in a significant surge in digital rights violations, particularly online threats, smear campaigns and hate speech on social media. Perpetrators often went unsanctioned as the government's capacities and willingness to counter growing digital threats, including cyberattacks, remained low.

TOTAL NUMBER OF VIOLATIONS 177

MOST RECURRENT VIOLATIONS

Insults and unfounded accusations	104
Publishing falsehoods and unverified information with the intention to damage reputation	27
Hate speech and discrimination	26

VICTIMS

Public persons	104
Citizens	25
Journalist	25

PERPETRATORS

Citizens	134
Online Media	19
Public persons	11

During the monitoring period, Montenegro underwent significant political turbulence caused by the country's various ethnic and religious disputes. The monitoring period came not long after political turmoil led to the fall of two governments. During the monitoring period, there were several local and state-level elections, including presidential elections in March and April 2023, followed by parliamentary elections in June the same year. Before the June 2023 elections, Montenegro operated under a technical government mandate for more than a year. From June to October 2023, there was no new government in place. An increase in digital security

violations accompanied this political instability.

BIRN documented 177 cases of digital rights violations in 2022-2023, an increase compared to the previous monitoring period, when only 65 cases were registered. The primary targets were politicians, reflecting the heightened tensions surrounding elections and the unstable governmental environment. In 104 cases out of 177, public figures, including politicians, diplomats, and representatives of the Serbian Orthodox Church, but also politicians and citizens from various different ethnic and religious groups, were directly targeted online by opponents. These statistics underscore the prevailing intolerance towards political adversaries in the country, as well as the ethnic prejudice that persists.

The most frequently occurring digital violations came under BIRN's monitoring category of 'Insults and unfounded accusations', reflecting the culture of aggressive rhetoric against political opponents. Twenty-two digital rights violations were registered against ordinary citizens, primarily in online comments that showed intolerance towards ethnic and sexual diversity.

During the reporting period, Montenegro also continued to feel the consequences of the August 2022 **cyberattack** on the country's public administration. The government's digital system was irrevocably damaged, and it became clear that the state did not have an appropriate **digital security policy**. The official position of the government has so far been that the perpetrators of the cyberattack are unknown. Despite numerous inquiries, the Ministry of Public Administration didn't answer BIRN's questions by the time of publication of this report about whether there have been any developments in identifying the culprits.

Combative Political Scene Fuels Enmity Online

The recently-formed centrist political movement Europe Now, with its young leaders Jakov Milatovic and Milojko Spajic, won both **parliamentary** and **presidential** elections, ending the 32-year rule of Milo Djukanovic and his Democratic Party of Socialists, DPS. The new president and the government without

the DPS promised sweeping reforms to end corruption and combat organised crime groups. Ever since **the DPS lost power in 2020**, its prominent members and allies have been accusing the country's new political rulers of being pro-Serbia and pro-Russia due to the involvement of ethnic Serbian parties in the new government.

The digital sphere mirrored this tense and unstable political atmosphere. ''A non-stop war of disinformation and propaganda, especially by bots and trolls in comments on well-read media websites, attests to the complicated political situation throughout the year, followed by series of false bomb alerts, which were especially notable during the elections,'' Branko Dzakula, a cybersecurity expert, told BIRN. Social media users and online media committed numerous digital rights violations resulting in **online conflict** between the representatives and supporters of opposing political, religious and ethnic groups.

The violations were mostly committed by people who generally use anonymous accounts, but also by online media. People used hate speech, insults and threats to attack political opponents. BIRN also **noted** a widespread network of paid online commenters and trolls supporting political parties and ideologies on their accounts during the monitoring period. Members of the public, bots and trolls committed the majority of digital rights violations in online media outlets' comment sections. For example, a user named Njegos Urbani, suspected to be a bot, **insulted** both the Montenegrin and Albanian prime ministers, Dritan Abazovic (who is of Albanian descent) and Edi Rama, and compared them to Nazis.

Montenegrin media websites showed substantial negligence in deleting such comments, although Media Law obliges websites to remove comments that violate human rights within 60 minutes of acknowledging that they are harmful. Most of the violations BIRN noticed during the monitoring period were such comments. Online media outlets committed 19 violations during the monitoring period, including publishing information about the **private lives of politicians**, **insults**, **falsehoods** and **hate speech and discrimination on an ethnic basis**. At the same time, **journalists**

were among the most frequent victims of digital rights violations, being subjected to insults and falsehoods aimed at damaging their reputation, as well as hate speech and threats.

Among the threats against political opponents, there were also several death threats directed at prominent political and public figures. BIRN detected six such cases during the monitoring period. Former president Milo Djukanovic was **threatened with hanging**. Politician Vladislav Dajkovic received **threats** due to his Serb ethnic background and was told that he "will be crucified".

Amid this heated political atmosphere, Montenegro's capacities to counter digital rights violations, particularly when it comes to state institutions' cybersecurity capacities, remained weak. Several attempts to establish a government agency to increase cybersecurity measures were deemed ineffective by experts. During the reporting period, several state institutions' websites and email services remained disabled due to **cyberattacks** and citizens' private information was **leaked**.

Misinformation Thrives and Threats Proliferate Around Tense Elections

There were significant misinformation and disinformation campaigns around the elections during the reporting period. In April 2023, the Centre for Democratic Transition **warned** of the spread of falsehoods about the electoral process on social media and news websites in Montenegro. **Falsehoods** were also used by some online media to target political parties and their leaders. One of the most prominent cases happened during the presidential elections in April 2023, when Montenegrin outlet Aktuelno **downplayed** a **physical attack** on candidate Jakov Milatovic. Some Montenegrin media outlets, such as the widely popular Pobjeda, **reported** that the claim that Milatovic was physically attacked was "**[media] spin**". But video recordings from public broadcaster Radio-Television Crna Gora confirmed that the attack happened.

Online insults and threats to public figures increased in Montenegro during the reporting period, with state authorities and political party leaders being the

main targets. The number of threats on social media mostly increased during the election campaigns or other significant political events in the country. Former Montenegrin president Djukanovic and his wife **received death threats** on X (formerly Twitter). One X user posted **a photo** of executed Italian dictator Benito Mussolini, adding that "Djukanovic and his wife Lidija will hang like Benito and his mistress Clara Petacci... The day of revenge and retaliation will come!" Former Prime Minister **Abazovic** also received a death threat via TikTok, where a user wrote: "Beware of the sniper, Dritan," There were also reports of death threats to **civic activists**, **Serbian Orthodox Church priests**, **local officials** and other **public figures**.

Journalists and Media Outlets Face Constant Attacks

During the reporting period, BIRN identified various violations against journalists. Journalists were victims of insults and falsehoods aimed at damaging their reputation, as well as hate speech and threats. There were around 30 cases of violations towards journalists and online media. Members of the public were responsible for half of these violations, mostly in the comment sections of online media outlets. In December 2022, police filed a charge against an ethnic Montenegrin for sending **threatening messages** on Facebook to the daughter of Sinisa Lukovic, a journalist at Montenegrin daily newspaper Vijesti, warning that her father "will be expelled from the country for supporting Serbian policies". In January 2023, the Basic Court in Kotor sentenced the perpetrator to two months in prison and prohibited any contact with the journalist's daughter. There were reports of threatening emails sent to the editor of Montenegrin online outlet M Portal Danica Nikolic, when one of the senders warned Nikolic that she would "**hang from a pole as an example**".

In late 2022, numerous digital rights violations were recorded in reaction to BIRN''s publication of an interactive map, which was part of a wider project entitled 'The Future of Extremism in the Western Balkans'. The map of far-right and extremist groups in the Balkans in-

cluded 71 organisations from the six Balkan countries.

After publishing the map in mid-November 2022 BIRN received a number of complaints. The complaints mainly referred to the inclusion of two organisations from Montenegro in the database: Bogougodnice ("God Praisers") and Komite i patriote Crne Gore (Komitas and Patriots of Montenegro). After a series of internal procedures and consultations, BIRN decided to take the map offline, without prejudice, for an independent review in December 2022.

At the same time, a number of online attacks and insults were aimed at BIRN's external collaborators and researchers, specifically at Jelena Jovanovic, a journalist for Montenegrin daily newspaper Vijesti, because of her role in the project. Jovanovic, who BIRN retained as an external researcher for Montenegro, suffered public ridicule and open hostility. BIRN's own journalists and editors were also harshly insulted and threatened online.

The insults and threats against Jovanovic appeared in online media and on social networks, while BIRN editors and journalists were branded in Montenegrin and some other tabloid press as allies of the governments of Serbian President Aleksandar Vucic and Russian President Vladimir Putin, amongst other things.

Several court cases were brought against BIRN and its employees and associates. An independent review of the mapping project started in December 2022, before any of these lawsuits were filed. The legal cases are still pending.

In October 2023, after a comprehensive review of the project, BIRN published a database focusing only on the extreme right-wing organisations in the region, while transparently addressing the **lessons learned** as a result of the review process.

Online Hate Speech and Ethnic Discrimination

Another major issue in Montenegro in the reporting period was online hate speech and discrimination. A total of 26 cases were registered compared to 12 cases in BIRN's last year report. Eleven incidents involved the targeting of

Serbs and members of the **Serbian Orthodox Church**. There were three cases with **Bosniaks** and **Muslims** as targets. The ethnic intolerance was mostly expressed by members of the public but also by media and public figures. The anniversary of Operation Storm, Croatia's military operation to defeat rebel Serbs in 1995, for example, sparked an outbreak of online hatred against Montenegro's Serb population. Videos were posted online containing hate speech and **threatening** messages, as well as **hate-filled comments** supporting the mass exodus of Serbs from Croatia that happened as a result of Operation Storm. Despite the fact that media outlets and journalists were mostly the victims of digital rights violations, in several instances, some media outlets were also the perpetrators. Pro-Serbian online media outlet IN4S used **insulting language** about Albanians in an article describing an incident in Ulcinj in which dozens of young people protested against Serbs and for the idea of a 'Greater Albania.' IN4S's report used an ethnically derogatory term for Albanians and described the youths' actions as "piggery".

