THE GREENS/EFA
in the European Parliament

THE DIGITAL ENIGMA:

AN INVESTIGATION INTO ILLIBERAL ONLINE PRACTICES IN THE BALKANS

Final Report
January 2024

IMPRINT

MEP Gwendoline Delbos-Corfield,
the Greens/EFA Group in the European Parliament
Rue Wiertz 60, 1047 Brussels

Contact:

Mila Bajić, mila@sharedefense.org
Jasmine Rowlands,
Office of MEP Gwendoline Delbos-Corfield, Brussels
jasmine.rowlands@europarl.europa.eu
Place of publication: Brussels, Belgium
Release date: January 2024
Proofreading: Chris Meikle
Cover photo: Sveta Zi/Shutterstock
Layout: Fita Hausdorf / kami studio

The opinions expressed in this report are
those of the authors and do not necessarily
reflect the views of the
Greens/EFA group in the European Parliament.

THEGREENS/EFA
in the European Parliament

AUTHORS

MILA BAJIĆ is the head of research at the SHARE Foundation. Her areas of interest and expertise include working on issues of online information disorders, hate speech, gender based online violence and online election manipulation tactics. She is also one of the Open Internet Leaders of the Open Internet for Democracy Initiative for 2023.

ANA MARTINOVIĆ is a lawyer working with the SHARE Foundation. She has over ten years of experience in human rights litigation, litigating cases concerning housing, discrimination, freedom of movement and minority rights. Before joining the SHARE Foundation, she worked at the European Court of Human Rights.

BOJAN STOJKOVSKI is a freelance journalist based in the Western Balkans, where he has been covering tech, innovation, business and digital rights for more than a decade. His work has been featured in global media outlets such as Foreign Policy, WSJ, ZDNet, The Recursive and Balkan Insight.

DANAI MARAGOUDAKI is a Greek journalist based in Athens. She works for independent media outlet Solomon and is a member of investigative team The Manifold. She has collaborated with Inside Story and vice.gr, as well as working for finance news site capital.gr. Her reporting focuses on transparency, finance, technology and digital threats.

TABLE OF CONTENS

EXECUTIVE SUMMARY

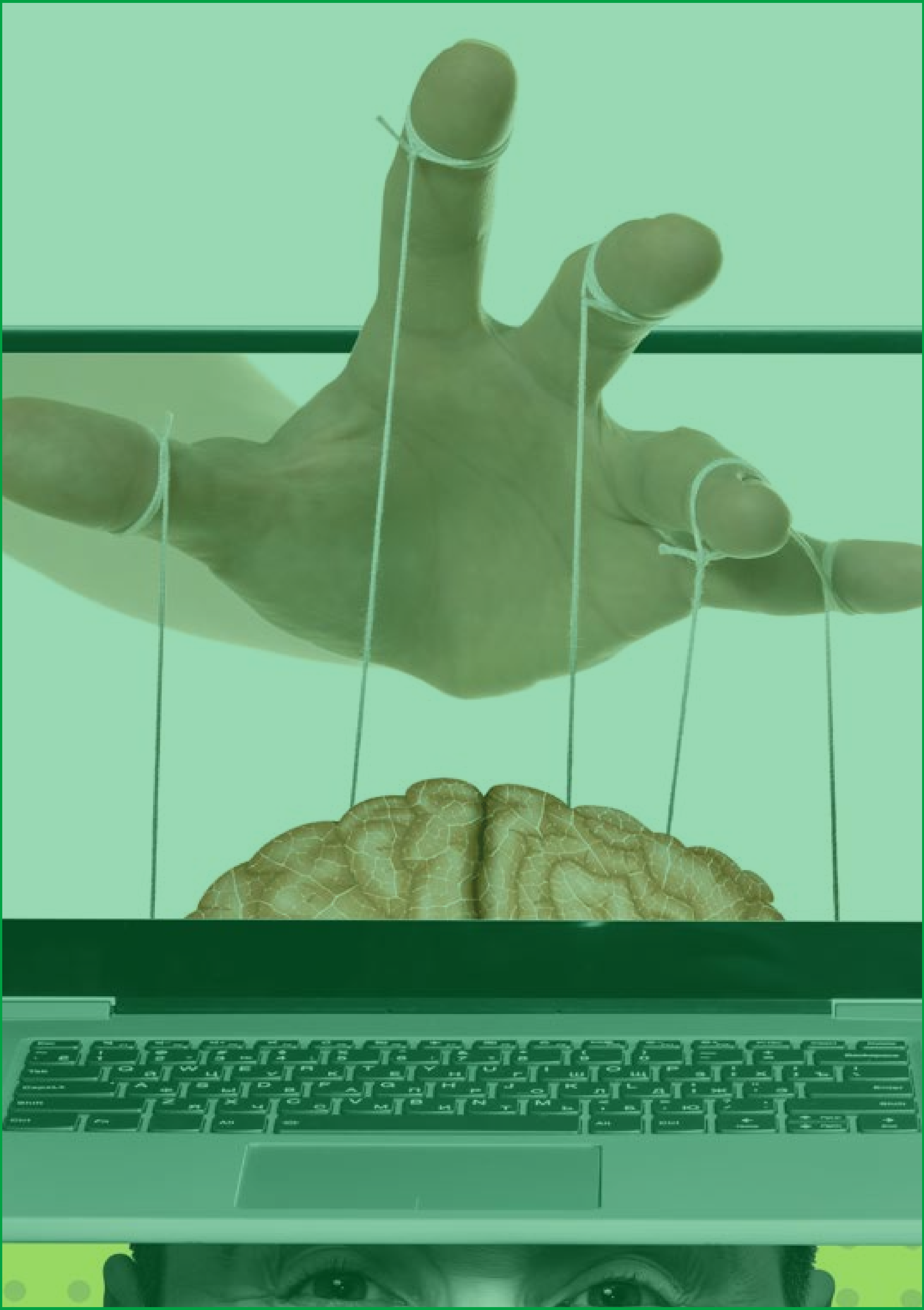
This report investigates the ways in which governments aim to co-opt new and emerging digital technologies to forward their agendas, and what impact that might have on citizens' civil liberties. The ease with which governments can exploit such powerful systems is a viable cause for concern. When digital technologies are integrated into government operations, there is a risk of overreach, discrimination and the erosion of civil liberties. Without robust regulations and oversight, illiberal digital practices can ensue, some of which we define as monitoring and tracking individuals' online activities, targeting specific populations based on race, religion or political affiliations, and suppressing dissenting voices.

> When digital technologies are integrated into government operations, there is a risk of overreach, discrimination and the erosion of civil liberties

Through the report, four main areas stood out and were identified as most relevant for this analysis. The areas in question are observing the governments' use of digital technologies for voter participation and election campaigning, (dis)respecting freedom of expression, surveilling citizens and populations on the move, and protecting and maintaining institutional human rights safeguards. In all four areas, the conclusion is that digital practices are being misused in certain areas, such as for stifling free speech and retaliation against perceived opponents (mostly independent investigative journalists, civil society and activists). It is understood that these types of limitations tend to hinder the free flow of information, impede journalistic integrity and undermine individuals' ability to express themselves freely in the digital realm.

Additionally, the report shows a clear discrepancy between the level of digital literacy and the overall use of digital technologies, with internet penetration levels and digital device usage being high and increasing, while elementary use of these devices and other digital services is still low. This indicates the existence of a high digital divide in these communities which might prevent citizens from recognizing their (digital) rights at all times or understanding what might constitute a violation of the same. It is also crucial to highlight the importance of governments integrating new technologies into citizen participation in a clear and understandable manner, which does not seem to be the current case in the given countries.

All three countries analysed in the report (Greece, North Macedonia and Serbia) show varying degrees of illiberal practices in use, as well as inclinations towards illiberal tendencies facilitated by the use of technology. Although taking into account differing historical, socio-political and economic factors, as well as other developments in the countries, the precise degree is hard to quantify. However, it could be argued that the state-sponsored use of technology, as well as citizens' digital habits, do give concern to the rise of digital illiberalism in parts of the Western Balkans region. This research demonstrates that a more open approach to individuals' online freedoms and rights is needed, as well as a more transparent and direct approach to digital rights regulation from governments.



Manipulation of a person with the help of media. Art collage. Photo: Sveta Zi/Shutterstock

ABBREVIATIONS

ADAE - Authority for Communication Security and Privacy
BIA - Serbian Security Information Agency
BIRN - Balkan Investigative Reporting Network
DIAS – Greek motorcycle police unit
DPA – Data Protection Authority/ Agency
EAD - National Transparency Authority
EYP - Greek National Intelligence Service
FRONTEX - European Border and Coast Guard Agency
GDPR - General Data Protection Regulation
IOM – International Organization for Migration
ISP - internet service provider
ITU - International Telecommunication Union
KRIK - Crime and Corruption Reporting Network
LEC - Law of Electronic Communications
Mbps - megabits per second
MUP - Ministry of Interior
NCSI - National Cyber Security Index
NIS - Greek National Intelligence Service
NUNS - Independent Association of Journalists
OPKE - Crime Prevention and Suppression Team
SLAPP - Strategic Litigation Against Public Participation
SNS - Serbian Progressive Party
UNHCR – United Nations High Commissioner for Refugees
UNS - Association of Journalists
VBA - Military Security Agency

ADAE - Authority for Communication Security and Privacy
BIA - Serbian Security Information Agency
BIRN - Balkan Investigative Reporting Network
DIAS – Greek motorcycle police unit
DPA – Data Protection Authority/ Agency
VBA - Military Security Agency

BACKGROUND

In the last decade, we have witnessed first-hand the rise in democratic backsliding and the sophistication of illiberal tendencies across the world. It is notable that these practices often go hand in hand. This is particularly the case in the world of digital innovation and technologies, a relatively young frontier, which has captivated the majority of the world's governments in their quest to solidify power. According to the Economist Group's 2022 Democracy Index, the global state of democracy has been either stagnating or deteriorating consistently in the last couple of years, with the most notable drop recorded following the pandemic, which started in 2020. The immersive shift to the digital space following the rapid spread of the coronavirus has left lasting changes in the ways in which governments interact with their constituents, both positively and negatively.

The protection of individual rights is essential to a liberal democracy

The core principles of liberal democracy include individual autonomy, the rule of law, protection of civil liberties, political pluralism and the separation of powers. These principles form the foundation of democratic governments that allow citizens to participate in the decision-making process and hold those in power accountable. The protection of individual rights is essential to a liberal democracy, and governments must ensure that these rights are safeguarded through strong institutions, such as independent judiciaries and free media. Additionally, liberal democracies value the principles of free and fair elections, where every citizen has the opportunity to vote and have their voice heard.

The rule of law provides a framework for democratic government, where laws apply equally to all citizens and officials are held accountable to the same legal standards as everyone else. Overall, liberal democracy is centred on the ideals of equality, freedom and justice, striving towards a society that values individual and collective rights, the rule of law, and democratic participation.

Overall, liberal democracy is centred on the ideals of equality, freedom and justice

Illiberal democracy is a term used to describe a political system that operates as a democracy, but does not adhere to the norms and values of liberal democracy. Unlike liberal democracies, illiberal democracies feature a strong central government that is often authoritarian and populist in nature, with limited respect for individual rights and the rule of law. These governments often use the democratic process to gain and maintain power, but once in power, they restrict the freedom of the press and the opposition, limit free and fair elections, and manipulate the judiciary to their benefit. Examples of illiberal democracies can be found in countries such as Venezuela, Turkey and Hungary. While not necessarily illegitimate, illiberal democracies do not uphold the principles of liberal democracy and pose a threat to the stability and prosperity of both their citizens and the region in which they operate.

Illegitimate, illiberal democracies do not uphold the principles of liberal democracy and pose a threat to the stability and prosperity

Therefore, the argument can be made that the countries of the Southeast European region share some specific practices when it comes to illiberal tendencies, and the ways in which they try to exert power and control their respective societies. In this report, the aim is to analyse how the proliferation of digital technologies and the undeniable turn towards state techno-solutionism has impacted the illiberalisation of societies in Greece, North Macedonia and Serbia. This research therefore attempts to present a baseline investigation into the ways in which digital illiberal practices are being deployed (if they are), and how they are affecting governance practices, as well as the general public. It also focuses on government-sponsored actions and aims to analyse how these practices impact human rights such as freedom of expression, freedom of assembly, rights to privacy, and the right to an effective remedy and to a fair trial.