There were also cases of misogyny and anti-LGBT hatred in Montenegro during the reporting period. The Centre for Investigative Journalism of Montenegro reported on the **widespread hate speech** towards LGBT people that media websites permitted in their comments sections just before the Pride event in 2022. There was an outburst of hate speech online media sphere after an LGBT psychologist appeared on a TV show. The psychologist received death threats and was subsequently physically **attacked**. Some Montenegrin social media users also **condemned** the engagement of a gay couple.

Female politicians were also often targets of online hatred and misogynistic insults. A Facebook user **called** Podgorica mayor Olivera Injac "a prostitute". News website Aktuelno called ruling United Reformed Action, URA MPs Bozena Jelusic and Suada Zoronjic **"starlets of political prostitution"**, while Branka Bosnjak, Montenegro's deputy parliament speaker was called a **"slut"**.

Although hate speech in Montenegro mostly goes unpunished as the country still **lacks** basic monitoring capaci-

ties and mechanisms for reporting hate speech, in March 2023 when the police **arrested** Milos Ostojic for allegedly inciting national and religious hatred on Facebook. Ostojic, a board member at the Port of Bar, was dismissed from his post after the arrest.

No Effective Government Response to Personal Data Breaches

In 2022-2023, governmental services were often unable to use official email addresses after a cyberattack, and public administration officers had to use private email **addresses**, violating the Law on Public Service. Government bodies' websites stopped working, which caused much information to be lost. A major cyberattack **halted numerous processes** including public procurement. In August 2023, the US State Department **offered** up to $10 million for information about the cyberattacks, targeting its offer at IT experts in Montenegro with an ad campaign in Montenegrin and Russian, as many Russian IT experts have moved to Montenegro.

During the reporting period, 14 cases fall into the BIRN reporting categories of "citizen's personal data breaches" and "publishing information about private life". Opposition Social Democratic Party MP Draginja Vuksanovic Stankovic **reported to police** that she was insulted on social messaging app Viber. Stankovic said that someone added her phone number to Viber groups in which she was threatened and abused for her political affiliations and statements. In July 2023, Montenegrin police arrested two people **for threatening** a Croatian citizen that they would publish a private video of him containing sexually explicit images, without his consent. Police said the perpetrators demanded 250,000 euros from the victim to not distribute the video. The Police Directorate of Montenegro did not respond to BIRN's inquiry about updates in the case by the time of the publication of this report.

In February 2023, the Ministry of Public Administration announced it is working on establishing an Agency for Cyber Security to accord with **EU Network Information Security Directive 2**. Experts **told BIRN** that Montenegro remains vul-

nerable to cyberattacks primarily due to the lack of investments in technology and human resources. **A BIRN analysis** in June 2023 revealed that the country's Computer Incident Response Team, CIRT, a state cybersecurity team, has just seven employees, while nine officials work at the Directorate for System and Information and Communication Infrastructure. These employees represent the whole of the cybersecurity workforce involved in protecting the public administration. Cybersecurity expert Branko Dzakula argued that the need for skilled staff is the greatest challenge for the new Agency for Cyber Security. ''CIRT's team is too small for a team that should protect the whole governmental digital system. Such a team should have at least dozens of high-level experts," said Dzakula.

Tense Atmosphere Means Online Violations are Likely to Persist

In the reporting period, digital violations in Montenegro primarily reflected ethnical and political divisions, as well as cultural and religious rifts. With such tensions showing no signs of de-escalation, similar digital violations are likely to continue over the next year. "There are no signs of an improvement in communication in the online space,'' Damir Nikocevic from the Centre for Civic Education, a civil society organisation in Podgorica, told BIRN. "Montenegro is a practically media-illiterate society, resulting from the marginalisation of civic education and media literacy in the education system," Nikocevic explained. "It's necessary to strengthen the legislative framework to punish hate speech online, but also introduce measures so political forces don't abuse the online space for their political battles, because it causes unprecedented political consequences," he added.

The digital security of the government and state institutions remained a problem and the consequences of the cyberattack in August 2022 persisted into

2023, causing significant damage. Experts remain unconvinced that the country's institutions would be able to defend themselves from future attacks, as they believe the state's response to previous incidents was inept.

Cybersecurity expert Dzakula said that "such attacks often have clear political motives and require enormous resources for the preparation and organisation of an effective defence system". He said he remains optimistic about the future as the education sector is focusing on cybersecurity and new jobs are being created in the private sector, but more investment in security measures is needed from the state.

Recommendations

The prevalence of online threats, hate speech and cyberattacks in Montenegro highlights the pressing need to ensure the security and rights of the country's citizens in the digital sphere. Although Montenegro has taken some commendable steps, the digital landscape remains riddled with systemic challenges. To fortify digital rights in an ever-evolving technological landscape, Montenegro's authorities must proactively address three pivotal areas: increasing cybersecurity capabilities, combatting disinformation, and holding those responsible for violations accountable.

- Increase investments in cybersecurity infrastructure and experts. The debilitating cyberattack in 2022 revealed Montenegro's vulnerabilities. The government should allocate increased financial resources for advanced security systems, introduce cybersecurity scholarships to nurture expertise, and provide incentives for technology professionals to go into public service.
- Initiate an anti-disinformation campaign centred on media literacy. The growth of false claims and conspiracy theories leaves the public vulnerable to manipulation. Implementing widespread educational programmes that emphasise critical thinking and verification skills can bolster societal resilience against disinformation.
- Reinforce legal protections and law enforcement responses to digital

threats. The current lack of accountability for online harassment, hate speech and privacy violations perpetuates these harmful behaviours. Policymakers should enact more robust legislation criminalising digital offences and establish dedicated units for the expeditious investigation of complaints, ensuring a swifter and more effective response.

NORTH MACEDONIA

TOTAL NUMBER OF VIOLATIONS 144

MOST RECURRENT VIOLATIONS

Other manipulation in the DR environment	55
Hate speech and discrimination	52
Computer Fraud	16

VICTIMS

Citizens	104
State Institutions	25
Public Persons	14

PERPETRATORS

Citizens	76
Unknown	43
Online Media	11

NORTH MACEDONIA URGENTLY NEEDS CYBERSECURITY OVERHAUL

During the past year, North Macedonia experienced increased cases of online scams, data breaches and cybercrime, with hackers targeting several government institutions and bodies. False bomb threats sent by email, predominantly targeting schools and disrupting the educational process, represented an alarming new trend. Ethnically-motivated online hate speech persisted, while the authorities still lack a roadmap to counter digital threats.

In 2022-2023, BIRN recorded an escalating number of online scams and frauds and data breaches in North Macedonia. This was accompanied with an unprecedented surge in cybercrime, particularly in the form of hacking attacks targeting the websites of public and governmental institutions. The monitoring period saw 144 cases of digital rights violations, of which there were six notable cases in which **government** institutions, as well as international organisations operating in the country, were targeted by hackers. There were also repeated DDoS attacks that obstructed access to critical infrastructure websites, while the **authorities** struggled to defend themselves against such digital threats.

North Macedonia's citizens have also been on the receiving end of various online scams, with 16 cases of computer fraud registered. In 2023, there was a rash of false bomb **threats** mainly targeting schools in the country through emails and disrupting the educational process for high schoolers for most of the school year.

Ethnically-motivated online hate speech was also a recurring trend: in the previous reporting period, there were 26 cases of hate speech and discrimination, while in this monitoring cycle, BIRN recorded 52 cases. This period also saw multiple instances (16 cases) of hacking and online fraud, which is threatening to become a chronic problem for North Macedonia's digital ecosystem.

North Macedonia Faces Escalating Digital Rights Violations and Cyber Threats

Throughout the period covered by this report, there have been no significant legislative changes in North Macedonia that would improve the protection of citizens' digital rights. There was an initiative to pass a new **gender equality law**, which would have provided better protection for transgender people (including against online harassment), but **it was rejected.**

Several government institutions suffered from cyberattacks and system failures, but there were no significant efforts to improve the cybersecurity of digital services that are vital to the public. The Health Insurance Fund's online services were blocked by hackers, but it remained unclear whether the Fund paid a ransom for its data sets to be released, as the institution didn't provide any answers to BIRN's queries. The government denied that a ransom was paid but refused to explain how it overcame the problem.

Instances of hate speech, discrimination and online threats were consistently reported to the police, particularly when journalists were targeted. The Journalists Association of Macedonia primarily handled these cases. However, there was no notable progress in completing investigations or bringing court cases.

One of the major trends in digital rights violations involved unknown perpetra-

tors stealing citizens' personal data to obtain **quick loans** online. Following complaints from several victims, the Ombudsman started pressing institutions to take more serious measures to resolve the cases, find the perpetrators and prevent future fraud cases. The Ministry of Finance then took action and sanctioned five quick loan companies. It also announced regulatory amendments to lower the risk of future quick loan scams using false identities. However, it is not clear when the changes will come into force as the Ministry of Finance told BIRN in a written statement in September 2023 that work on them is still ongoing.

Regarding the theft of personal data, the Interior Ministry in July 2023 **warned the public** to be wary of fraudulent prize promotions in which the logos of well-known retail chains are abused and the 'winners' are asked to provide personal data to receive their prizes. Such **campaigns** are usually short-lived and social media companies take them down after the companies concerned or other parties report them, but they manage to attract a few thousand visitors in the few days they are active.

Hackers Breach Firewalls of North Macedonia's Institutions

North Macedonia also witnessed a concerning **rise** in cyberattacks. One prominent **example** was the targeting of the Agriculture Ministry by the infamous BlackByte ransomware hacking group. The consequences of this severe attack were **far-reaching**, as ministry employees grappled with a complete loss of internet access within the ministry premises for more than a month. The electronic addresses of staff members stopped working, preventing them from carrying out essential tasks.

The consequences of the breach were felt by the public as well, as critical electronic systems required for services like subsidies for farmers and the issuing of solutions were only available for a limited part of the day, causing substantial disruption. Another **significant target** of hacking attacks was North Macedonia's Health Insurance Fund, which fell victim to a prolonged **cyber offensive**. The aftermath of the assault left the Fund's

online system incapacitated for several weeks, causing considerable inconvenience to both healthcare providers and patients. As a result, the authorities sought help in dealing with the attacks from **expert teams from Germany**. BIRN contacted the Macedonian authorities and the German experts about the incident but received no response by the time of publication of this report.