PURPOSE AND METHODOLOGY

This study's main objective is to look for connections between the use of digital technologies and illiberal tendencies by governments in Greece, North Macedonia and Serbia. This research also looks into how these technologies influence the rise of illiberal tendencies in society, as well as determining whether technology is helping or hindering the spread of illiberal sentiments in these contexts.

To this end, four main areas were chosen for analysis:

1 Elections and political participation:
looking at the ways in which governments utilise new technologies to gather support while election campaigning, as well as how well-equipped the public sector is with digital services.

2 Freedom of expression:
looking at the ways in which civil society organisations, journalists and citizens are treated in online spaces, with a special emphasis on censorship and retaliation from governments against individuals for posting online.

3 Internal policing and external border security:
assessing how the government uses technology to police citizens internally, as well as how (and if) it monitors its borders, and what impact this has on populations on the move that are trying to enter or pass through the country.

4 Institutional human rights safeguards:
analysing how the state responds to incidents that include privacy violations, such as massive data breaches, personal data disclosure and overall independence of the judiciary in such cases.

To facilitate a clear and concise comparison between the three countries, we organised and compiled all relevant data into a comprehensive report. This consolidation enabled us to present the information in a structured manner, making it easier to identify and comprehend similarities, differences and trends across the four areas of analysis in this report. By synthesising the data into a single report, we aim to provide a coherent overview that effectively highlights the strengths and weaknesses of each country in the context of the spread of illiberal sentiments and digital authoritarianism.

Our decision to prioritise desk research as the primary method of data collection was motivated by the need for a comprehensive and systematic analysis of the selected countries. This approach allowed us to gather information from a wide array of reliable sources, including academic publications, government reports and reputable databases. By drawing from such diverse sources, we ensured the accuracy and depth of our findings, covering various aspects such as socio-economic indicators, political landscapes and cultural dimensions.

We believe that the chosen methodology offers several advantages. Firstly, it ensures the inclusion of diverse and reliable sources, thereby enhancing the credibility of our analysis. Secondly, the consolidation of data simplifies the process of comparing and contrasting the analysed countries, enabling readers to readily identify patterns, trends and key findings. Lastly, this approach promotes efficiency in accessing and interpreting the data, allowing stakeholders to extract valuable insights promptly. Also, taking into account that the scope of the research was only three countries, we found it would be much more immersive to organise the data in such a way that would clearly present a holistic understanding of the similarities and differences among the countries, rather than presenting country by country–type reports.

It should be noted that this report is a stepping stone in the investigation of such phenomena in the region and should be viewed as a starting point for future research on the topic. That being said, the three countries selected for the research not only vary in their different approaches to governingand internal policies, but also in the broader geopolitical context, such as their relation to the European Union.

SCOPE OF THE RESEARCH

Three countries were selected for this report, all belonging to the Southeast European region, in different stages of membership or accession to the European Union. As was confirmed by the research, the selected countries also have different internal characteristics that stand out, but on the whole, share similar struggles in their efforts to maintain civil liberties and rights at a high level. All three countries were considered flawed democracies in the 2022 EIU Democracy Index; however, it should be noted that digital competency is not a big area of interest in this index. Even though there are a number of indexes that focus on counties' digital developments, many of them are more concerned with policy developments and formal governmental strategies. For transparency and comprehension, we have also included the information listed in these indexes for reference, but it should be taken into consideration that these indexes lack nuance and are more focused on the theoretical accomplishments, rather than the practical implications, of the policies and laws.

COUNTRY CONTEXTS

Greece, an EU Member State since 1981, is still a country with strong democratic principles when it comes to political pluralism and freedom of speech. However, the country's treatment of populations on the move, such as migrants, refugees and asylum seekers, which has garnered a lot of negative attention in the last couple of years, continues to decline.

According to a 2022 survey conducted by the Hellenic Statistical Authority, 85.5% of households in Greece have access to the internet. Compared to 2012, a 59.5% increase has been recorded in household internet access. At the same time, however, Greece, along with Croatia (86%) and Bulgaria (87%), had the lowest rates of household internet access among the EU Member States. According to Ookla's Speedtest Global Index from April 2023, median download speeds in Greece were 67.80 megabits per second (Mbps) for mobile connection and 44.25 Mbps for fixed broadband connection. Greece ranked in 7th place in the National Cyber Security Index (NCSI), with a perfect score for cybersecurity policy development and the protection of essential digital services, among other aspects.

GREECE RANKED IN 7TH PLACE IN THE NATIONAL CYBER SECURITY INDEX (NCSI)

GREECE

North Macedonia has seen its democracy scores increase in recent years, albeit the overall situation remains a concern in terms of freedom of expression and the electoral process. The country has been part of the EU accession process since 2005, but a number of tumultuous turns over the years have complicated the situation. According to data from the country's State Statistical Office, in the first quarter of 2022, 86.6% of households in North Macedonia had access to the internet at home. In the first quarter of 2022, 88.3% of the total population aged 15–74 used the internet, while 73.9% used the internet several times per day. There have been no instances of internet shutdowns in the country, or broader attempts of internet capture or censorship. According to Ookla's Speedtest Global Index from May 2023, median download speeds in North Macedonia were 77.06 Mbps for mobile connection and 38.27 Mbps for fixed broadband connection. In the NCSI, the country is in 59th place globally when it comes to the management and prevention of cyber incidents, mostly because of its lack of a government state cyber security policy department, which would be responsible for policy development and essential service protections in the country. The country has yet to introduce regulation that would cover the area of cybersecurity.

IN THE NCSI, THE COUNTRY IS IN 59TH PLACE GLOBALLY WHEN IT COMES TO THE MANAGEMENT AND PREVENTION OF CYBER INCIDENTS

NORTH MACEDONIA

THE COUNTRY RANKED 21ST IN THE NCSI, WITH HIGH SCORES FOR PERSONAL DATA PROTECTION AND COMBATING CYBERCRIME

SERBIA

Serbia, an EU candidate state since 2012, has been steadily declining on most of the world's democracy and freedom lists, due to growing nationalist sentiments and state capture by the ruling party. However, when it comes to digital infrastructure, Serbia's internet penetration rate has steadily increased in recent years. According to data from the Statistical Office of Serbia for 2022, 83.2% of Serbian households had an internet connection, with 91% using fixed-line broadband service and around 75% using mobile broadband. More than 80% of Serbians have access to the internet according to statistical data from the International Telecommunication Union (ITU). The government does not disrupt or restrict access to the internet in the country, and it has no past record of imposing internet shutdowns amid elections or other national events. According to Ookla's Speedtest Global Index from May 2023, median download speeds in Serbia were 47.37 Mbps for mobile connection and 66.24 Mbps for fixed broadband connection. The country ranked 21st in the NCSI, with high scores for personal data protection and combating cybercrime, because of the existence of the Law on Personal Data Protection, which in many ways can be viewed as a carbon copy of the EU's General Data Protection Regulation (GDPR).

Woman watching fake news. Photo: Roman Samborskyii/Shutterstock

ELECTIONS AND POLITICAL PARTICIPATION

Online mobilisation tactics employed by politicians and other stakeholders, as well as engaging in online voter manipulation, fall under the scope of the first category analysed in this report – elections and political participation. These tactics manifest through garnering support online, sometimes through spreading counter narratives, disinformation, fake news and conspiracy theories, as well as non-transparent advertising on social media and pressuring voters through dubious means, including the misuse of personal data, threats and surveillance.

Online public participation promotes transparency and accountability in governance. By providing accessible platforms via which citizens can express their views, monitor government actions and provide feedback, the public's ability to hold decision-makers accountable is enhanced. E-participation tools, such as online consultations and participatory budgeting platforms, allow citizens to directly influence policy formulation and resource allocation. This increased transparency helps to mitigate the risks of corruption, favouritism and arbitrary decision-making. Actively involving citizens in decision-making processes encourages them to take an active role in shaping their communities and societies. Engaging citizens in meaningful participation online can strengthen their trust in democratic institutions, increase their sense of ownership and empower them to address social challenges collectively.

ONLINE MOBILISATION

The official webpage of the government of North Macedonia features a section called 'Open Government', which contains an additional segment titled 'Open government partnership'. According to the explanation on the website, the platform represents a central point for consultation, monitoring, networking and the notification of all stakeholders and interested parties in the process, and is intended for the electronic information of citizens, non-governmental organisations, business entities and state institutions. Additionally, the platform is meant for their inclusion in the implementation activities of the Partnership for Open Government in the country. The platform also has a section for proposals that have been submitted from citizens and civil society organisations.

In Serbia, these systems are not widespread or advertised, and even though they do exist, it can oftentimes be more complicated to finish things online than offline. While there is no online system that allows for the direct participation of citizens in the legislative process, citizens do have some other options. The website of the Serbian National Assembly includes a section that allows citizens to directly pose a question, either to the president of the National Assembly or to members of parliament. Questions are uploaded through the chat box system, where the citizen leaves their full name and email address. In addition, there is the possibility of contacting presidents of different parliamentary groups via a standardised form on various issues, such as petitions, proposals and initiatives. There is, however, no available data as to how often these mechanisms are used and how responsive this service is within the National Assembly.

According to Greek law, the legislative procedure foresees that any draft bill submitted by the government has to undergo a two-week period of public consultation prior to its introduction into parliament. The public consultation process takes place via the government portal. Once the consultation period is complete, a report is drafted with the results of the public consultation, which is subsequently published along with the draft bill on the parliament's website. As for the citizens' usage of the public consultation platform, according to statistics available on it, for 1,104 draft bills, 340,014 comments were submitted. As for those that use the platform, both individuals and professional associations use the portal. However, participation of the broader public is still very low. This could be due to the very limited period of two weeks which is allowed for consultation after the announcement of a bill. This leaves many associations and citizens' rights groups unprepared. Furthermore, instead of allocating an actual two-week consultation period, the government body often allows only a few days to elaborate. A recent example was the consultation for a huge bill from the Ministry of the Environment, which was given only three days. Other than this, the platform seems to operate without any major issues.

Man typing breaking fake news under boss control. Photo: Anton Vierietin/Shutterstock

GATHERING SUPPORT

Social media is a very important part of the general interaction that politicians have with constituents in Serbia. The president is predominantly active on Instagram, where he shares candid photos of himself and other state officials, either in official or private interactions. When, in 2021, a number of media outlets were marked as government affiliates, the president urged Twitter to ban his account, emulating Donald Trump's ban on the platform. After a list of 14,000 bot accounts for the Serbian Progressive Party (SNS) was leaked online in the beginning of July 2023, President Vučić posted on his Instagram declaring himself a bot as well. Most other politicians instead opt to use Twitter as their main outreach platform, where they regularly engage with individuals and, sometimes, bots.

Most politicians in North Macedonia use either Facebook or Twitter as their preferred channel of communication with their constituents

Inauthentic social media accounts are not a rare occurrence on Serbian political social media. In February 2023, Meta released a security report highlighting Serbia as a particularly concerning case. According to the report, a vast network of accounts was found to be operating within the country whose primary purpose was to boost the popularity of President Vučić, as well as the leading Serbian Progressive Party. One of the biggest distinguishing features of the network was that the accounts made it seem as though the support was organic. Only a couple of years prior, the Stanford Internet Observatory released an investigative report in which it uncovered another vast network of bot accounts posting praise of the president and the ruling party, and attacking opposition politicians and civil society members. The report led to a Twitter purge in which 8,500 accounts were removed from the platform.

Most politicians in North Macedonia use either Facebook or Twitter as their preferred channel of communication with their constituents. In some cases, the politicians have been using their own profiles and creating organic content by themselves, while in other cases, the content has been curated. This has been noticed on Twitter, in particular, where there has been use of bots to boost the popularity of certain politicians or political parties. In some cases bots are used with the sole purpose of boosting popularity – but there are also so-called covert bots (with real people behind these profiles) that are used to drive certain discussions or to instigate unrest and target those users that are criticising the politicians or political party that they represent.

A considerable number of Greek politicians interact with constituents via their official social media accounts (Facebook, Twitter and, more recently, TikTok). The content is usually organic, although during pre-election periods, it may be curated. It has been reported that certain high profile politicians make use of bots to boost their popularity via social media (for example, the Twitter followers of New Democracy's Vice President and other prominent politicians have been reported to be more than 67% fake). It is also common knowledge that both New Democracy and SYRIZA have recruited "armies" of trolls and fake accounts to further disseminate their messages or attack the opposition.

NON-TRANSPARENT ADVERTISING

Mirroring the rest of the region, Serbia is largely unregulated when it comes to transparent and fair political advertising. In 2020, Meta, Facebook's parent company, expanded its political advertising policies to oblige sponsored election-related posts on the platform to be more transparently marked. The move included a number of countries outside of the EU, including Montenegro, North Macedonia and Serbia. This decision allowed greater transparency for researchers who follow election campaigns, and also for users who want to know more about the ways in which the people posting these ads choose who to target, as well as how the ads are financed. Analysis of the 2022 elections in Serbia revealed that there is still so much more to be done to increase transparency in the field of online campaigning. According to SHARE Foundation's analysis of advertising practices surrounding the 2022 parliamentary and presidential elections, it was clear that the government is very keen to occupy the online space and curate its presence on each platform specifically. On Facebook, significant funds are dedicated to advertising and single ads are targeted to specific demographics. The majority of these funds tend to go unregistered with the Agency for Corruption Prevention, which is to say that political parties neglect to disclose the exact amount of finances they allocate for the purposes of online campaigning. Another important thing to note is that online advertisements in themselves are not subject to the Law on the Financing of Political Activities; that is, they are not explicitly prohibited during the period of information embargo that is mandated to take place in the two days before the election.

Serbia is largely unregulated when it comes to transparent and fair political advertising

In North Macedonia, the majority of political ads have been clearly marked and are regularly featured in different reports on how politicians are spending their budgets when it comes to political advertising. Many of these reports have also highlighted the questionable amount of funds being used by politicians and have called this practice into question, as well as the reasoning behind it and how these payments were being made. One significant difference between Serbia and North Macedonia in relation to Greece is that the GDPR binds big tech companies operating in the EU jurisdiction to abide by transparency regulations and submit regular and comprehensive transparency reports. This is not the case in the rest of Europe, and therefore it is impossible to get advertising data from Google for Serbia and North Macedonia. There are similar rules for social networks as well, with Twitter and Meta delivering more detailed information on political activity for the EU bloc and overlooking other parts of Europe. Although still not at the same level as the big global markets such as the US, UK, Australia and the EU, introducing the marking of political ads in North Macedonia represents a step in the right direction when it comes to political and electoral transparency online.

In Greece, there is no specific regulation on social media advertising. Ads are not clearly marked unless they are sponsored (paid) posts. No reported instances exist to this day of political actors employing non-transparent methods to promote themselves online. According to reports based on Google's dedicated page on political advertising, between 20 March 2019 and 12 May 2020, New Democracy had spent €648,950 on political advertising via Google. The aforementioned amount is striking given the party's dire financial state and massive (largely unserviceable) bank loans amounting to over €308 million. In the last elections (May–June 2023), during the pre-election period (1 April to 20 May 2023), the cost for New Democracy ads on Google was almost €200,000, and for SYRIZA about €135,000. On Facebook, New Democracy spent about €160,000 on advertising related to the party and Kyriakos Mitsotakis, and Syriza spent about €85,000 on advertising related to the party and Alexis Tsipras.

PRESSURING VOTERS TROUGH DUBIOS MEANS

In Serbia, there have been uncorroborated reports and images surfacing of individuals taking photos of their ID cards in the voting booth to prove their loyalty to the ruling Serbian Progressive Party. However, these instances seem to be voluntary actions by individuals who willingly support the party, rather than evidence of coercion or pressure on voters.

In North Macedonia, past practices have involved authorities pressuring public administration employees to submit a list of contacts that were certain to vote for a specific political party. Failure to comply with such requests could result in threats of termination or making their work environment more challenging. This activity indicates a coercive approach to ensuring political support, potentially undermining freedom of choice for voters.

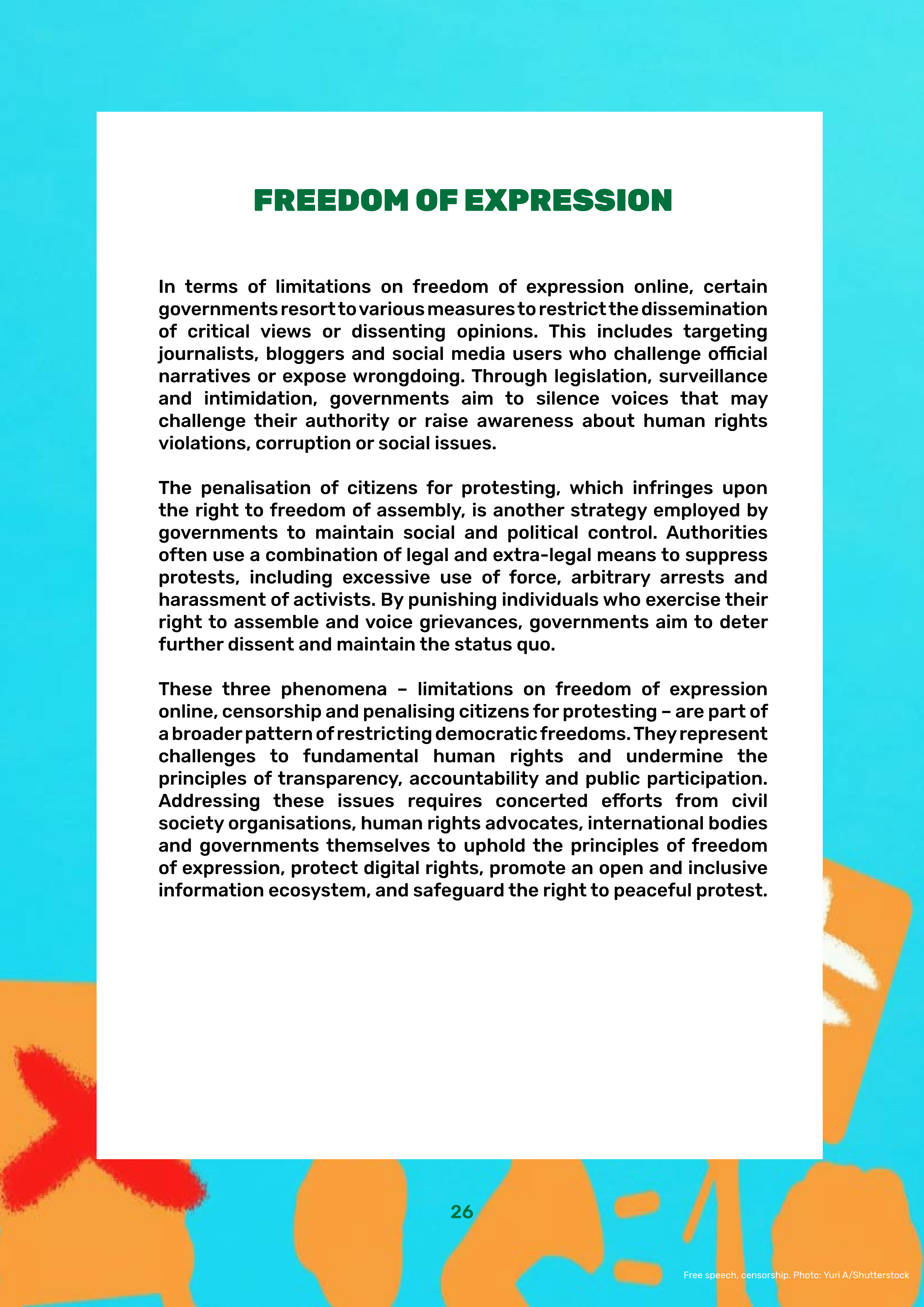
In Greece, there is no current evidence suggesting direct coercion of voters. However, it is important to consider other factors that may indirectly affect the electoral process. The recent spyware scandal involving the National Security Service and the mishandling of vast amounts of personal data by the Ministry of Education raise concerns about privacy and the potential manipulation of information. Additionally, the existence of secret contracts between the government and tech company Palantir Technologies, specialising in security and surveillance, raises questions about the possible use of advanced technologies in political processes.

FREEDOM OF EXPRESSION

In terms of limitations on freedom of expression online, certain governments resort to various measures to restrict the dissemination of critical views or dissenting opinions. This includes targeting journalists, bloggers and social media users who challenge official narratives or expose wrongdoing. Through legislation, surveillance and intimidation, governments aim to silence voices that may challenge their authority or raise awareness about human rights violations, corruption or social issues.

The penalisation of citizens for protesting, which infringes upon the right to freedom of assembly, is another strategy employed by governments to maintain social and political control. Authorities often use a combination of legal and extra-legal means to suppress protests, including excessive use of force, arbitrary arrests and harassment of activists. By punishing individuals who exercise their right to assemble and voice grievances, governments aim to deter further dissent and maintain the status quo.

These three phenomena – limitations on freedom of expression online, censorship and penalising citizens for protesting – are part of a broader pattern of restricting democratic freedoms. They represent challenges to fundamental human rights and undermine the principles of transparency, accountability and public participation. Addressing these issues requires concerted efforts from civil society organisations, human rights advocates, international bodies and governments themselves to uphold the principles of freedom of expression, protect digital rights, promote an open and inclusive information ecosystem, and safeguard the right to peaceful protest.



Free speech, censorship. Photo: Yuri A/Shutterstock

LIMITATIONS ON FREEDOM OF EXPRESSION ONLINE

When analysing the environment for freedom of expression online in Serbia, North Macedonia and Greece, distinct patterns and practices emerge. In April 2020, just as the coronavirus pandemic was intensifying, the Serbian government proposed a decree, which mandated the centralisation of all information on the novel disease. The document stipulated that only higher government officials or members of the COVID-19 Response Team were able to release information concerning the virus during daily press conferences. The decision resulted in journalist Ana Lalić being held in custody for 48 hours due to her reporting on poor hospital conditions related to the coronavirus pandemic that was published on the Nova.rs news portal. Amid public dissatisfaction with the move, the decree was soon dropped, although it is worth noting that it was never even officially adopted, despite its short implementation. Government-affiliated media continued to harass Lalić, representing a persistent restriction on freedom of expression and, more broadly, on press freedoms.

In North Macedonia, while there have not been cases of opposition politicians, journalists, activists or civil society actors being penalised for their online activities, there have been instances of online threats, harassment and hate speech directed towards politicians and journalists on social media platforms. Social media posts have been used as evidence for the detainment or arrest of individuals promoting hate speech.

In Greece, there is an alarming trend regarding the penalisation of online activities. In 2022, there were abusive lawsuits filed by Grigoris Dimitriadis, the Greek prime minister's nephew and former Secretary General of Kyriakos Mitsotakis who also supervised the Greek National Intelligence Service, against media outlets and journalists. The lawsuits targeted reports alleging Dimitriadis' involvement with the wiretapping scandal in Greece. Hundreds of people were wiretapped by the Greek National Intelligence Service for "national security" reasons and in the same time they were also surveilled with spyware called Predator. In the above case, Dimitriadis has sued Thanasis Koukakis, a journalist who was both spied on by the Greek National Intelligence Service and with Predator spyware, demanding the withdrawal of his tweets about his involvement in the case. This wiretapping scandal raised concerns about journalists' privacy, source protection, and press freedom. Changes to legislation restricted the right of citizens to seek information about government surveillance for national security reasons, undermining transparency and accountability.