Another notable incident saw the Facebook account of the OSCE Mission in North Macedonia **hacked**, illustrating how even international organisations operating in the country are being targeted. Such incidents **prompted** NATO to send a team of experts to the country in an effort to assist the authorities in dealing with cyberattacks and hybrid attacks.

School Year Disrupted by Fake Bomb Threats

Schools across North Macedonia were troubled by a series of false bomb threats in 2022-2023. The perpetrators, who remain unidentified, systematically targeted educational institutions, sending threats to the official email addresses of various schools. The capital city Skopje bore the brunt of the problem, which **persisted for several months**. In the capital alone, more than 30 elementary schools were **repeatedly targeted** by these threats.

According to the authorities, all the educational institutions received the threats almost simultaneously, always at 12.30pm, via emails, some of which had a Gmail **domain**. In response, law enforcement officers had to evacuate schools daily, implementing thorough anti-terrorist checks to ensure the safety and security of schools' premises. According to Interior Ministry data sent to BIRN by email, during the last school year, 544 false bomb threats were received in primary schools, 332 in secondary schools and 42 in other facilities – a total of 918 locations. The threats came from 76 email addresses, and so far criminal charges have been filed against four people. Additional investigations are still ongoing, the Interior Ministry told BIRN in September 2023.

Rise of Personal Data Thefts and Scams

There has been an alarming increase in cases of personal data theft, with the authorities struggling to mount an effective response or prevent such incidents. The modus operandi of the attacks involves exploiting stolen data to apply for quick loans online, all without the knowledge or consent of the unsuspecting victims. These victims, including a **person with disabilities**, a hospital **nurse** and a **local farmer, amongst others**, found themselves indebted to quick loan companies operating within the country. The consequences of the frauds committed by unknown perpetrators actions have been exacerbated by **exorbitant interest rates**, causing victims' debts to balloon. Despite the gravity of the situation, and the amount of individuals who have fallen prey to these frauds, the response from the authorities has been far from satisfactory.

The Ombudsman **called** on the authorities to address this issue with the gravity it deserves and to take robust measures to prevent future scams. Ombudsman Naser Ziberi told BIRN that a coordination meeting was held in September 2023 between him, the Deputy Prime Minister for Good Governance, Slavica Grkovska, and representatives of the National Bank, the Interior Ministry and the Ministry of Finance. He said that in the meeting it was agreed that quick loans would not be issued with online identification anymore and that the companies offering this service would be required to personally identify the loan applicants in order to avoid the risk of abuse of stolen personal data. Ziberi also said that in the future, quick loans would have to be transferred to the bank accounts of the applicants and not issued in cash or transferred to the sellers of products in order to further lower the risk of the money ending up in the wrong place without the knowledge of the victim.

The Ministry of Finance told BIRN in an email that middlemen –people who are not employees of the quick loan companies but are authorised by them to sell their loans – are being the most likely to abuse personal data because they were not ensuring that the applicants were not using stolen identities. As a result, five

quick loan companies were banned from selling loans through middlemen. The ministry also announced it will amend its Credit Risk Rulebook and require all credit applicants, including quick loan applicants, to be physically present and identified when obtaining loans.

Online Hate Speech and Discriminatory Rhetoric Against Minorities Persists

Ethnically-motivated hate speech and **discrimination against the LGBT** community have continued in North Macedonia, as in previous years. In one instance, polarising former TV host Milenko Nedelkovski used Facebook to **use hate speech** against a journalist of Albanian descent. The journalist, Furkan Saliu, shared a photograph of himself alongside Kosovo Prime Minister Albin Kurti on social media, with a welcoming message to Kurti during his visit to North Macedonia. This prompted Nedelkovski to share a screenshot of Saliu's post and add an offensive message, which sparked further hate speech in comments subsequently made on the post.

Skopje Pride Month and the subsequent **Pride Parade** in June 2023 ignited **another wave** of online hate speech and discrimination. The targets were not just the LGBT community but also **individuals**, organisations and businesses that expressed their solidarity with the cause of LGBT equality and human rights. In general, during 2022-2023, BIRN noted an alarming escalation in organised attacks and smear campaigns against LGBT people on social media.

Critical 2024 Elections Hang in the Balance Due to Cybersecurity Issues

Digital rights violations recorded in 2023 have highlighted the significant challenges that North Macedonia faces in terms of cybersecurity infrastructure, as well as the importance of international **cooperation to combat them**.

The false bomb threats targeting schools also showed the need for comprehensive strategies to address such incidents and ensure the security of educational institutions and the safety of their students.

The rise in personal data thefts and scams highlights the urgency of implementing effective regulatory and enforcement mechanisms to safeguard citizens from financial exploitation. The government's response to this issue must involve improving law enforcement capabilities and prioritising the protection of vulnerable individuals who have fallen victim to these schemes.

"The first and most important thing is to strengthen the capacity for cybersecurity awareness, since users are the weakest links. Therefore, we need to make sure that all phishing campaigns are properly detected and dealt with," Skopje-based cyber security engineer Milan Popov told BIRN.

"Data protection is next, since it is still not clear how much of our data was leaked during the attacks on government agencies in recent years. We can protect all of that by investing in people and technologies, and one of the best solutions would be, since there is a lack of experienced engineers working for state agencies, to aggregate the systems and manage them in a centralised environment where these skilled workers would deal with various cybersecurity challenges," Popov added.

The country will also have new parliamentary elections in 2024, which will undoubtedly generate more digital violations in what can be an ethnically-tense country, highlighting the need to create a safer online environment.

Recommendations

The escalation of cyberattacks, misinformation campaigns and personal data violations in North Macedonia highlights the need for robust action to safeguard the public in the digital realm. While North Macedonia possesses a legal framework on cybersecurity and data protection, systemic weaknesses undermine enforcement. To secure digital rights as technology advances, policymakers in the country must urgently prioritise reforms across three vital areas: fortifying cyber defences, regulating online financial services and countering disinformation.

- Centralise cybersecurity operations to defend critical systems. Decentralised and under-resourced cybersecurity has left institutions vulnerable, as shown by recent hacking incidents. North Macedonia should consolidate cybersecurity under the Ministry of Information Society and Administration and devote adequate funding to hire experts and implement advanced threat detection systems.

- Increase oversight of online lending companies to combat predatory practices. The rise in personal data thefts used for unlawful loan applications reveals regulatory gaps. Policymakers should mandate know-your-customer practices for digital lenders, limit excessive interest rates and establish penalties for facilitating identity fraud.

- Bolster societal resilience to misinformation and disinformation through educational campaigns. The spread of false claims and conspiracy theories enables the manipulation of public opinion. Large-scale programmes run by civil society groups focused on verifying sources and thinking critically can improve people's abilities to identify misinformation and disinformation.

ROMANIA

TOTAL NUMBER OF VIOLATIONS 169

MOST RECURRENT VIOLATIONS

Other manipulations in the digital environment 59

Threatening content and endangering of security 45

Publishing falsehoods and unverified information with the intention to damage reputation 34

VICTIMS

Citizens 126

State Institutions 49

State Official 12

PERPETRATORS

Citizens 55

Unknown 34

Online Media 27

ROMANIA SUFFERING FROM MEDIA MANIPULATION, ONLINE ATTACKS ON WOMEN AND JOURNALISTS

Romania witnessed an increase in digital rights violations, with 40 more incidents documented than in the previous reporting period. The increase was influenced both by internal factors, such as the governing coalition undermining media objectivity by directing generous amounts of money in state grants to media companies, a practice criticised by the US State Department, and the war in Ukraine, which brought new disinformation narratives to Romania.

During 2022-2023, digital rights violations in Romania increased and deepened, with 169 cases documented by BIRN compared with 128 recorded in 2021-2022. Romania enjoyed relative political stability, with a coalition government leading the country since late 2021. However, there was an increase in political control over specific media outlets — mainly traditional electronic media — through political parties' funneling of money they received in state grants to media companies. Statistics **showed** that the two ruling coalition parties spent the most on media and promotion in 2022. On the other hand,

Romania still has a vital sphere of independent media outlets, mainly online, which are critical to the government.

More than a third of all cases registered by BIRN involved fake news, disinformation, propaganda or misinformation. This represented a substantial increase from the 19 cases reported in the previous year, with the recurrence of online scams and a growth in misinformation campaigns related to Russia's war against Ukraine.

Ordinary citizens remain the primary targets of online attacks, with one in five of these being sexual in nature. There were 28 violations connected to sex crimes recorded during the reporting period, ranging from recruiting victims online to the distribution of sexually-explicit images and child pornography. This trend complements the view of the US State Department, which described Romania as a **prime** source country for sex trafficking victims in Europe. But it also indicates how criminals involved in sexual exploitation have adapted to using new technologies in Romania.

Governmental Stability Doesn't Ensure Online Calm

During the reporting period, there were no elections in Romania. Since late 2021, the country has been governed by a coalition formed by the Social Democratic Party and the National Liberal Party. This was reflected in the amount of state cash passed on by the political establishment to the media, with the total doubling in 2022 to 20 million euros, **according to the NGO Expert Forum**. The money comes from state grants received annually by all parliamentary parties in Romania, depending on their representation in the Senate and Deputies Chamber. It is then transferred by the parties to advertisement agencies, which in turn direct the money onwards to online media and TV companies.

This opaque and often corrupt media-financing mechanism was **criticised by the US State Department**. The two parties making up the coalition government spent by far the most on advertising contracts with media companies, **said the Electoral Authority**. The two coalition members, the Liberals and the Social Democrats, respectively directed 70.7

percent and 58.5 percent of the state grants they received as parliamentary parties towards media and promotional spending. Comparatively, the biggest spender from the opposition allocated just 27.6 percent of the money it received in state grants for spending on contracts with media companies.

Romania has been on alert due to the full-scale Russian invasion of neighbouring Ukraine. However, Romania has not been exposed to serious security threats, with only a few reported incidents involving a couple of mines on the shore and missile debris falling in remote areas on the border with Ukraine. Since the invasion started, there have been several disinformation campaigns about a purported compulsory general mobilisation, **according to the Romanian Defence Ministry**. Although the Romanian authorities didn't blame the Kremlin, they did accuse the perpetrators of seeking to incite panic during the most recent 'compulsory mobilisation' disinformation campaign **in March 2023**.

Romania saw significant advancements in legislation **surrounding AI**. June 2023 saw the passing of a much-awaited **bill making so-called 'revenge porn' a crime**, punishable by up to three years in jail, as well as the introduction of **restrictions on the use of deepfakes** in Romania. There were also two significant cases involving journalists. In April 2023, the death by suicide of Iulia Marin, a reporter for the daily newspaper Libertatea, dominated headlines. After Marin's suicide, journalists who work for **broadcaster RTV** questioned the reliability of investigations published by Marin in Libertatea. The Audiovisual Council **ordered** RTV to pay a record fine of 20,000 euros for its biased coverage of Marin's death.

Meanwhile, investigative journalist Emilia Sercan criticised the prosecution's slow pace in investigating the leaking of her intimate photographs from a police file in early 2022. "The Prosecutor's Office is still ignoring the details that could solve a leak from inside the police," **Sercan said in February 2023**. However, in early November 2023, Romania's Prosecutor Office at the Bucharest Court of Appeal abruptly closed the smear campaign investigation against

journalist Emilia Sercan. This caused a dozen international media organizations to express their "dismay at abrupt closure of investigation" in a **joint letter**.

Sex-Related Crimes Go Digital in Romania

Sex-related crimes perpetrated using digital methods represented 16 percent of all cases documented by BIRN between September 1, 2022 and August 31, 2023. A total of 18 out of the 28 sex-related digital violations involved either child pornography or the distribution of sexually explicit images of individuals without their consent.

Perpetrators used social media platforms, mostly Facebook and Instagram, to both **recruit underage victims** for the production of child pornography and to **spread so-called 'revenge porn' material**. Mobile apps were used to exchange child pornography, as in **the case of a psychotherapist** from a social services centre who was indicted for producing child pornography with two male minors, and sentenced to three years of **probation** in August 2023.

"In recent years, there has been a massive increase in the number of people sexually exploited online. In 2022, there were 1,246 child pornography cases on trial around Romania. And this is just the tip of the iceberg, as many parents don't go through with their criminal complaint. They give up because of the system," Loredana Mirea-Urzica, advocacy director at eLiberare, a Romanian NGO assisting victims of sex trafficking, told BIRN.

Romanian judges work according to a **law from 2008**, which makes it possible to give offenders suspended sentences. Of the three sentences convicting child pornography offenders that were recorded by BIRN, only one included jail time. However, there were important advancements in legislation, with the passing of a law designed to **criminalise so-called 'revenge porn'**, as well as an **increase in jail time** for statutory rape if the crime happened after June 2023. Previously, sexual offenders could get a minimum sentence of one to two years' probation for statutory rape while now there is a minimum sentence of seven years in prison when the victim is younger than

16 and there is an age difference larger than five years.

BIRN documented nine cases in which Romanian traffickers used social media platforms to recruit women and girls for prostitution, either in the country or in Western Europe. Romania is as a prime source country for sex trafficking victims in Europe, the US State Department said in its **2023 Trafficking in Persons Report**. However, the Romanian the authorities gained international plaudits on December 2022 by dismantling an **operation run by influencer Andrew Tate**, which involved alleged sexual exploitation through 'cam girl' work by women recruited on social media platforms. Tate and his co conspirators are currently awaiting trial in Bucharest.

Spending by Political Parties Undermines Media Objectivity

Romania's position in the annual World Press Freedom Index, **compiled by Reporters Without Borders**, RSF, has been falling steadily in recent years, from 44th out of 180 countries worldwide in 2018 to 53rd in 2023. "The lack of transparency of media financing, especially from public funds... is undermining the reliability of information and the trust in the media," **said RSF**, calling the media funding mechanisms used by political parties in Romania opaque and corrupt.

In recent years, some media companies have become more and more reliant on the state grants received by political parties based on their performance in general and local elections. In 2022, political parties received more than 51 million euros in state grants, a huge increase from the six million euros they were receiving in 2017, before the political parties' funding bill was amended by the Social Democrats. The law allows parties to divert the state funding they receive towards advertising agencies, which then award generous contracts to online media and broadcasters. As these contracts are protected by commercial confidentiality, the public are unable to see how much money a media company has received from a political party.

Although political parties splashed 20 million euros in state cash on media companies in 2022, BIRN's monitoring showed scarce covering of this issue in national media, with articles only to be

found in several online and print sources, among them Radio Free Europe Romania, Libertatea, and G4Media.

"This media financing mechanism is lacking in transparency, especially when it comes to the big political parties - the Social Democrats and the Liberals. It's a toxic system, through which money goes to certain online media, but we don't know to whom. In 2024, paid information might distort the elections. I've already seen instances of self-censorship in reporters", Cristian Andrei, a political journalist at Romanian daily newspaper Libertatea who investigated state cash being distributed by political parties to the media, told BIRN.

Romanian Army Targeted by Disinformation Campaigns

Since the beginning of Russia's full-scale invasion of Ukraine, many countries in the region have seen an increase in disinformation campaigns. These activities also targeted institutions, like the Romanian Army, one of the country's most trusted institutions, as noted by **Bertelsmann's 2022 Transformation Index**. However, a survey by the **Romanian Academy** showed a 10 percent drop in the public trust enjoyed by the Army at the end of 2022. This overlapped with five disinformation campaigns about alleged compulsory mobilisation in Romania.

On March 9, 2023, the Defence Ministry warned the public to be wary of compulsory mobilisation posts, which once again gone viral on TikTok and Instagram. This also happened on **February 9, 2023**, **October 14, 2022**, and in the first two months of the full-scale Russian invasion of Ukraine. This trend is likely to continue, given Russia's new focus on bombing Ukrainian grain transports going to Romania.

Romania Starts Addressing Responsible Use of AI

On June 27, 2023, the Romanian parliament's upper house voted in favour of a bill meant to **criminalise** the "malicious use of technology" by restricting the use of deepfakes. Though it still has to pass the he lower house of the Parliament, the bill is already making history as the first to address the responsible use of artificial intelligence in Romania,

one of the last countries in the EU lacking a national strategy on AI, **according to the government**. If the legislation is adopted, lawbreakers would face a fine of 2,000 to 20,000 euros, with a maximum fine of 40,000 euros being given to repeated offenders by the National Audiovisual Council.

So far, few AI-related violations have reached the courts, and those which have were in civil trials. Most recently, **in Giurgiu**, 60 kilometres south of the capital Bucharest, a teenage girl was found guilty in April 2023 of publishing a deepfake porn video on YouTube. In the video, she used the face of one of her schoolmates, a male minor. Judges at Giurgiu Court ordered the girl's parents to pay 1,000 euros in compensation to the victim's family. Such cases might be differently handed in the future, as the Romanian authorities put together a **committee** in November 2022 to develop a national strategy for AI in collaboration with experts and NGOs.

Young Hacktivists Target Public Institutions in Romania

On June 29, 2023, prosecutors detained three suspects, including a minor, accusing them of conducting so-called **'hacktivism' attacks** on Romanian public institutions since November 2022. An investigation is ongoing into suspected members of Romanian Operation, a hacking group which compromised websites and social media pages belonging to public institutions and officials to denounce corruption. While the exact number of attacks has not been specified, the group gained notoriety for **defacing** the Ministry of Education's website in May 2023. Two suspects were put in pre-detention by the Bucharest Tribunal a month later, while a minor was released on probation.

In an unconnected incident in September 2022, prosecutors **dismantled** a hacking operation led by 'Meowless', an alias used by a teenage hacker with minimal formal education, who learned hacking skills from YouTube and was involved in targeting a police website and a county council website.

Stronger Legal Framework Needed to Tackle Violations

In the reporting period, there was an increase in attacks directed against individual citizens, with 125 such incidents recorded. Around one quarter of them were sexually motivated attacks on women or girls. Still, Romania lacks not only the resources but also the personnel trained to deal with sex-related crimes. The US State Department recommending introducing measures to ensure access to assistance for all women, training for investigators, prosecutors and judges working with trafficking victims – some of whom have been exploited in online pornography schemes in Romania – as well as the proactive identification of vulnerable women.

The political landscape next year is likely to remain dominated by the National Coalition for Romania, formed by the two biggest political parties in late 2021. There are **ongoing negotiations** for a common list at the parliamentary elections, which are set to take place at the end of 2024. The current situation, in which there has been increased censorship at media organisations because their finances are sustained by large state grants given by the Liberals and Social Democrats, could persist after the general elections.

Looking ahead to 2024, it is crucial for Romania to further strengthen its legal framework to ensure that digital rights and privacy are protected. "When it comes to regulating the digital [sphere], almost no authority or institution understands its role. If we're talking about the IT parliamentary committees, their members don't even know the difference between the types of providers mentioned in EU legislation," Bogdan Manolea, executive director at the Association for Technology and Internet, told BIRN. "The Romanian authorities are unprepared. The Digital Services Act should come into effect on February 17, 2024. And so far, there is no public information about who should do what to enforce the DSA," Manolea said.

The role of social media platforms in addressing these issues will also be a critical factor, as fake news, disinformation and misinformation campaigns increased to make up 59 out of the 169

digital violations which BIRN registered during the reporting period.

Recommendations

The rise of online exploitation, disinformation campaigns and threats to media independence in Romania highlight the need for multifaceted actions to secure digital rights. While Romania has passed some legislation, systemic weaknesses in enforcement undermine protections. To safeguard digital rights as technology advances, decision-makers in the country must urgently prioritise reforms across three key areas: strengthening child safety systems, countering propaganda and ensuring media objectivity.

- Establish a national task force on online child protection. The disturbing prevalence of child pornography and grooming cases necessitates a coordinated response. Romania should create a specialised law enforcement task force dedicated to promptly tracking online offenders, providing assistance to victims and implementing preventive education. This task force can serve as a dedicated unit to combat child exploitation in the digital realm, ensuring that the most vulnerable members of society are protected from online predators.
- Launch anti-propaganda initiatives to build societal resilience. The dissemination of false narratives, particularly on sensitive topics such as the military, leaves citizens vulnerable to manipulation. Large-scale media literacy campaigns can empower individuals with critical thinking skills, enabling them to discern propaganda and false information from credible sources. By fostering a more discerning and resilient society, Romania can reduce the impact of propaganda campaigns on its citizens.
- Increase transparency around media funding and ownership. The lack of clarity regarding financial ties and political influence raises concerns about media objectivity. Policymakers should introduce reforms aimed at enhancing transparency, such as requiring mandatory public disclosures of media backers and implementing restrictions on

state advertising. By shedding light on media ownership and funding, Romania can bolster the objectivity and integrity of its media landscape, ensuring that citizens have access to unbiased and trustworthy information sources.