More specifically, the Greek wiretapping scandal, or Predatorgate, saw politicians, journalists and business people having their phones bugged by a spyware called Predator, and also by the Greek National Intelligence Service (NIS). Predator was developed by Cytrox, a North Macedonian startup, which was then bought by Intellexa. 'The initial targets for testing out the software were journalist Thanasis Koukakis and political leader and MEP Nikos Androulakis, who have both been shown to have been a common target of both the NIS and the spyware operators, with the government continuing to deny any official involvement with Predator. Stavros Malichudis, another Greek journalist, was the first to report (in 2021) that he was wiretapped by the NIS. In the wake of the revelations in the summer of 2022, the head of the NIS and the Prime Minister's chief of staff – and also nephew – who oversaw the secret service, Grigoris Dimitriadis, stepped down. In 2022, there was a Greek parliamentary inquiry into the surveillance scandal, but the ruling New Democracy party blocked dozens of witnesses proposed by opposition parties, including journalists whose phones had been wiretapped. In addition, the ruling party-controlled committee conducting the inquiry decided that all inquiry meetings would be held behind closed doors and remain confidential. During 2023, reports showed that Intellexa – the company that markets the Predator spyware – had edited a Greek Intelligence Service document proving that there is a link between the company and the Greek Secret Service. Also, it was reported that the Greek state gave the licensing of spyware exports to the authoritarian regimes of Sudan and Madagascar, as well as Ukraine. The investigation is still ongoing.

SHARE Foundation produced a comprehensive analysis into how authority figures in Serbia have created a direct system that allows them to access retained information from internet service provider (ISP) networks

On a couple of occasions, SHARE Foundation has analysed the government's data retention practices in Serbia. In 2017, SHARE Foundation produced a comprehensive analysis into how authority figures in Serbia have created a direct system that allows them to access retained information from internet service provider (ISP) networks. This system allows intelligence agencies to circumvent official channels, which normally require agencies to obtain warrants.

SHARE Foundation's 2020 analysis confirmed that information submitted by ISPs to the Data Protection Authority's office is often scarce and lacks broader context, and that this has been an ongoing trend in the last couple of years. This kind of lax approach to control mechanisms by the state leaves greater room for personal data to be misused by state authorities, notably the Serbian Security Information Agency (BIA), the Ministry of Interior (MUP) and the Military Security Agency (VBA). BIA has a direct link to the operators' retention database that allows them to surpass any formal request processes and extract any telecommunications metadata that they wish to obtain. This information has, on multiple occasions, been released from the intelligence offices, mostly straight into the tabloids, and in that way contributed to targeting individuals and obstructing police investigations.

Internet service providers in North Macedonia have privacy clauses for the handling and usage of customer data. Regarding government demands for account restriction, in the Terms of Use of T-Mobile, it is stated that when there is a criminal procedure, or when required in the interest of the security and defence of North Macedonia, a procedure for account restriction may be initiated. However, it is not disclosed what that particular process is. It is also not elaborated upon under which legal framework the government may require such restriction.

A1 Macedonia, a telecommunications company operating in North Macedonia that is owned by A1 Telekom Austria Group, points out in its Terms of Use that the company maintains the right to restrict customer access in the case of a governmentally identified breach of the Law of Electronic Communications (LEC). Additionally, when a breach of LEC is identified by governmental organs, the company will terminate the contract of the user. However, the process for responding to governmental identification of LEC breaches and notification of the client is not disclosed.

In Greece, there are significant concerns over what the state deems 'legal wiretapping'. In 2022, the wiretapping scandal affected journalists' privacy, journalistic source protection and press freedom in general. As Media Freedom Rapid Response reported, soon after New Democracy came to power in 2019, it moved to bring the intelligence service under the direct purview of the office of the Prime Minister and amended the requirements for the position of Director of Intelligence, in order to enable a preferred candidate of the Prime Minister to be appointed. In March 2021, the governing party rushed through a legislative amendment that changed the legal provisions, which allowed citizens to be informed by the Authority for Communication Security and Privacy (ADAE) about whether they had been under surveillance if it had taken place for national security reasons. Until March 2021, a person under government surveillance for national security reasons had the right to file a request with ADAE for information about themselves. However, ADAE would only provide that information once those measures were no longer in effect and, notably, only if disclosure would not compromise the purpose of the investigation.

An amendment adopted at the end of March 2021 (with retrospective effect) made it impossible for someone under government surveillance for national security reasons to receive information about the process or to seek a remedy. In early 2023, the Chief Prosecutor ruled in favour of restrictions that would permit the ADAE from conducting independent audits of telecommunications companies in order to determine if individuals are being surveilled by the government. Cases such as that of investigative journalist Thanasis Koukakis, as well as other journalists who report in the public interest, serve to underscore the problematic nature of this exemption, highlighting the potential for abuse of this clause. According to the latest report by the ADAE in 2021, there were 15,475 prosecutorial orders issued for 'national security' reasons. The number of authorised wiretaps has increased substantially over the years, from 4,871 in 2015 to 11,680 in 2019, and to 15,475 in 2021. The constant increase, during the last decade, of waivers for reasons of national security depicts the abusive practice and the broad interpretation of that concept by the Greek authorities.

Another issue is that the law does not define 'national security' or specify the exact circumstances of surveillance. Constitutional theory has interpreted the vague concept of national security as the protection of the country from external threats. When public authorities request the waiver of confidentiality for the purpose of verifying crimes, the judicial order (of the Judicial Council) should include the suspect's name, address and the judge's reasoning. In contrast, the name of the person and the underlying reasons for the surveillance are not mentioned in the order for national security, issued within the extremely short timeframe of 24 hours. Furthermore, there is no time limit regarding the duration of the judicial order, which can be renewed indefinitely by the Prosecutor of the Court of Appeals.

CENSORSHIP

In a report published by Citizen Lab in December 2021, it was discovered that government agencies in Serbia were most likely utilising the Predator software. Subsequently, in May 2022, Google's Threat Analysis Group reported that 'government-backed actors' in Serbia were likely employing Cytrox's spyware to exploit zero-day vulnerabilities in Android devices. This revelation came after a separate report by Citizen Lab in December 2020, which implicated BIA as a potential customer of Circles, another spyware tool enabling the monitoring of calls, texts and mobile phone geolocation by exploiting weaknesses in mobile telecommunications infrastructure.

In more than one instance, members of the Serbian Progressive Party have made comments about unpublished articles and correspondence between investigative journalists and their sources. The leaks have also found their way onto the front pages of government-affiliated tabloids, most notably in the case of Stevan Dojčinović, editor of the Crime and Corruption Reporting Network (KRIK), who has had his personal correspondence repeatedly intercepted by state agencies and published in government watchdog media.

A number of journalists in North Macedonia were targeted by the mass wiretapping incident that was uncovered in 2015, and which had been carried out by leading officials from the conservative VMRO-DPMNE party during the period between 2008 and 2015. According to the then President of the opposition party SDSM, Zoran Zaev, more than 100 journalists were wiretapped, including prominent names such as the late Nikola Mladenov (who passed away in 2013), who at the time was the managing editor of one of the country's most influential weekly newspapers, Fokus. The list of journalists who were wiretapped during that period also included prominent household names such as Sasho Ordanovski, Borjan Jovanovski and Goran Mihajlovski, among others. On the other hand, there have not been cases of journalists who have been penalised for posting on social media, or cases where social media posts have been used to discredit journalists' reporting.

In a report published by Citizen Lab in December 2021, it was discovered that government agencies in Serbia were most likely utilising the Predator software

As mentioned above, the spy scandal in Greece involved, firstly, the use of wiretapping by the National Intelligence Service for national security reasons, and secondly, the use of the Predator spyware. According to reports, the Greek government and the Ministry of Foreign Affairs gave their permission to Intellexa in order to export Predator spyware to Madagascar, Sudan and Ukraine. The Greek Prime Minister admitted there were mistakes made regarding the use of legal wiretapping by the

NIS; however, he still denies having used the Predator spyware. Despite journalists having established links between spyware companies and high-ranking government officials, the National Transparency Authority (EAD) cleared the government in its *ex officio* investigations.

Thanasis Koukakis, a financial reporter, has been working for CNN Greece for many years, as well as collaborating with other Greek and international media, such as the American CNBC, the Financial Times and Inside Story. Examples of his work include the 2019 investigation into Piraeus Bank, its former chairman Michalis Sallas and a number of transactions relating to the Libra business group, owned by the shipowner George Logothetis, which ultimately proved damaging to the bank (Financial Times 1.11.2019; Inside Story 28.1.2020 & 21.2.2020)

In November 2019, Koukakis also published an article in the Financial Times concerning how the Mitsotakis government had amended the Penal Code in a move that appeared 'to overturn Greece's commitment to international standards on combating corruption and money laundering'. His ongoing surveillance is suspected to be an act of harassment from the government. The same applies for Solomon's journalist Stavros Malichudis, who was the first person that was reported to have been wiretapped by the NIS. It related to an article that Solomon was preparing about the story of Jamal, a 12-year-old Syrian refugee who was being held at a detention centre on the island of Kos. The Greek National Intelligence Service (EYP) asked its officials to gather information on the source that Malichudis was in contact with (for the purposes of the article), in addition to information about the 12-year-old refugee himself.

PENALISING CITIZENS FOR PROTESTING (FREEDOM OF ASSEMBLY)

Following the December 2021 protests in Serbia against the planned construction of a lithium mine by the Australian company Rio Tinto, journalists and citizens involved in the protests were visited by the police at their homes and editorial offices. In a clear intimidation attempt, journalists and civil society activists across the country were advised by the police that they should not report on the ongoing protests and that they should also not participate in the road blockades that were taking place. Many of those that were targeted by the police operation were confused by the move, as many of them had only posted calls for mobilisation on their social media accounts. Both the Association of Journalists (UNS) and the Independent Association of Journalists (NUNS) identified the move as a clear intimidation tactic by the authorities, and called on the state to allow journalists to do their jobs unhindered.

In North Macedonia, citizens have later been identified in cases where protests turned violent, and there was notable damage to North Macedonia's institutions, such as the storming of the country's parliament on 27 April 2017. The perpetrators were identified thanks to videos and photos made from surveillance cameras inside the parliament, as well as the material that was made from the various media outlets that were using video and photo cameras inside the institution.

Retaliation for participation in protests in Greece is not applied directly, but citizens are put on the radar of the police, especially if they also have a certain political alignment (most notably in cases of leftists and anarchists). From that point on, there is a personal file created for them, and there is a heightened chance that they might be surveilled. In the case of an arrest, the aforementioned information could be used against them. One example of this is the case of Aris P., an anarchist who was arrested and questioned at Athens Police headquarters in 2021. He later sued the police, claiming he was beaten and tortured by masked officers and threatened with rape.

Furthermore, as of 2021, the Greek police have started to use body cameras, supposedly for safety and transparency reasons. The use of surveillance systems with the reception or recording of sound or images in public places is regulated by Decree 75/2020. The cameras are placed on the uniforms of police officers of different teams, such as the Crime Prevention and Suppression Team (OPKE), the motorcycle police unit (DIAS) and so on. Most of these cameras record incidents, and the relevant visual material can be searched and analysed at a later stage. Some cameras, however, transmit live images to the operational centre of the Greek Police. They are mainly used in cases of demonstrations, and they are activated after a decision by the head of the police force on site. The crowd present is immediately informed of the police operation.

However, according to lawyers, video recording constitutes an interference with protesters' right to privacy and right to demonstrate. The rights of a protester are likely to be restricted through video recording, as they may be reluctant to participate for fear of being recorded. Additionally, according to the Hellenic Data Protection Authority, the privacy of communications is affected where the reception and processing of audio data concerns communication between two or more persons, even if it occurs in a public place. In this respect, there is a need for better protection of data, as well as the development of a protection policy detailing who has access to the data of the demonstrators.

INTERNAL POLICING AND EXTERNAL BORDER SECURITY

The analysis and critical examination of how digital technologies are being utilised in national security and border practices is of utmost importance in today's rapidly evolving technological landscape. These technologies, including surveillance systems, facial recognition software and data collection mechanisms, have the potential to significantly impact individuals' privacy, civil liberties and human rights. Understanding and scrutinising their usage allows us to assess the implications for democratic principles, ethical considerations and the potential for government exploitation.

Governments around the world have increasingly embraced digital technologies as tools for enhancing national security and border control. While there are legitimate concerns regarding public safety and the need to protect national interests, it is crucial to balance these considerations with the protection of individual rights and freedoms. An analysis of the deployment and impact of these technologies allows us to assess whether they are being used within legal and ethical boundaries, and whether the benefits truly outweigh the potential harms.

The analysis and criticism of how digital technologies are employed in national security and border practices are vital for safeguarding individual rights, promoting transparency and maintaining democratic principles. By evaluating the ethical implications, assessing potential risks and advocating for responsible use, we can strive for a balanced approach that upholds both security and civil liberties in the digital age.