SERBIA

TOTAL NUMBER OF VIOLATIONS 103

MOST RECURRENT VIOLATIONS

Threatening content and endangering of security 35

Hate speech and discrimination 16

Computer Fraud 14

VICTIMS

Citizens 50

Journalists 20

Public Persons 13

PERPETRATORS

Citizens 20

Unknown 41

Online Media 9

DIGITAL RIGHTS VIOLATIONS INTENSIFY AS SERBIA'S POLITICAL CRISES MULTIPLY

Digital rights violations in Serbia became more severe in 2023 after two unprecedented mass shootings sparked outrage. There were large numbers of cases of hate speech, private data breaches, and discriminatory rhetoric, with journalists and activists facing an increase in threats and insults.

In Serbia, the number of digital rights violations covered by this report, **spiked drastically** in May 2023 after two mass shootings, in Belgrade and villages Malo Orasje and Dubona in the Mladenovac municipality, with more serious violations recorded than in the rest of the year. Dissatisfaction with the government erupted into mass protests after the shootings, and demonstrations continued on a smaller scale into the late autumn. The reporting period was characterised by intense political discord, protests, governmental upheavals and heightened rhetoric.

Over the course of a year, BIRN registered 103 cases of digital rights violations in Serbia. The most frequent targets of these incidents were citizens (50 incidents), while a significant number

of incidents affected journalists (20). A considerably smaller number of incidents affected politicians, political parties and government institutions. Many of the perpetrators of digital rights violations remained unidentified (41 cases), and the source of many attacks remained unclear despite the targets being evident. The anonymity of attackers in the digital sphere reflects a lack of accountability for digital rights violations and a lack of transparency. BIRN repeatedly asked Serbia's specialist prosecutors' office for high-tech crimes for a comment on this issue but received no answer by the time of publication of this report.

The majority of digital rights violations in Serbia came under BIRN's reporting category of "threatening content and endangering security" (35 cases). A significant number of cases (16) involved hate speech and discrimination. Many attacks targeted people who are vulnerable or publicly exposed, including children, female journalists and investigative reporters. Institutional protection mechanisms and existing regulations were **not sufficient** to deliver an adequate response to these incidents. Although there were fewer cases compared to the previous reporting period, the violations themselves have become significantly more intense in character.

Political Tensions Spark Digital Rights Violations

The tension in the digital space in Serbia over the past year has been a direct result of conflicts in the political sphere. During the reporting period, two major issues have generated the largest number of cases in the monitoring. The first was the mass shootings in **Belgrade** and villages **Malo Orasje and Dubona**, which left 18 people dead and 19 people injured and provoked **street protests**. Demonstrators expressed their discontent about the endorsement of violent behaviour in the public arena by pro-government media. Anger was **directed** towards public broadcaster RTS and the Pink media company, whose owner, Zeljko Mitrovic, has been accused of using Pink's national frequency to spread disinformation and propaganda.

The other major issue causing digital violations was the political tensions

around Kosovo. At the end of 2022, Kosovo Serbs **left Kosovo state institutions** and boycotted **local elections** in April 2023. The situation in Serb-majority northern Kosovo then **escalated in May 2023**. When Kosovo Albanian mayors took their seats in Serb-majority municipalities, there was an **outbreak of violence** between Kosovo Serb protesters and Kosovo police, which then involved NATO peacekeepers. The violence happened on the same day as a rally organised by the ruling Serbian Progressive Party in Belgrade aimed to show support for the government amid the mass protest in Serbia. In this tense situation, there were several attacks on journalists, media workers and activists, particularly those who have expressed critical opinions about the Serbian Progressive Party or the **Orthodox Church**.

After protesters and the political opposition called for an end to the promotion of aggressive rhetoric in the Serbian media, the owner of pro-government Pink TV responded by using artificial intelligence to create videos mocking opposition politicians. The Serbian President and the Government **announced** Parliamentary and local elections for December 17, 2023, even though presidential and parliamentary elections were held in 2022. Elections will take place in the atmosphere of the increased tensions in the digital space. There was an increase in the use of social media accounts run by paid online propagandists, while threats and insults directed at journalists and activists became increasingly commonplace.

The **Freedom on The Net 2023** report from Freedom House rated Serbia's digital environment as free, but said it had suffered a slight decline since the previous year. The main problems identified by Freedom House were pro-government news sites that engage in disinformation campaigns, employed paid online propagandists, the surveillance infrastructure and Strategic Lawsuits Against Public Participation (**SLAPP lawsuits**). According to a **report** for 2023 by the CASE coalition, which campaigns against SLAPPs, 28 SLAPP cases were recorded in Serbia during the year.

Unethical Use of AI Boosts Digital Rights Violations

A recent example of unethical usage of the AI was a news article about Serbia allegedly ordering 20,000 Shahed armed drones from Iran, which was first published by Terror Alarm, and was entirely generated by AI. The false AI-generated report was then republished by many outlets. It turned out that the AI technology used to generate the article made a mistake. However, Serbia's Deputy Assistant Minister for Bilateral Cooperation Goran Aleksic did visit Tehran in August 2023, and met his Iranian counterpart Ali Bagheri, but there was no information about Serbia ordering Shahed drones.

In another example, a deepfake was used to spread false information. On August 7, 2023, Zeljko Mitrovic, owner of pro-government TV Pink, published AI-manipulated footage of **Marinika Tepic**, the vice-president of the opposition Freedom and Justice Party, misrepresenting her remarks. On August 12, 2023, Mitrovic did the same with **Dragan Djilas**, president of the Freedom and Justice Party, airing the video on TV Pink as 'satire'. Mitrovic **posted** a deepfake on X (formerly Twitter), and later showed it on TV, without the audience being properly informed while it was showing that it was fabricated. The deepfakes included simulated voices falsely pretending to be Tepic and Djilas mocking opposition colleagues and speaking offensively about them. After facing a lot of criticism, the **Regulatory Authority for Electronic Media** argued that it is the responsibility of the media to prevent the improper use of someone's likeness and voice, yet it did not take any tangible steps towards implementing its decisions or take measures to deal with the issue.

Djilas sued both **Mitrovic and TV Pink**. He also requested the removal of the contentious video from YouTube and sought a court order for temporary measures to prohibit the broadcasting and rerun of the video. However, the video remained available on Mitrovic's YouTube channel. This is the first time that a high-level private lawsuit has been launched in Serbia over the alleged misuse of artificial intelligence. In his response to the lawsuit, Mitrovic stated

that the video was satire and represented legitimate artistic expression. A hearing in the case has yet to be scheduled.

"The use of AI in media is perceived as a form of entertainment," Aleksandra Krstic, a professor of media sciences at the University of Belgrade's Faculty of Political Science, told BIRN. "This is truly dangerous because when we put words into the mouths or facial expressions onto people who did not have those facial expressions or utter those words, we enter a realm in which disinformation spreads, public opinion is manipulated and individuals are abused. It also sends a message to the public that anything goes in the public arena," she added.

In Serbia, the rise of fake accounts and fabricated content is notable, with 12 cases documented during 2022-2023. Despite the government's **2020-2025 AI Development Strategy** and associated **Ethical Standards**, which it adopted in March 2023, no regulations specifically address AI-generated media content. This regulatory gap leaves **the field unchecked.**

Personal Information Leaks Put Public at Risk

The first of the two mass shootings in May 2023, at the Vladislav Ribnikar school in Belgrade, was a **trigger** for privacy and personal data breaches, data leaks and illegal data processing. After the school shooting, Veselin Milic, the chief of the City of Belgrade Police Department, revealed the first and last name of the minor who was the perpetrator, and displayed a list of children that the perpetrator intended to kill. A few hours later, the president of Serbia, Aleksandar Vucic, quoted private information about the teenage boy.

"There are two key issues here - one is ethical reporting by the media and the other is how institutions manage information," Ana Toskic-Cvetinovic from Partners Serbia, an NGO, told BIRN. Toskic-Cvetinovic said that "no one raised the question" of holding anyone responsible for revealing personal information about the minor.

In the days that followed, mainstream media in Serbia published large amounts of personal data about the victims and

the underage perpetrator, and about their families and friends. Several days after the school shooting in Belgrade, videos allegedly depicting the incident began circulating on TikTok. The **exposure of personal data** — the victims', their families and the perpetrator's - seriously compromised their privacy and security and motivated members of the public to begin **street protests**.

The authorities responded with police action against people who glorified the teenage murderer, resulting in **several arrests.** Twenty-nine elementary school students were arrested for copycat attacks (mostly without weapons) or for celebrating the murders on TikTok. Criminal charges were **filed** against 82 individuals within a month of the mass shootings.

Months after the incident, private data leaks persisted. Court hearings in the case against the underage perpetrator were held, with mainstream media repeatedly disclosing information about them, as the crime continued to be a catalyst for widespread digital rights violations. However, Toskic-Cvetinovic said the case should be a catalyst for establishing better practices. "Such a case should set a precedent for establishing standards and practices for accountability because it is a sensitive case involving children, and it is necessary to determine responsibility [for any violations]," she said.

Human Rights Defenders Smeared Online and Offline

After Sofija Todorovic, the programme director in NGO Youth Initiative for Human Rights in Serbia, **called** for Kosovo to be given membership of the United Nations, she was attacked on social media and the façade of the building where she lives was defaced with **threatening graffiti** including her full name and a sexist and misogynistic insult, as well including the letter 'Z', which symbolises support for Russia's war against Ukraine. When the Youth Initiative for Human Rights published information about the **attacks** on social media and the graffiti, the attacks intensified, and Todorovic and anyone who expressed support for her and her statements was harassed on social media. The Youth Initiative for Human Rights said it noti-

fied the police about the threats and intimidation, criticising the lack of a clear response from the institutions to the attacks on the activist.