INTERNAL POLICING

Personal data centralisation is a practice that is not alien to the Serbian government. Although it usually ends in data breaches and cyberattacks, which expose citizens' sensitive information, another major point of contention in recent years has been the massive system of biometric surveillance. According to SHARE Foundation, the Serbian Ministry of Interior has been closely cooperating with China and Huawei in order to deploy a system known as the 'Safe City' solution, which would monitor the movement of all peoples residing on the territory of the capital Belgrade, as well as gathering their biometric data. However, even today, the government claims that this system is still not in use and that there have not been any definitive cases that would confirm its use; yet activists have demonstrated that the cameras have already been installed, and are visible across the city. The government has also attempted to regulate their use on several occasions.

Aside from the authorities' legal regulations and procedures, when it comes to storing such data on citizens, there is no evidence about the existence of a system or structure that would carry out a similar surveillance operation in North Macedonia.

A country partnership operation with FRONTEX, the European Border and Coast Guard Agency, on North Macedonia's external border was launched in April 2023. As the joint statement points out, the FRONTEX operation will, at first, cover North Macedonia's border with Greece, and it will later expand to also include the country's borders with Albania and Serbia. According to FRONTEX, more than 100 standing corps officers will support document checks and assist the local authorities in establishing the nationality of migrants. Per the press release, 'FRONTEX deploys border guards and patrol cars to North Macedonia to support local authorities with border surveillance and border checks, including checking documents as well as assisting in screening of migrants and gathering information on cross-border crime'.

According to information in the joint press release, officers working in North Macedonia under the FRONTEX-coordinated operation will use equipment provided either by the Member State that deploys them, the agency or by the North Macedonian authorities, including patrol cars, border surveillance equipment and equipment needed for document checks. According to the results from the first few months of the joint mission, the number of migrants and persons on the move has decreased by 25% in the first five months of the year compared to the same period in 2022.

Greece still has a legal framework in place that allows for the retention of metadata of electronic communications of all users of e-communications in Greece. Despite the fact that the EU Directive (2006/24), based on which the Greek law was adopted, was invalided by the EU Court of Justice in 2014 (Digital Rights Ireland Case), the Greek state never revised Law 3917/2011, continuing to allow the mass surveillance of all individuals residing in Greece. The Hellenic Ministry of Justice put in place a law-making committee back in 2014 to revise the law and produce related reports. However, thanks to a freedom of information request submitted by Homo Digitalis, it was revealed that the law-making committee produced zero output, and, as a result, it was dismissed in 2018. The telecom operators, not the police, maintain these databases, although the police can be granted access to them. This mass collection of e-communications metadata and storage (which is in its first year of use in Greece as of 2023) violates the EU Charter. Homo Digitalis also has a legal complaint before the Greek Data Protection Authority against Vodafone Greece on this matter, which has been pending since August 2019. It is the oldest running complaint, and the last communication on the complaint was in October 2022, stating that it is still under investigation as it deals with a complex matter.

BORDER AND MIGRATION PRACTICES

So far, there have been no instances of data interception from devices used by people on the move trying to enter into or crossing through Serbia. However, various reports have documented hostile and abusive practices at the neighbouring borders with Hungary and Croatia. This has also raised questions of potential cooperation between border forces.

Although no information has explicitly been provided to the public, an official agreement has been signed between the National General Directorate for Foreigners of Hungary and the Ministry of the Interior of Serbia that deals with asylum and migration. In 2022, President Vučić also signed a memorandum of understanding with Hungarian Prime Minister Viktor Orbán and Austrian Chancellor Karl Nehammer on curbing illegal migration, with Austria pledging to deploy manpower, as well as technical equipment such as drones and thermal vision cameras, to Serbia's border with North Macedonia. Witness testimonies and local organisations that work with populations on the move have also reported that Hungarian authorities, in cooperation with Serbian border patrols, have been complicit in border violence and pushbacks. Pushbacks refer to the practice of forceful removals of individuals back across a border to land that they were trying to flee, preventing them from entering the destination country. This can occur when individuals are denied entry, for example, due to not having the correct travel documents, violating immigration laws or their asylum claims being rejected. In any case, pushbacks are considered to be an inhumane practice and are often accompanied by harassment and violence against those who are subject to it.

Witness testimonies and local organisations have reported that Hungarian authorities have been complicit in border violence and pushbacks

Additionally, the role of FRONTEX should also not be overlooked. Over the last couple of years, the agency has been working on increasing and enhancing surveillance capabilities at the EU borders. Given that Serbia, a member hopeful, is one of the countries on the fringes of the Union, it is important to investigate whether similar practices are taking place at the Serbian borders. However, there has yet to be any evidence uncovered of border authorities using such technologies. A similar situation has been observed in North Macedonia, with no conclusive evidence available to suggest that surveillance technologies are being used at border crossings or that populations on the move are being subjected to practices such as device confiscation, surveillance or personal data retention.

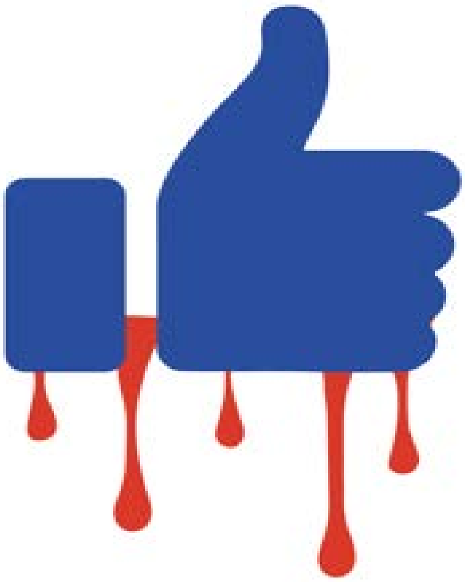
Greece is a well-known hotspot for individuals trying to enter the European Union from a number of third countries, which means that the number of people entering the country is exponentially higher than in the other two countries analysed in this report. Despite many controversies in the past, Greece has continued with its questionable practices when it comes to the treatment of people on the move. A 2022 report revealed that there were over 200,000 illegal pushbacks at external EU borders in 2022 alone, with more than 26,000 of those cases documented in Greece. The Greek digital rights organisation Homo Digitalis has worked with civil society organisations active in the field that provide support to asylum seekers.

Greece has continued with its questionable practices when it comes to the treatment of people on the move

Through their work on the ground, they have received information that electronic device extraction tools have been used. Even though survivor testimonies are the only evidence available for such claims, the stories paint a concerning picture.

According to the Balkan Investigative Reporting Network (BIRN), the Greek government repurposed pandemic recovery funds supplied by the EU in order to implement two new systems for monitoring people on the move and in makeshift refugee camps. The two systems, named HYPERION and CENTAUR, track people throughout the country, in and outside of asylum camps, using behavioural analysis algorithms, as well as fingerprint identification. They also send CCTV and drone footage directly to the Ministry of Migration and Asylum.

Social media platforms continue to play a large role in amplifying the spread of conspiracy theories and misinformation in Serbia and this trend has not evaded populations on the move. The biggest example is the Facebook group previously known as 'STOP the Settlement of Migrants', which has been active since the start of the coronavirus pandemic and has been deplatformed and reported multiple times. The group later rebranded itself as 'Stop Censorship' in January 2021, amassing around 320,000 members. The page is still run by a far-right group called People's Patrols, which has organised a number of anti-migrant rallies in Serbia's capital and participated in the July 2020 anti-government protests. Another prominent example is the case of a man livestreaming himself on Facebook while driving his car into the Obrenovac migrant reception centre. It was later revealed that the man was a member of the far-right organisation Leviathan, known for its hateful and discriminatory stances. The incident happened in 2020, during the coronavirus pandemic, and was influenced by the proliferation of hate speech and xenophobia directed towards people on the move residing in the country. This was also mirrored in the state's decisions regarding refugee and migrant populations residing in Serbia when the coronavirus state of emergency was introduced. Specifically, the government deprived migrants and asylum seekers of their movement rights as part of the national lockdown plan, unless special permissions were granted to them. The decision was



interpreted as a deprivation of liberty by civil society organisations and scrutinised for its speedy and potentially unlawful adoption. Anti-migrant rallies have also been organised across the country in which far-right actors have been critical of the country's acceptance of refugee and migrant populations, and have reinforced viral conspiracy theories such as 'the great replacement'.

During the refugee and migrant crisis on the Balkan route in 2015, multiple cases portrayed both migrants and refugees as a threat towards North Macedonia and its society. These cases have been reported via different media sources in the country, as well as through different social media channels. The far right in North Macedonia has mostly been spreading hateful rhetoric towards ethnic minorities in the country – and although there have been similar cases regarding migrant populations, they have so far been insignificant. MKD reports that North Macedonia is not seen as an attractive destination for migrant populations to move to, but instead is used as a transit country. In contrast, there have been no reports of the government using hateful content or rhetoric to influence public opinion on refugees and migrants.

In North Macedonia, the process of identifying migrants follows strict legal regulations and established procedures. Individuals are registered in a central database, involving the collection of their personal information, photographs and fingerprints. Those found to have entered the country illegally undergo interviews to determine their identity and the circumstances of their illegal border crossing. For individuals lacking proper identification documents, they are registered based on personal statements, with photographs and fingerprints taken. Measures are then taken to verify their identity within the bounds of the law. As for asylum seekers without documents, their process begins with a personal statement.

In North Macedonia, the process of identifying migrants follows strict legal regulations and established procedures

North Macedonia cooperates with international organisations such as the International Organization for Migration (IOM) and the United Nations Refugee Agency (UNHCR), utilising trained interpreters proficient in Pashto, Urdu and Farsi dialects to facilitate communication with migrants. Asylum seekers are provided with identification documents, which may be replaced with identity cards if their asylum status is granted, or retained as identification for asylum seekers throughout the procedure. Those without legal residence, including those who entered the country illegally, are processed according to legal regulations and receive appropriate decisions during the procedure, but they do not receive identification documents.

In Greece, there is often reporting containing hateful content or rhetoric, including some showing big groups of people on the move, or people staying in facilities hosting asylum seekers. In most cases, such reporting can be found in social media groups, on Twitter and YouTube, and, in some cases, also in online forums of various types: army forums, car forums, general topic forums and so on. During the far-right party Golden Dawn's tenure in parliament (2012–2019), they frequently used photos of refugees, trying to portray them as threats to Greek society. The government does not use these materials in official documents; however, they are still massively and openly used by government-affiliated media in order to influence public opinion.

A recent example is the 2023 Evros summer wildfires. During the fires, a man in Evros appears, in a video on social media, to have caught 13 migrants and crammed them into a trailer. He was claiming that they set the fire in Evros. The man and two more were arrested and accused of racially motivated violence and racially motivated kidnapping. The video, and others like it, tapped into suspicions among residents of Evros that the wildfires were the fault of migrants, thousands of whom pass through the region's forest every year en route to Europe. That led to violence and 'pogroms' by vigilantes that were 'hunting down' migrants. From that point, there was a government effort for a narrative that included the possibility – if not assertion – that refugees crossing the borders set the wildfires. Even the prime minister blamed the fires on populations on the move across Greece, claiming that the fires were almost certainly set by humans crossing the border routes. However, he did not present any evidence to back up his claim.

SURVEILLANCE INFRASTRUCTURE

As mentioned in the section on internal policing, the partnership between the Serbian government and the Chinese government and tech companies, more specifically Huawei, has been a point of contention for the last couple of years. Although there are no laws in Serbia regulating the use of biometric surveillance or mass personal data collection and storage, this has not deterred the government from rolling out surveillance cameras with biometric capabilities across Belgrade. The project would allow the Serbian government to surveil and collect the personal data not only of citizens, but of any people residing or visiting the city, as well as create a massive database that could be cross referenced with other government databases, which contain medical, employment and other personal information. SHARE Foundation has been fighting against the normalisation and implementation of such a system for years. Due to efforts from civil society and international awareness raising, the government backtracked on the 2022 Draft Law on Internal Affairs that would have legalised the use of biometric technologies in public spaces. The passing of such a law would have made Serbia the first European country to effectively legalise the use of such invasive technologies on a wide scale, with Belgrade being the first capital in Europe to be subject to complete biometric surveillance.

No such cases of mass surveillance infrastructure use have been reported so far in North Macedonia. However, it should be noted that the popular spyware tool Predator, which originated in the country, was found to be used to target individuals, including politicians, journalists and activists. The software has been found globally in countries such as Saudi Arabia, Egypt, Oman, Greece, Indonesia and others. As mentioned in the previous sections (on the limitations on freedom of expression online and censorship), Cytrox is part of the Intellexa allegiance, which deals with surveillance infrastructure and supplies governments around the world with invasive technologies that infringe on individuals' rights to privacy. Most recently, Predator and Cytrox were in the news again for targeting an Egyptian politician's devices, the same politician that was also mentioned in Citizen Lab's 2021 report.

The smart policing project of the Hellenic Police (a €4-million project, which was delivered by Intracom Telecom last September) is a good example of the use of surveillance technologies in Greece regarding facial recognition and fingerprint identification. It involves portable electronic devices, which are connected to the existing national and European databases and can retrieve biometric features, such as licence plate numbers and data documents. The Hellenic Police's goal is to use these devices to target third country nationals living in Greece in so-called irregular situations. However, these tools could also be easily used to monitor public assemblies and to identify people participating in them.

In the digital context, international human rights safeguards play a critical role in upholding civil liberties, protecting personal data and ensuring an independent and impartial judiciary

Homo Digitalis has had a pending complaint before the Hellenic Data Protection Authority (DPA) on this case since March 2020. The last update on this complaint was sent by the DPA to Homo Digitalis in October 2022, in which it was stated that the case should be discussed in a plenary session in order to take a decision on this matter. The Hellenic Police have acquired the devices, but we are not aware if they are using them, or whether they are waiting for the DPA's verdict.

Also in 2022, the Greek Migration Ministry announced it would use EU-funded drones with Artificial Intelligence to track people seeking refuge at the border. According to reports, EU-funded CENTAUR and HYPERION surveillance systems are also violating fundamental rights in Greece. These systems were deployed to monitor populations on the move, and are also examples of invasive surveillance practices. The systems were launched without basic data safeguards required under EU law.

INSTITUTIONAL HUMAN RIGHTS SAFEGUARDS

In the digital context, international human rights safeguards play a critical role in upholding civil liberties, protecting personal data and ensuring an independent and impartial judiciary. As technology continues to shape our societies, it is essential to establish robust safeguards that address the potential risks and challenges posed by the digital realm.

One of the key areas of concern in this section is the approach towards civil society in the digital space. International human rights safeguards emphasise the importance of promoting and protecting the rights of individuals and groups to freely express themselves, assemble and associate online. Governments should, by extension, then commit to respecting the right to digital privacy and refrain from censoring online content, as well as from imposing undue restrictions on civil society organisations using digital platforms to further their causes. Additionally, it is crucial to ensure that legal frameworks uphold the rights of civil society actors to operate independently and without fear of surveillance, harassment or reprisals, and to provide for adequate procedural safeguards in cases of violations, online harassment and threats.

Another critical aspect is the protection of citizens' personal data from being exploited by the government. International human rights safeguards seek to prevent the unauthorised collection, use and sharing of individuals' personal data by governments, corporations or other entities. Strong data protection laws and policies are essential to safeguard individuals' right to privacy and autonomy over their personal information. Governments must adopt transparent and accountable practices concerning data collection and processing, ensuring that data protection measures are in line with international human rights standards.

Moreover, the independence and impartiality of the judiciary are fundamental to upholding human rights in the digital context. An impartial judiciary ensures fair and just legal processes, preventing abuse of power and protecting individuals' rights against potential digital surveillance or arbitrary measures. International human rights safeguards call for an independent judiciary that is free from political interference, and any aspect of judicial proceedings tied to the online space should adhere to the principles of fairness, transparency and due process.

APPROACH TOWARDS CIVIL SOCIETY

In all three countries, civil society activists are subject to online threats and harassment. Drawing from the information produced by this research, it would appear that the state response to online harassment of civil society activists is either not the most agile or is inadequate.

In Serbia, online harassment towards citizens, including journalists, activists, women, marginalized communities and artists, is subject to prosecution. After acting upon criminal complaints, in the period between 2017 and 2022, domestic courts delivered 32 judgments in these cases. Of these, perpetrators were found guilty in 30 cases and sentenced to prison.

Journalists are routinely harassed online in Serbia, with NUNS documenting around 500 cases in the last three years. Most notably, writer and podcast host Marko Vidojković received more than 40 death threats in 2022, with only two of these resulting in court cases and sentences. Due to the high frequency and severity of the threats, Vidojković and his family left the country at the beginning of 2023 and resettled at a secret location. Notably, the threats were also coming from Aleksandar Šapić, a high-ranking official in the Serbian Progressive Party and, at the time, acting mayor of Belgrade. Vidojković's podcast co-host Nenad Kulačin, who was also threatened alongside his family members, stated that the prosecutor's office first encouraged the journalists to drop the case and then proceeded to dismiss the case against Šapić immediately, because his threat was expressed in the conditional tense.

Media outlets and individual journalists are subject to draconian fines for their independent investigations or opinions

In many cases, it is the media outlets and houses that are being sued. Strategic Litigation Against Public Participation suits, or SLAPP suits, have become increasingly routine in Serbia. Media outlets and individual journalists are subject to draconian fines for their independent investigations or opinions. The suits against journalists and media outlets are usually filed by high-ranking members of parliament or by their close associates. Investigative portal KRIK is one of the media outlets most targeted by this practice, due to its reporting on state corruption and government connections to criminal groups. They have also been subject to other intimidation tactics, with three female members of staff having their apartments broken into and ransacked in the past years. All the cases were reported, but so far, have not been investigated or solved, even though the intimidation element was clear since none of the women had anything taken from their apartments, but rather their things were ransacked, with drawers emptied and the contents scattered everywhere.

In North Macedonia, civil society activists have been subject to online threats and harassment, and many of them have turned to the authorities for protection. The Ministry of Interior has taken appropriate steps against those responsible for these actions and is also cooperating with civil society organisations in order to prevent future incidents. Notably, in cases where the authorities have been too slow to react and punish those responsible, civil society organisations have been among the most vocal advocates for justice for those that were harmed.

In cases of online threats, insults, blackmail or slander in North Macedonia, it is often considered the responsibility of the injured party to file a criminal complaint in order to initiate the proceedings. The criminal complaint also requires the evidence to be procured before the police are able to start the investigation. Affected parties tend to be reluctant to enter into this process and feel discouraged by the police and the amount of material that needs to be gathered in order to prove their allegations. By contract, in cases of allegations of incitement to disobedience and the spreading of fake news, the authorities can act *ex officio* and start criminal investigation on their own initiative.

In Greece, civil society activists are often the victims of online threats and harassment. This especially applies to activists dealing with migration issues or women's rights. A characteristic example is activist Iasonas Apostolopoulos, who, once celebrated for his efforts in rescuing refugees off the Greek coast, has in the past year been mysteriously denied a medal he was due to be awarded by the Greek president. Apostolopoulos was publicly accused of insulting his country by the prime minister's spokesperson for speaking out about illegal pushbacks of asylum seekers from Greece's borders.

In cases of online threats, insults, blackmail or slander in North Macedonia, it is often considered the responsibility of the injured party to file a criminal complaint in order to initiate the proceedings

The legal and institutional framework of protection available to individuals is insufficient, and there is no clear legal framework for the provision of protection upon request. The affected party is able to file a complaint, can provide the evidence for the threats and/or harassment and can ask for protection if their life is in danger. Technically, the police could provide a security escort to civilians for special security reasons, but it is the responsibility of each General Police Directorate to make a decision on a case-by-case basis. However, most of the security escorts approved are for journalists or business people, and very rarely in the case of civil society activists. Recent reports show that about 15,000 police officers are guarding politicians, business people, judges, journalists, diplomats and other designated 'targets'.

PERSONAL DATA EXPLOITATION

This section explores possible legal penalties, harassment or violence from the government or powerful non-state actors, in retaliation for critical remarks expressed by users of personal online communications, including direct messages, voice or video applications, or social media accounts with a limited audience.

Individuals in Serbia have been subject to different degrees of intimidation and harassment in response to their online activities. Most notably, in May of 2023, a nuclear engineer working at the Directorate for Radiation and Nuclear Safety and Security, who was active on her personal social media account and had been critical of the government in the past, was unexpectedly fired. As she posted on her social media, she believed the layoff was a direct response to her support for nationwide protests condemning the government's reaction to two mass shootings that took place earlier that month. The tweets were even cited as evidence of her firing, with the explanation for the termination of her contract being that 'that's what the [secret] services demanded'.

Furthermore, in December 2021, during the environmental protests against Rio Tinto's lithium mining project that rapidly spread across Serbia, it is suspected that the authorities exploited the personal data of the participants. As a means of intimidation, police visited activists, citizens, journalists and local community activists who had posted about the protests on Facebook, with the intention of discouraging them from attending any further gatherings. Seven such cases of police visits to activists were recorded. Community members, including journalists and civil rights activists that were labelled as part of the protest organisation team, received misdemeanour charges. The charges were based solely on the information they posted on social media regarding the protests. Three journalists were also targeted with court summons for allegedly participating in the organisation of protests in towns around the country.

Unlike in Serbia, in North Macedonia and Greece, no cases of retaliation against individuals through the use of personal data exploitation have been reported. Journalists in these countries are subject to other kinds of pressures and attacks, but the majority of these cases do not make it to court. North Macedonia has not had any documented cases of SLAPP suits in recent years either. In Greece, SLAPP suits are used by the government, although the verdicts are mostly in favour of journalists. However, despite the increased use of surveillance in Greece, journalists and civil society have not reported facing any retaliation in the form of personal data exploitation.