Hate speech in Serbia, particularly directed at activists, **journalists** and public figures, is not uncommon. Besides the Todorovic case, Serbia has witnessed at least 15 other cases of hate speech over the past year, but the authorities have not taken any appropriate steps to prevent such cases in the future. The ruling Serbian Progressive Party has been increasingly antagonistic towards activists and journalists, as well as everyone working in the human rights sector, in recent years. This has created an atmosphere in which it is considered normal to direct insults and threats at activists and journalists. These insults and threats no longer originate solely from officials, but also from ordinary citizens and members of the public. Often such intimidation goes unpunished. In July 2023, a group of around 50 individuals attempted to disrupt a forum against **hate speech and homophobia in Krusevac** after misinformation about the event spread on social media. During the attack, an LGBT activist was assaulted.

Alleged Online Propaganda Network Linked to Serbia's Ruling Party

A **list** of over 14,000 suspected fake accounts allegedly associated with Serbia's ruling Serbian Progressive Party, SNS surfaced on X (formerly Twitter). The list, complete with names and locations of those allegedly behind the accounts, implicates individuals who work in the public sector across the country, raising serious questions about their involvement in political activities during work hours. According to the list published by **Fake News Tragac**, there are 3,162 individuals engaging in propaganda activity on behalf of the ruling Serbian Progressive Party. Although the list includes 14,000 accounts, one person typically manages multiple accounts, presenting themselves under various false identities.

In 2020, **BIRN** reported on the widespread use of paid online propagandists to agitate for the Serbian Progressive Party. BIRN gained exclusive access

to the network for several months in 2019, observing how hundreds of people across Serbia logged into the Castle, an internet database used by the ruling party to manage the paid propagandists, everyday during normal working hours. The paid propagandists then used their accounts to promote Progressive Party propaganda and disparage opponents, in violation of rules laid down by social network companies like X (formerly Twitter) and Facebook to avoid the coordinated manipulation of opinion. X (formerly Twitter) disclosed three years ago that it had removed **8,500 accounts** that were serving the Serbian Progressive Party.

Of particular concern is the reported involvement of public sector employees in these activities, conducting political work under their own names during official working hours. While some individuals have **confessed** to their participation and issued apologies, others swiftly deleted their accounts. The response of the government and the Serbian Progressive Party has been the launch of a campaign called '**I am also a bot.**' Politicians from the ruling party expressed their support for the campaign by **sharing photos** of young people on social media, accompanied by the message: "Yes, I am an SNS [Serbian Progressive Party] bot. I love Serbia and the Serbian Progressive Party more than anything in the world."

Serbia Lacks Comprehensive Strategy to Counter Digital Threats

The trends and major cases registered during the reporting period shed light on key issues in Serbia's digital landscape. Most of these issues recur year after year. But an important new trend is the misuse of artificial intelligence, which has emerged as a potentially potent tool for manipulating public opinion and discrediting political opponents. The use of AI has also raised serious questions about journalistic ethics and transparency. The legal ramifications and societal implications of the misuse of AI are a topic of widespread concern and debate.

The unauthorised leaking of private information, especially in the aftermath of tragic events or crimes, has demonstrated a glaring gap in digital privacy aware-

ness and responsible data handling. The uncontrolled dissemination of personal data has not only compromised individuals' privacy but also fuelled the spread of misinformation and sensationalism, making a significant impact both on the individuals who are directly affected and the general public.

The continuing problem of hate speech against activists and journalists online highlights the need for robust responses from institutions to protect free speech and promote respectful dialogue. The prevalence of misinformation-spreading paid online propagandists within the Serbian political landscape raises serious questions about the integrity of public discourse and the role of public sector employees in such activities. The governing party's response - a campaign that appeared to celebrate this phenomenon - underscores the complex relationship between politics and social media in Serbia. This is particularly concerning ahead of elections in Serbia at the end of 2023. Furthermore, since there is no regulation to guide AI usage, it may be expected that the abuses of this technology will increase. "Serbia lacks a comprehensive strategy to combat disinformation and to make efforts to defend public opinion and citizens' public interest from digital rights violations in the online world," media sciences professor Krstic said.

A recently-adopted set of media laws is unlikely to resolve the issue of distorted and polarised public narratives. One of the main criticisms of the legislation is that it legalises the state's re-entry into media ownership, allowing it to own media outlets via its control over telecommunications company **Telekom Serbia**.

As for the other trends observed in this report, they are also likely to intensify before and after the elections, as periods of tension often result in attacks, hate speech and threats against activists and journalists. Therefore, the coming period could see numerous violations, possibly including SLAPP lawsuits aimed at silencing journalists.

Recommendations

At the end of 2023, Serbia finds itself at a critical crossroads in the realm of digital rights, grappling with an intricate

set of challenges that demand immediate attention and innovative solutions. The country's digital landscape has witnessed a notable increase in digital rights violations, exacerbated by political turmoil and the unchecked exploitation of artificial intelligence and social media platforms. Consequently, the authorities should adopt a measured approach, considering alignment within the EU regulatory framework in the AI sector, reinforcing institutional protections for digital rights and encouraging the activities of civil society organisations that are actively engaged in addressing these concerns.

- Media regulatory and self-regulatory bodies, along with civil society, academia, media associations and other professional bodies should begin dialogue about the establishment of clear professional and ethical standards for AI usage in media content production. The result of this dialogue should be embodied in the Code of Journalists and upcoming regulatory initiatives to encourage responsible use of AI.

- Strengthening and empowering current bodies. A prudent course of action would be to enhance the capacities of entities such as the Ombudsman, the Commissioner for Freedom of Information and Data Protection, the Commissioner for Protection of Equality and the established working group for journalists' safety, as well as to ensure that they carry out their mandates thoroughly. This approach would optimise resources and expertise while reinforcing the current framework for protecting digital rights and addressing violations effectively.

- Support grassroots digital literacy initiatives. Encourage and fund local grassroots initiatives, led by civil society organisations and community leaders, to educate the public, particularly people who live in marginalised areas, about digital media literacy. These initiatives should employ culturally tailored strategies to impart critical thinking skills, promote responsible online behaviour and help individuals differentiate credible information from disinformation.

By engaging at the community level, Serbia can empower its citizens to be active and informed online.

DIGITAL RIGHTS UNDER ATTACK FROM ERDOGAN'S ISLAMIST GOVERNMENT

Digital rights violations in Turkey in 2023 continued to escalate as President Recep Tayyip Erdogan's election-winning government use draconian laws and regulations to target media houses and social media platforms with court cases and fines. Meanwhile citizens' private data remain unprotected, and vulnerable groups' rights in the digital arena were repeatedly violated in what remains a highly polarised society.

TOTAL NUMBER OF VIOLATIONS 42

[THE MONITORING IN TURKEY STARTED IN JULY 2023]

MOST RECURRENT VIOLATIONS

Pressures because of publishing information	11
Insults and unfounded accusations	7
Hate speech and discrimination	6

VICTIMS

Citizens	16
Online Media	14
Public Persons	7

PERPETRATORS

State Institution	13
State Official	7
Public Persons	3

In 2022-2023, digital rights violations in Turkey intensified as the government of President Recep Tayyip Erdogan deployed courts, fines and government agencies to limit the free speech of media houses, social media companies, journalists, artists and others. As a result of the government's policies, Turkish society has remained highly polarised, divided by ethnic, religious and cultural issues. This has resulted in vulnerable groups such as the LGBT community and refugees being targeted online by pro-government media and Islamist groups that enjoy impunity.

BIRN's Digital Rights Violations database started to register incidents in

Turkey for the first time in July 2023. Before that, digital rights violations in Turkey were covered by Balkan Insight, BIRN's flagship English-language publication. This country report is based on July and August 2023 data, but also on Balkan Insight articles, including news reports, interviews and analysis pieces that focused on digital rights violations in Turkey over the rest of 2023.

In July and August 2023, a total of 42 cases were registered in the BIRN database. Citizens being the most frequently affected parties (16 cases). What was particularly alarming was that people categorised as either "unknown" and/or "state official" were registered as being responsible for most of the incidents (33 cases each).

Incidents registered under the BIRN database's category of "insults and unfounded accusations" (eight in total) highlighted the aggressive nature of some of these violations, which often targeted individuals and media outlets.

The violations in 2023 are a direct result of deterioration in digital rights in Turkey in previous years. Legislation and regulations such as the so-called disinformation law or new regulations aimed at increasing government control over digital platforms aiming have become the main basis for the authorities' abuses in the digital sphere.

Elections and Autocratic Political Islamism Shape Turkish Digital Space

Events in 2023 in Turkey revolved around the parliamentary and general elections held in May 14, 2023. A united opposition bloc in Turkey has high hopes of unseating Erdogan and his Justice and Development Party, AKP, in the elections after years of economic turmoil, deepening authoritarianism, and twin earthquakes in February 2023 that killed more than 55,000 people and exposed widespread corruption in the building sector. With the elections fast approaching, President Recep Tayyip Erdogan issued a warning to those who criticised his government's response to the crisis in the media: "We will never forget them." Watchdogs **said** there has been a "spike in censorship" in Turkey since the elections in May 2023, with the gov-

ernment using the courts to exact revenge on journalists and media outlets that went against the president and his ruling party.

The election process fuelled misinformation on social networks. Some of this was even spread by President Erdogan himself, when he showed an election video made by the opposition alliance that had been manipulated by unknown people to include the leaders of the outlawed Kurdistan Workers' Party, PKK. Portraying alleged "terrorist" leaders as supporting the opposition was aimed at harming the opposition in the eyes of the electorate. "The fact that an edited video was widely shared on social media accompanied by the claim that it was part of the opposition's election campaign, and that it was personally shown by the president at a political rally, is a very worrying development as regards digital rights in Turkey. Far worse than this, no legal steps were taken and there was no major public debate about this," Gurkan Ozturan, Media Freedom Rapid Response Coordinator at the European Centre for Press and Media Freedom, and country author for Turkey of Freedom House's Freedom on the Net report, told BIRN.

A **new regulation** obliging social media platforms to hand over users' personal information if the authorities ask for it was also adopted in April 2023, just before the elections; a move that was condemned by the opposition.

Erdogan proved many predictions wrong and won the elections in May 14, 2023, securing his presidential position again with 52.16 percent of the vote ahead of opposition challenger Kemal Kilicdaroglu at 47.84 percent. The ruling AKP and its allies also secured a comfortable majority in parliament, paving the way for more Islamist policies in the coming five years. Right after the election victory, Erdogan **accused** the entire opposition of being pro-LGBT and against family values.

The Turkish digital space is being shaped by an increasingly authoritarian government emboldened by its election triumphs and by identity politics that divide the already highly polarised country further. Many media organisations, social media companies and digital plat-

forms have been fined; courts have repeatedly ordered blocks on access to articles that criticise the government; vulnerable groups such as LGBT and refugee communities face widespread hate speech online and perpetrators face no consequences. President Erdogan has become the country's sole decision-maker since the new presidential system was **introduced** in 2018 and transparency and accountability no longer exist. Meanwhile, the government made no public statements about the biggest ever data leak in the country.

Access Blocks and Court-Ordered Content Removal

Following complaints about the slow official response to the earthquakes in February 2023, the government **blocked** most access to X (formerly Twitter) – a main source of communication for relatives of victims, survivors and aid campaigners. The government said it made the decision to counter disinformation and fake news using authority granted by **a law adopted in 2022**. This was another example of how the government has limited social media access during times of crisis at the expense of rights and freedoms. The government **previously restricted** social media access following disasters, terror attacks and protests.

The government also blocked access to several media outlets to force them to observe new rules and regulations. After the Turkish service of Germany's Deutsche Welle and the US Voice of America Turkish's website was blocked by a government agency in August 2023 after they failed to apply for a government licence, describing it a censorship, the US authorities **called** on Turkey to respect freedom of expression. The government ignored the call. Turkish courts have meanwhile **ordered the removal** of tens of thousands of online articles and blocked access to social media posts. The majority of this content was critical of government policies or of people linked to the government and **President Erdogan's family** or influential leaders of organised criminal groups.

A report claimed that Turkey is copying the Russian 'playbook', using the judiciary to silence critical journalism and freedom of expression. For example, as

of mid-September 2023, **Turkish courts ordered the removal** of 201 online content items following a request made by Yasam Ayavefe, a convicted fraudster and businessman. BIRN and its Greek partner Solomon published **an investigation** into Ayavefe, and how he acquired honorary Greek citizenship. Emboldened by the Turkish court's decision to order the takedown of the articles, Ayavefe's representative also called on BIRN in July 2022 to take down its articles about Ayavefe in line with the Turkish rulings, although one of the judgments clearly stated that domestic courts cannot remove content of "foreign origin". BIRN has refused to remove any content. BIRN and its Greek partner media outlet Solomon's websites came under **a major DDoS** after the publication of **an investigation** into Ayavefe's acquisition of a Greek passport.

Hate Speech Against LGBT Groups Intensifies

As a result of the Islamist policies of President Erdogan's government, hate speech against vulnerable people such as the LGBT community intensified in 2023. LGBT groups, Pride week events and supporters of LGBT rights are often targeted by Islamist and nationalist groups associated with President Erdogan and his allies. A concert by famous singer Gokce, a supporter of LGBT causes, was **cancelled by AKP mayor Mustafa Col** in the district of Sandikli in Afyon province after a smear campaign against Gokce on social media. Col stated that Gokce would not be able to "cross the borders of Sandikli" because she celebrated Pride week and supported LGBT rights. Many other festivals and concerts **were also cancelled in 2023** by governors and mayors from Erdogan's ruling AKP after being targeted online by conservative groups that deemed them immoral, pro-LGBT or against religious values.

Turkey's world- and European championship-winning women's volleyball team also suffered digital bullying and hatred. Ebrar Karakurt and Cuban-born Melissa Vargas, two star volleyball players who contributed greatly to the Turkish victories, came under attack from Islamist groups at home due to their sexual orientation. In an organised social media

smear campaign that involved senior members of Erdogan's ruling AKP, Islamists targeted the two players with homophobic comments and condemned the team for wearing uniforms deemed not acceptable under Islam. They also urged the team to expel certain players including Karakurt.

Fines and Imprisonment

Increasingly Islamist policies also resulted in fines being imposed on digital platforms. The state agency that monitors radio and TV, RTUK, fined digital streaming platforms including Netflix and Amazon Prime for **allegedly** promoting homosexuality and undermining Turkish 'moral values'. In August 2019, RTUK was given the authority to oversee digital streaming platforms with a regulation change that increased government control. Following this, several fines were imposed on digital platforms in parallel with the government's **increased pressure** upon and censorship of media outlets and the internet. RTUK also imposed fines on independent media platforms and journalists. The European Centre for Press and Media Freedoms, ECPMF and its partners **said** that RTUK has become a government tool to silence media and online critics of President Erdogan. RTUK banned independent TV channel TELE1 from broadcasting for seven days over remarks by veteran journalist Merdan Yanardag criticising the contact ban imposed upon Abdullah Ocalan, jailed leader of outlawed Kurdistan Workers' Party, PKK. Yanardag was sent to prison in June 2023 after nationalist and Islamist groups targeted him online, spreading a video from Yanardag's speeches in which his words were taken out of context via social media platforms. Rights groups **called** on Turkey's government to release Yanardag but were ignored. Yanardag was later released from prison in October 2023 but then **sentenced** to two years and six months in prison for making terrorist propaganda.

During the elections and the earthquake disaster, journalists, academics and ordinary members of the public who posted critical content on social media platforms were detained by police for spreading misinformation. Police said they identified 90 people who had spread fake news and disinformation

about the earthquake on social media, four of whom were detained. **One was Ozgun Emre Koc**, a political commentator with the Daktilo 1984 academic news website, detained in February 2023 over his critical posts on X about the government's response to the quake.

Turkish Citizens' Private Data 'Unprotected'

In June 2023, Turkey **recorded** its worst online data breach in its history. A website called sorgupaneli.org said it could provide details of Turkish citizens' private data, which had been stolen from the e-Devlet government services website. sorgupaneli.org even claimed it was able to provide President Erdogan's personal information. The hacked information was being offered for free by the website in return for a membership sign-up. The data includes ID numbers, phone numbers and information about people's family members. More sensitive information, including full addresses, real estate deeds and education details, was offered by sorgupaneli.org with a paid premium membership. When BIRN accessed the sorgupaneli.org website, it said that the personal data on offer included information about high-ranking state and government officials including Erdogan and Turkey's main opposition leader at the time, Kemal Kilicdaroglu.

The government offered little public response to the leak. However, criminal charges were **filed** against people who reported the incident or shared it on social media platforms, accusing them of "spreading misinformation". "Unfortunately, citizens' personal and private information of the citizens has now become public information and we still don't know how that happened," Veysel Ok, the president of Media and Law Studies Association, MLSA, the organisation that exposed the massive data breach, **told BIRN in an interview**. Ok said that the current laws and regulations are more than enough to prevent data breaches but "the government uses them to target journalists and not for their real purpose".

No Improvements Expected in Turkish Digital Space

Turkey's digital space was directly affected by political and societal devel-

opments in the country in 2023. Erdogan's government remained the worst abuser of rights and freedoms in the digital world. The majority of these abuses were rooted in years of movement from democracy towards an autocratic Islamist regime, and the creation of new laws and regulations that claim to target disinformation or to defend moral values but effectively increase government control over online media, social media companies and digital platforms. Following the government's line, Islamist and nationalist groups target government critics and LGBT groups with fake news, disinformation campaigns or hate speech and enjoy full impunity. Government agencies, courts and other state institutions fine online media and digital platforms, order content removal and pressurise or jail critics.

Artificial intelligence and digital surveillance were not major issues in Turkey in 2023, but several developments suggested that they could posed threats to digital rights and freedoms in future. In May 2023, four former executives from the Munich-based FinFisher company, which develops spyware, were **charged** with illegally selling software to Turkey's secret service so it could spy on the country's opposition. Turkey also **announced** in September 2022 that it is developing its own digital surveillance system that will obtain, process and store data from digital media to transmit it quickly to state authorities. The impact of AI and digital surveillance technologies on digital rights and personal data privacy could become a major trend in 2024 and beyond.

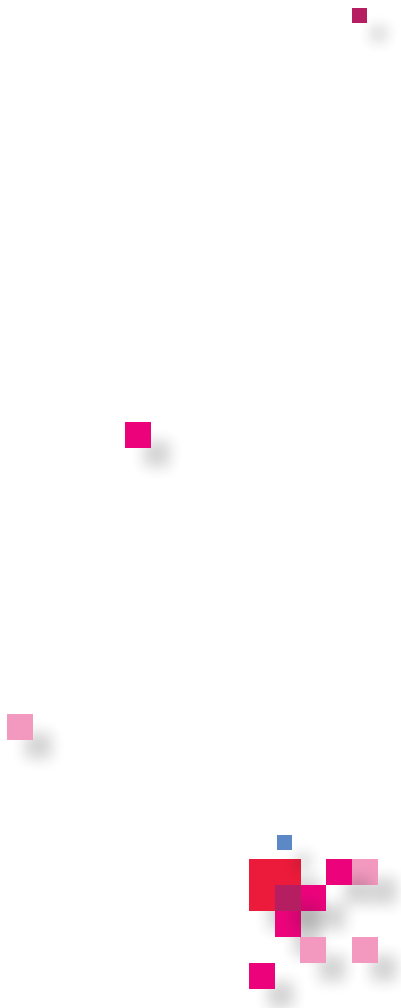
"Unfortunately, we can expect to see similar practices such as disinformation and the troll activities that we encountered during the general election held in May, in the local elections to be held in March 2024," said Ozturan of the European Centre for Press and Media Freedom. In the local elections in March 2024, Erdogan is expected to boost his illiberal and polarising agenda in a bid to secure another election victory and win Turkey's largest cities back from the opposition. This will affect the digital space in 2024, and is predicted to result in another increase in digital rights violations.

Recommendations

In 2023, digital rights violations in Turkey reached alarming heights as President Erdogan's government employed oppressive laws and regulations to suppress dissent and criticism, affecting media outlets, social platforms, journalists and artists. The prevalence of censorship, legal action and state interference raised serious concerns about the erosion of digital rights. Policymakers, legislators, and relevant authorities must take decisive action in three key areas to safeguard the digital rights of Turkish citizens: introducing legal reform to protect free speech, strengthening data protection and countering online hate speech.