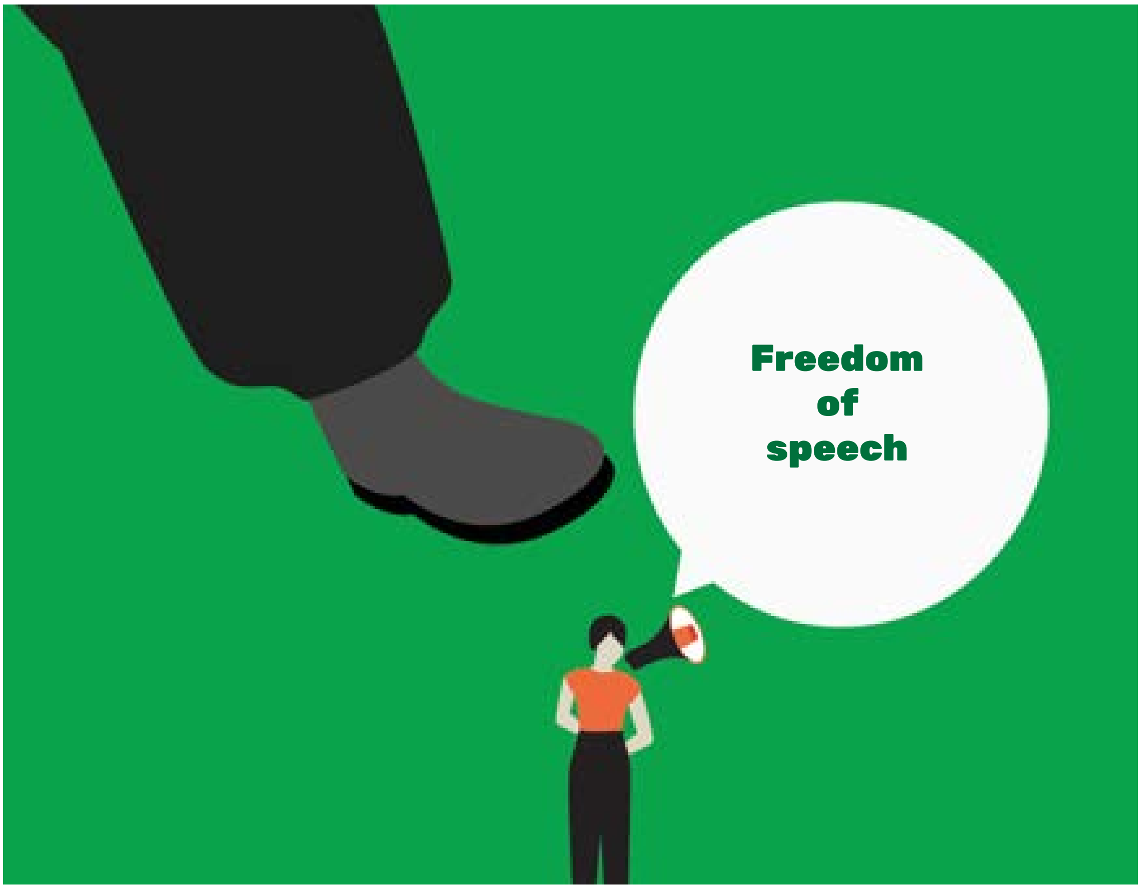
INDEPENDENCE AND IMPARTIALITY OF THE JUDICIARY

The independence and impartiality of judges and prosecutors due to their views expressed online has so far not been a topic of in-depth exploration. There is no data available on whether online content consumed by judges and prosecutors in Serbia impacts their objectivity and attitudes in the proceedings, and whether this serves as valid grounds to request their withdrawal from cases. However, the online presence of judges and prosecutors has in recent years become a topic of discussion in the Serbian public space. In 2021, the Council of Europe and the European Union facilitated the production of a comprehensive Guide on Ethical Aspects of Use of Social Networks, intended for judges and prosecutors. The guide covers various elements and contains recommendations concerning the freedom of speech of judges and prosecutors in the online space, as well as privacy issues, digital security and ethical behaviour expected from judges and prosecutors online. In addition, there are reports that suggest judges and prosecutors tend to face significant pressure in cases where public officials, including politicians, are the alleged victims of online harassment, raising questions about their bias towards high-profile cases. Judges and prosecutors involved in these cases come under pressure to conduct trials with extreme expediency, which has not been demonstrated in other cases of online harassment complaints. Prosecutors seem to easily enter into agreements of admissions of guilt with alleged perpetrators, in order to bring the case to a close, which raises questions about whether the alleged perpetrators are signing these admissions entirely on their own volition. However, no tangible data on potential recusal requests is available in these cases.

Comparably, there is no available data on potential recusal of judges and prosecutors in North Macedonia. In Greece, which has similar procedural requirements to Serbia when assessing the independence and impartiality of judges, the judge decides freely on the basis of the evidentiary procedure conducted before them. Judges are obliged to provide thorough reasoning in their decisions, which are subject to review by the higher court. The parties can allege the influence of the judge and ask for their recusal; however, it is quite difficult to succeed with such a request. Online portals commonly report on various court cases. Nonetheless, there is no hard data to attest whether such reporting influences judicial decision making.

In the case of Serbia, online threats directed at judges, prosecutors and other actors in court proceedings are not unheard of. According to a comprehensive research report on freedom of expression online, carried out by the Committee of Lawyers for Human Rights (YUCOM) and published in August 2022, public officials are often faced with threats from social media, most of which are through Facebook. This also includes judges and prosecutors. One example of such a case was a criminal trial in which the accused was found guilty of threatening the judge, the public prosecutor and their families online, using his Facebook profile. The court found him guilty of the criminal offence of endangerment of safety, and sentenced him to two years and two months imprisonment. In addition, the accused was prohibited from leaving his apartment during the criminal proceedings, which lasted for one year and four months.

In North Macedonia, there have been no reported cases on the independence and impartiality of the judiciary so far. Prosecutors face various threats, including online ones, most of which are made through social media channels. In such cases, police authorities act in accordance with the legal procedures of finding and sanctioning the perpetrators. If reported, it is up to the Ministry of Interior to act through its Department for Computer Crimes and Digital Forensics. In Greece, to initiate proceedings upon an alleged online threat, the victim would need to file a criminal complaint, as the state does not initiate these proceedings itself. In cases where the safety of prosecutors, investigative officers and judges handling certain cases is at risk, there is a provision for a police escort, following a relevant order of the competent public prosecutor. Such measures cease six months after the case being handled has concluded or can be extended for a further six months by a new reasoned order of the competent public prosecutor. For lawyers, there is no such dedicated provision; however, in certain cases, protection could be provided to them under the general protection procedures and provisions.



North Macedonia and Greece both enable users to monitor the course of cases online

When it comes to access to databases of national courts, Serbia has a court portal that includes the network of civil and criminal courts. By selecting the appropriate court and inserting the case file number, it is possible to obtain information on the value of the dispute, name of the judge to whom the case is assigned and the course of the proceedings, including the dates of hearings and submissions. However, the content of submissions is not available. Due to data protection regulations, it is impossible to search for a case based on names of the parties or lawyers representing them, so this search serves more those involved in the case to follow their own proceedings in an electronic format, rather than the interested general public. The Appellate courts, Supreme Court and the Constitutional Court all have their own websites through which they allow parties to follow the course of the proceedings, and they occasionally publish excerpts from judgments relevant for the development of Serbian case law, with personal data. The introduction of these online tools has significantly contributed to the efficiency of the work of the courts in Serbia.

Illiberal or liberal symbol. Photo: Dmitry Demidovich/Shutterstock

North Macedonia and Greece both enable users to monitor the course of cases online. In North Macedonia, it is even possible to access court documents, with certain restrictions (for example, if the text of the decision is too long, it might not be available in the online database). In Greece, Solon, the Digital Civil and Criminal Justice portal, provides electronic services to citizens and lawyers, such as the electronic deposition of documents and certificates, and the possibility of following the course of the proceedings. Although there is no free database where one can access decisions and data relating to court proceedings, the service platform is simple for those involved in the trial, in order for them to be informed about the basics without having to go to the court. At the same time, there are databases of court decisions that upload selected and anonymised cases so that jurisprudence can be gathered and studied.

CONCLUSION

In conclusion, given the current political and socio-economic climate, not just in the Western Balkans but in the whole world, it is important to highlight the ways in which digital technologies can be harmful to citizens, and especially marginalised communities, if left unchecked. Therefore, a number of measures are needed to not just curb existing harmful practices, but also account for potentially new threats that might arise from bad actors taking hold and experimenting with these technologies. The importance of pre-bunking both misinformation and disinformation campaigns, as well as strict regulation of the use of automated mass biometric and other invasive surveillance technologies, is a big but necessary task. It is also important to note that this is not just relevant to the Western Balkans region, but to Europe more broadly, as well as the rest of the world.

The issues that have been observed in this report are far from isolated and have all been present to varying extents in other parts of the world. Election manipulation and fraud, targeting and harassing civil society members and journalists online, misusing the private data of people on the move, and spreading misinformation and fake news online to further conspiracy theories or other nefarious causes are all unfortunate realities of our current global situation. This is why it's important to collaborate with decision makers within our respective communities, and also for governments to collaborate with each other in order to identify threats more effectively and find ways to combat malicious actors and attacks across the board.

BELOW ARE SOME CONCLUSIONS DIVIDED BY THE AREAS OF STUDY IN THIS RESEARCH REPORT, INCLUDING SOME OVERARCHING RECOMMENDATIONS TO FOLLOW:

- ### ELECTIONS AND PUBLIC PARTICIPATION

→ Bot accounts seem to be an integral part of the online election process in all three countries, increasing their activity during campaign cycles. The bots are mostly responsible for boosting the popularity of the ruling party or individual politicians, and seem to work undisturbed, in spite of reporting around how they operate.

→ Online public participation in debates about proposed laws does not seem to be very effective in the analysed countries; while each country to some degree allows online engagement with proposed laws, there still seems to be a lack of incentive from the government to involve people in the process of public discussion and consultation.

- ### FREEDOM OF EXPRESSION

→ The legal frameworks in all three countries seem to be stable and prevent various violations of rights, but in practice, these institutional frameworks have not provided sufficient guarantees in terms of the implementation of these rights.

→ Information disorders, such as hate speech, the spread of disinformation and limits on freedom of expression, have been reported in all three countries. In a number of cases, these limits seem to be orchestrated by the government, most notably in Serbia, where government agencies and officials explicitly misuse their positions to threaten and intimidate individuals, usually journalists, civil society members and activists.

→ Activists and journalists in all three countries are often victims of online threats and harassment. Although there is a legal framework allowing them to initiate court proceedings and seek redress, it appears that the official response in all three states is not fast enough and does not provide an adequate level of protection and redress. In addition, there are cases of journalists' and activists' personal data exploitation, which in some instances made them victims of retaliation by the state.

- ## INTERNAL POLICING AND EXTERNAL BORDER SECURITY

→ The use of invasive surveillance technologies has been documented in all three countries analysed in the report; however, there seems to be a lack of more in-depth information regarding how the state uses surveillance technologies to monitor citizens, and more specifically, civil society organisations, journalists and human rights advocates. However, various reports have shown that the spyware Predator has notably been used in Serbia and Greece to surveil journalists.

→ Given that all three countries are located on the Balkan route, migration matters are considered to be a focal point of internal and external security. In Greece, invasive surveillance technologies that are being used to monitor people on the move and store their personal information have been reported on extensively, but the government has failed to prove their legitimacy or necessity. In Serbia, there have been no official reports of such technologies being used at border crossings, but cross border cooperation with countries such as Hungary and Austria, as well as cooperation with FRONTEX, have been outlined as potential threats to the rights of people on the move.

- ## INSTITUTIONAL HUMAN RIGHTS SAFEGUARDS

→ In Serbia, there were several documented cases attesting to the possibility of prosecutorial and judicial bias when it comes to dealing with cases of online threats received by politicians. No such information was gathered for North Macedonia and Greece. Judges and prosecutors in Serbia do face various online threats, some of which have been subject to criminal proceedings. In North Macedonia, prosecutors face various threats; although the data on court proceedings is lacking, there is a legal framework allowing for recourse in such cases.

→ All three countries have online accessible court databases that contain information about cases and verdicts, which contributes to the transparency and efficiency of the decided cases and can be beneficial for bolstering public confidence in proceedings.

RECOMMENDATIONS

- **COMBATTING BOT INFLUENCE**

All three countries should implement stringent measures against bot accounts, particularly during election periods. It is paramount for governments to find a way to collaborate with social media platforms to identify and eliminate fake accounts. This is specifically important for North Macedonia and Serbia, since Greece's regulation is harmonised with the rest of the EU when it comes to big tech companies complying with citizens' digital rights through acts such as the Digital Services Act and Digital Media Act. Countries outside of the EU are often more vulnerable to rights violations on social media, and it is harder for them to get in contact with these platforms or impose any kinds of fines on them.

- **COMPREHENSIVE CYBERSECURITY REGULATIONS**

A lot of work is needed for governments to properly and responsibly introduce and enforce cybersecurity regulations to manage and prevent cyber incidents effectively. Effective and up-to-date cybersecurity regulations should be implemented in order to facilitate appropriate responses to incidents, protect institutions and individuals, and ensure resilience of critical infrastructure. In an era of dynamic and innovative digital threats, it is crucial for regulators to be vigilant and in step with emerging trends.

- **ENHANCING ONLINE PUBLIC PARTICIPATION**

There should be a push to incentivize government involvement in public discussions on proposed laws. Governments should work to develop user-friendly online platforms to encourage citizen engagement. This way, citizens would feel more included in the decision-making process and might be more motivated to participate in, and contribute to, public discussions on upcoming legislation and other topics that are important to democratic processes in their county.

- **STRENGTHENING LEGAL FRAMEWORKS**

Governments should evaluate and strengthen legal frameworks to ensure practical implementation of freedom of expression across digital spaces, and also ensure full functional independence of relevant regulatory bodies, preventing political pressures. Initiatives should also be proposed to review and amend laws, which would allow for the government to address information disorders and protect journalists, activists and other members of civil society, as well as citizens at large.

- **COMBATTING INFORMATION DISORDERS**

Work should also be done to strengthen collaboration between the government and civil society organisations to address online threats and harassment promptly. Additionally, there should be an effort put forth to enhance legal protections for journalists and activists against online threats and harassment conducted in collaboration between the government and civil sector to ensure transparency and accountability. Civil society and the media sphere should be able to freely investigate and address government involvement in spreading disinformation.