- Rein in use of broadly interpreted laws to silence dissent. Turkey's legal framework contains vague and broadly interpreted regulations that have been consistently abused to silence criticism of the authorities and restrict freedom of expression. It is imperative to amend or repeal such laws to ensure they align with international human rights standards. Any restrictions imposed on digital rights must be clearly defined, proportionate and necessary for a legitimate purpose. Ensuring that the legal framework respects the principles of free speech and the right to dissent is crucial for safeguarding digital rights.
- Strengthen data protection and enact harsh penalties for violations. Turkey should prioritise comprehensive data protection legislation that empowers individuals to have greater control over the usage of their personal data. This legislation should not only limit the collection of personal information but also establish stringent requirements for obtaining consent. To enforce these protections, the government should create a dedicated regulatory agency with the authority to investigate and penalise data breaches. The penalties for violations should be substantial enough to serve as a strong deterrent against data privacy infringements. This will not only protect citizens' privacy but also foster trust in the digital environment.
- Counter online hate speech through positive messaging. Tackling the massive spread of online hate speech

is essential for creating a more inclusive and respectful digital space. Government officials should take a proactive stance in condemning hate speech and expressing their commitment to upholding the equal rights of all citizens, including vulnerable groups like the LGBT community. Civil society initiatives can also play a pivotal role in combating toxic narratives by promoting positive portrayals of marginalised communities. By spreading messages of tolerance, acceptance and diversity, society can collectively work to counteract the harmful effects of hate speech and promote a more inclusive online environment that respects the digital rights of all individuals.



RECOMMENDATIONS

Strengthen Cybersecurity to Protect Digital Rights

In the countries monitored by BIRN, there was a noticeable **surge** in cyberattacks, notably phishing and ransomware incidents, which posed a significant challenge to the protection of digital rights and the advancement of online freedoms. These concerns are firmly substantiated by the compelling findings within this annual report. To effectively address digital rights violations and foster online freedoms, tangible, targeted actions are imperative to bolster cybersecurity and shield both citizens and institutions from the escalating cyber threats targeting all countries in the region. Stakeholders must also be aware of and prepared for new digital threats emerging in parallel with technological advancements, the malicious use of AI tools in particular.

Governments and Policymakers

It is crucial that governments proactively enforce stringent cybersecurity regulations, promote cross-border collaboration and allocate resources for educational and public awareness campaigns. Governments should also increase investment in infrastructure that will protect citizens' private data and online government services. By doing so, they can also help to defend digital rights and online freedoms. Governments should do this in cooperation with civil society groups, experts, the media and the private sector.

Private Sector and Critical Infrastructure Owners

Businesses and other entities responsible for critical infrastructure must make substantial investments in robust cybersecurity measures. The private sector must acknowledge the importance of private data protection and citizens' digital rights

as well as profit. It should also actively engage in sharing threat intelligence and prioritise the protection of customer data while adhering rigorously to data protection regulations.

Civil Society Organisations

Civil society groups need to intensify their efforts in advocating for digital rights and freedoms. Collaborative partnerships with relevant stakeholders are essential, and they should redouble their endeavours to raise public awareness about the critical importance of cybersecurity.

Media and Journalists

Media outlets and journalists can play a pivotal role by reporting vigilantly on cyber threats. They should also take on the responsibility of educating the public about cybersecurity, collaborating closely with experts in the field to empower individuals with the knowledge and skills required for online safety.

International Organisations

Drawing inspiration from the recent **Tirana Declaration**, made after the EU-Western Balkans Summit in December 2022, the international community should continue to assist by offering technical assistance and fostering capacity-building initiatives in the region.

Citizens

Digital security starts from the smallest segment of society: individuals. In addition to the effort of other stakeholders, citizens must start to think about their own digital security following the instructions and recommendations of governments, tech companies, media and experts in order to be aware of the growing digital threats.

Foster Media Freedom and Plurality for a More Inclusive Digital Space

Challenges to media freedom and pluralism are a growing concern in the countries monitored by BIRN. In Hungary, the erosion of media pluralism and freedom of expression is evident, with a "politically controlled media regulatory authority and

distortionary state intervention" in the market, as Freedom House **quoted** Dunja Mijatovic, the Council of Europe's Commissioner for Human Rights, as saying. According to Reporters Without Borders' latest **Press Freedom Index**, the media landscape in the Western Balkans continues to present challenges. In **2023**, countries like Montenegro and North Macedonia made notable progress, albeit with room for further improvement. However, Turkey and Serbia have experienced significant setbacks, with their media environments being increasingly constrained by governmental actions that curtail journalistic independence. This persistent issue highlights the urgent need for comprehensive reforms to protect citizens' digital rights and promote online inclusion, safety and accountability.

Governments and Policymakers

To combat misinformation and promote a diverse media landscape, governments should invest in public awareness campaigns that educate the public about media literacy and critical thinking. Additionally, they should demand the transparency in media ownership and financing, support fact-checking initiatives and platforms, and establish regulatory frameworks that penalise the spread of false information. However, governments should not use new legislation to target freedom of speech and journalists for their own benefit,as has been seen in Turkey and Hungary, countries whose governments have adopted increasingly autocratic policies. Also, the support for independent, fact-based reporting by providing resources and protection for journalists who uncover the truth is rarely seen across the countries in this report. Government should also closely work with media experts and rights groups to protect the rights of journalists and freedom of speech when they prepare their agenda to counter misinformation.

Media Outlets and Journalists

Combatting digital rights violations, measures against misinformation cannot be solely left to governments. Media outlets and journalists should be at the forefront of combating digital rights violations. Media outlets should prioritise providing the capacity building and constant learning for their journalists in

unbiased reporting and fact-checking. They should also start collaborating with international fact-checking organisations to verify information. The media outlets should engage with the public more often, through responsible reporting and providing space and way for open dialogue. The diversification of content to offer a wider range of perspectives remains unfulfilled duty of the majority of the media outlets in the countries this report covers.

Civil Society Organisations

CSOs need to intensify their efforts to counter misinformation and one-sided narratives by using already used methods, but also exploring new and innovative approaches. Closer collaboration between CSOs and tech companies and academia is much needed in order to develop tools for detecting false information. CSOs should use all the public platforms they have access to, to advocate for policies that protect digital rights, including freedom of information. In their projects and activities CSOs should increase promotion and learning media literacy through workshops and local campaigns, and also encourage watchdog journalism.

Educational Institutions

Educational institutions on all levels should revamp their curricula to include digital literacy and media literacy as essential subjects. This should be done in tandem with encouraging critical thinking and media analysis. Schools and other educational institutions should equip students with the skills to identify and critically evaluate information they are exposed to. At higher level of education, institutions should support research on media freedom, disinformation, and the impact of one-sided media narratives.

The Public

The public can play an active role in fighting digital rights violations, first and foremost, citizens should aspire not to fall victim to spreading disinformation online, by cross-referencing the information from diverse sources. This could result in more responsible sharing of information on social media and encourage reporting false information and one-sided narratives when encountered.

CONCLUSION

During the reporting period for BIRN's Digital Rights Violations Annual Report 2022-2023, as explained in detail in this report, digital rights violations increased significantly in parallel with the often-turbulent political situations in the countries monitored and with wider geopolitical developments. This turbulence resulted in online conflicts in which hate speech, discriminatory rhetoric and disinformation campaigns flourished. Autocratic governments often exploited or stirred up these conflicts for their own purposes.

Legislation to counter such digital rights violations remains weak in the countries monitored, but almost all governments are preparing new laws. However, this planned legislation has alarmed rights groups and journalists, as governments in Turkey and Hungary have already used existing legislation to target dissent online.

While freedom of speech came under attack online, the infrastructure of state and government agencies in almost all countries surveyed remained exposed to digital threats such as cyberattacks and leaks of citizens' private data. Meanwhile, members of the public were also targeted by online fraudsters using phishing techniques. The perpetrators behind these leaks and scams usually remained unidentified and went unpunished due to governments' and security agencies' inability to counter such threats. Worryingly, governments in some of the countries monitored by BIRN now plan to use new technologies, including artificial intelligence and digital surveillance tools, to establish **digital autocracies**.

Political tensions are to persist in the countries covered by BIRN's digital rights programme because several of them, including Bosnia and Herzegovi-

na, Hungary, Serbia and Turkey, will hold elections in the final months of 2023 or in 2024. This is likely to create fertile ground for digital rights violations, as has previously been observed in highly-polarised societies ahead of critical elections.

Domestic crises in countries like Bosnia and Montenegro and in the north of Kosovo are also expected to continue as domestic and international actors' attempts to intervene have failed. Crises outside the region, including Russia's invasion of Ukraine and the conflict between Hamas and Israel in Gaza, will also contribute to shaping the overall digital environment. Taken together, these issues are expected to continue generating fake news, hate speech and disinformation campaigns on social media platforms.

Journalists, the LGBT community, women and ethnic minorities are likely to remain targets online due to the lack of legislation to protect them or the malicious use of existing legislation. Governments do not have enough capacity and/or willingness to counter such attacks on journalists and vulnerable groups, or to stop violent incidents being livestreamed on social media, as happened in Bosnia. Neither do they appear able to prevent major data leaks of citizens' private information or to curb online fraudsters, as the cybersecurity capacities of state and government agencies appear to be weak. Governments seem to need outside help to educate their staff and improve their technological infrastructure.

Finally, the malicious use of AI and digital surveillance should ring alarm bells. The countries surveyed by BIRN are following global trends in terms of AI and digital surveillance but are lagging because of their weaker economies and lower levels of technological advancement. This allows autocratic governments to manipulate the digital space and abuse digital rights for their own benefit, using security reasons as an excuse. In the next reporting period and in the years ahead, violations arising from the malicious use of AI and digital surveillance are likely to dominate the debate on digital rights and security.

BIRN
BALKAN INVESTIGATIVE
REPORTING NETWORK

DECEMBER 2023


BIRN
BALKAN INVESTIGATIVE
REPORTING NETWORK
DECEMBER 2023