- **A BAN ON SURVEILLANCE PRACTICES**

Governments should introduce comprehensive regulations on surveillance technologies and investigate the use of invasive surveillance technologies, especially on journalists and human rights advocates. With that in mind, independent investigations on the uses of such technologies should not be prohibited or stifled in the event that misuses of such technologies are discovered, but moreover, should be addressed and accounted for by government actors and other malicious actors which might be implementing them. Adoption of legislation regulating the state's use of spyware should also be considered, ensuring legality, proportionality and scrutiny. Additionally, an independent review of border surveillance practices should be carried out and these practices should be prohibited in all instances of illegitimate use.

- **ADDRESSING BIAS IN LEGAL PROCESSES**

Governments should investigate cases of prosecutorial and judicial bias, particularly in regards to online threats towards judges, prosecutors and plaintiffs, and strengthen legal frameworks to protect judges, prosecutors, and public officials from online threats. The judicial system should ensure fair treatment of cases related to online threats against politicians and public figures. Promoting transparency in legal proceedings should continue through online accessibility of court databases.

SOURCES

https://www.frontiersin.org/articles/10.3389/fpos.2022.966472/full

https://pages.eiu.com/rs/753-RIQ-438/images/DI-final-version-report.pdf?mkt_tok=NzUzLVJJUS00MzgAAAGMBmNsugKkdVDioA5MUEdcSL4Zht9NfTm13Su-xVCibXZ9MVj0r9-9kk02SpFNYvzdbdJb9audE9jJ8MhT-oIEnOVsHlYt810qpqz3Z1qgKhll6Q

https://www.populismstudies.org/Vocabulary/liberal-democracy/

https://www.illiberalism.org/the-illiberal-experience-in-venezuela-the-transition-from-representative-democracy-to-authoritarianism/

https://www.foreignaffairs.com/russian-federation/erdogans-russian-victory

https://www.theatlantic.com/international/archive/2020/04/europe-hungary-viktor-orban-coronavirus-covid19-democracy/609313/

https://pages.eiu.com/rs/753-RIQ-438/images/DI-final-version-report.pdf?mkt_tok=NzUzLVJJUS00MzgAAAGMBmNsugKkdVDioA5MUEdcSL4Zht9NfTm13Su-xVCibXZ9MVj0r9-9kk02SpFNYvzdbdJb9audE9jJ8MhT-oIEnOVsHlYt810qpqz3Z1qgKhll6Q

https://freedomhouse.org/country/greece/freedom-world/2022

https://www.hrw.org/report/2022/04/07/their-faces-were-covered/greeces-use-migrants-police-auxiliaries-pushbacks

https://www.bbc.com/news/world-europe-65942426

https://www.statistics.gr/en/statistics?p_p_id=documents_WAR_publicationsportlet_INSTANCE_qDQ8fBKKo4lN&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_cacheability=cacheLevelPage&p_p_col_id=column-2&p_p_col_count=4&p_p_col_pos=1&_documents_WAR_publicationsportlet_INSTANCE_qDQ8fBKKo4lN_javax.faces.resource=document&_documents_WAR_publicationsportlet_INSTANCE_qDQ8fBKKo4lN_ln=downloadResources&_documents_WAR_publicationsportlet_INSTANCE_qDQ8fBKKo4lN_documentID=496978&_documents_WAR_publicationsportlet_INSTANCE_qDQ8fBKKo4lN_

locale=en

had the lowest rates

https://www.speedtest.net/global-index/greece#mobile7th place

7th place

https://pages.eiu.com/rs/753-RIQ-438/images/DI-final-version-report.pdf?mkt_tok=NzUzLVJJUS00MzgAAAGMBmNsugKkdVDioA5MUEdcSL4Zht9NfTm13Su-xVCibXZ9MVjOr9-9kkO2SpFNYvzdbdJb9audE9jJ8MhT-oIEnOVsHlYt810qpqz3Z1qgKhll6Q

https://freedomhouse.org/country/north-macedonia/freedom-world/2023
https://www.stat.gov.mk/PrikaziSoopstenie_en.aspx?rbrtxt=77

https://www.rferl.org/a/macedonia-eu-bulgaria-veto/31910319.html

https://www.stat.gov.mk/PrikaziSoopstenie_en.aspx?rbrtxt=77

https://www.speedtest.net/global-index/north-macedonia

https://ncsi.ega.ee/country/mk/

https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471

steadily declining

https://www.theguardian.com/global-development/2022/apr/21/serbia-sliding-towards-autocracy-as-president-secures-second-term

https://publikacije.stat.gov.rs/G2022/PdfE/G202216017.pdf

https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

https://www.speedtest.net/global-index/serbia

https://www.oecd.org/gov/open-government/open-government-an-integrated-approach-promotion-transparency-integrity-accountability-and-stakeholders-participation.pdf

https://www.un.org/esa/desa/papers/2020/wp163_2020.pdf

https://www.oecd.org/gov/oecd-guidelines-for-citizen-participation-processes-highlights.pdf

https://vlada.mk/node/18489

http://www.parlament.gov.rs/грађани/питајте.53.html

http://www.opengov.gr/home/

https://www.instagram.com/avucic/?hl=en

https://www.instagram.com/p/Cuj0UoblApP/?igshid=MzRlODBiNWFlZA%3D%3D

https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf

https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/serbia_march_twitter.pdf

https://balkaninsight.com/2019/12/18/alexander-the-bot-the-twitter-war-for-the-macedonian-soul/

https://www.gmfus.org/news/how-disinformation-harmed-referendum-macedonia

https://miir.gr/en/investigations/tweets/

https://medium.com/@andefined/-μ--ϖϖ-pt-2-607fb0bf725c

https://miir.gr/en/investigations/tweets/

https://balkaninsight.com/2020/03/06/facebook-extends-political-ads-rules-to-balkans-before-elections/

https://www.sharefoundation.info/wp-content/uploads/Izbori-2022.-izvestaj.pdf

https://crta.rs/wp-content/uploads/2023/01/Izbori-2022-godine-_CRTA-Zavrsni-izvestaj-sa-preporukama.pdf

https://faktor.mk/ne-stivnuvaat-reakciite-za-fejsbuk-reklamite-na-politicharite-kolku-potroshile-politicharite https://denesen.mk/ilievski-influenserot-kovachevski-vo-eden-den-frla-22-435-denari-za-fejsbuk-za-da-ve-ubedi-deka-e-vreden-i-uspeshen/

https://www.expres.mk/antikorupciska-povede-postapka-za-reklamiranjeto-na-kovachevski-na-fejsbuk/

https://thepressproject.gr/kyvernisi-youtuber-me-tis-megalyteres-diafimistikes-dapanes-stin-evropaiki-enosi/

https://www.efsyn.gr/politiki/390705_oi-dapanes-ton-kommaton-kai-ton-ypopsifion-se-google-kai-facebook

https://www.vice.com/sr/article/gy8n47/uobicajene-nepravilnosti-ili-izborna-kraduckanja-u-beogradu

https://m.mkd.mk/node/337798

https://transparency.mk/2009/02/26/glasachki-dvaesetki-narachuva-vmro-dpmne/

https://www.youtube.com/watch?v=SpitB6p7-W4

https://vouliwatch.gr/actions/article/palatirn-coivd-pierrakakis

https://www.danas.rs/vesti/drustvo/tajna-odluka-vlade-o-stavljanju-pod-kontrolu-informisanja-o-pandemiji/

https://www.article19.org/resources/serbia-journalist-ana-lalic-arrested-for-reporting-on-inadequate-hospital-facilities-for-coronavirus/

https://civilmedia.mk/smrtni-zakani-za-zaev-sela-i-dhaferi-na-fejsbuk/

https://360stepeni.mk/mazh-se-zakanuval-so-ubistvo-na-politichari-na-fejsbuk-obvinitelstvoto-otvori-predmet/

https://makfax.com.mk/makedonija/видео-три-години-и-еден-месец-затвор-з/

https://rsf.org/en/abusive-lawsuits-against-journalists-amid-political-tension-greece

https://www.politico.eu/article/greece-spyware-scandal-cybersecurity/

https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf https://insidestory.gr/article/evidence-joint-nis-predator-surveillance-centre

https://wearesolomon.com/mag/our-news/i-am-the-journalist-being-watched-by-the-greek-secret-service/

https://insidestory.gr/article/intellexa-makes-corrections-greek-intelligence-service-document

https://insidestory.gr/article/exagoges-kai-ekpaideysi-spyware-me-ti-sfragida-tis-ellinikis-kyvernisis

https://insidestory.gr/article/flight-predator

https://labs.rs/sr/zadrzavanje-podataka-o-komunikaciji-u-srbiji/

https://www.sharefoundation.info/sr/zadrzani-podaci-o-komunikacijama-u-2020-godini-formalnost-umesto-kontrole/

https://www.sharefoundation.info/wp-content/uploads/Zadrzani-podaci-2020_izvestaj.pdf

https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

https://www.balkanfund.org/site/pubs/uploads/publications/think%20and%20link/The_Anatomy_of_Capturing_Serbias.pdf

https://balkaninsight.com/ranking-digital-rights-in-the-balkans/north-macedonia-report/

https://balkaninsight.com/2023/06/12/data-spies-and-indifference-how-mitsotakis-survived-his-watergate/?utm_source=pocket_saves

https://www.mfrr.eu/greece-mfrr-alarmed-by-latest-revelations-of-spying-on-journalists/

https://balkaninsight.com/2022/08/23/how-many-greek-spyware-scandal-just-getting-started-says-targeted-reporter/

https://www.euractiv.com/section/politics/news/chief-prosecutor-puts-greeces-rule-of-law-to-the-test/

https://rsf.org/en/abusive-lawsuits-against-journalists-amid-political-tension-greece

https://balkaninsight.com/2020/12/04/serbian-security-service-named-among-users-of-israeli-surveillance-software/

https://www.balkanfund.org/site/pubs/uploads/publications/think%20and%20link/The_Anatomy_of_Capturing_Serbias.pdf

https://www.krik.rs/en/smear-campaign-against-krik/

https://www.danas.rs/vesti/drustvo/vucic-se-zali-na-prisluskivanje-ne-i-kad-prisluskuju-novinare/

https://prizma.mk/vkupno-55-godini-zatvor-vo-target-tvrdina/

https://www.mkd.mk/node/425740

https://mkd.mk/node/294557

https://insidestory.gr/article/greek-ministry-foreign-affairs-secret-investigation-reveals-predator-spyware-export-licenses

https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

https://insidestory.gr/article/flight-predator

https://insidestory.gr/article/intellexa-makes-corrections-greek-intelligence-service-document

https://www.reportersunited.gr/8948/o-megalos-anipsios-ki-o-megalos-aderfos/

https://www.ft.com/content/7a0fda92-e515-11e9-b112-9624ec9edc59

https://insidestory.gr/article/agogi-trapeza-peiraios-kata-proin-stelehon-eikonika-timologia?token=EMeBhQzwnt

https://insidestory.gr/article/praxeis-proigoymeni-dioikisi-trapeza-peiraios?token=J55XFm7hcu

https://wearesolomon.com/mag/our-news/solomons-reporter-stavros-malichudis-under-surveillance-for-national-security-reasons/

https://n1info.rs/vesti/nuns-policija-od-jutros-zastrasuje-novinare-po-srbiji/

https://n1info.rs/vesti/aktivista-iz-nisa-policija-me-probudila-u-7h-zbog-poziva-na-protest-na-fejsbuku/

https://www.theguardian.com/world/2017/apr/27/macedonia-protesters-storm-parliament-and-attack-mps https://sdk.mk/index.php/makedonija/organizatorite-na-27-april-vratarite-od-sobranieto-ushte-se-na-sloboda/

https://thepressproject.gr/i-confirm-what-the-greek-police-is-saying-no-one-called-dimitris-was-tortured-but-i-aris-was/

https://en.protothema.gr/major-reforms-announced-in-greek-police-all-officers-to-wear-body-cameras/

https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/proedriko-diatagma-75-2020-phek-173a-10-9-2020.html

https://www.in.gr/2021/11/05/greece/el-energopoiei-4-000-kameres-se-astynomikous/

https://www.syntagmawatch.gr/trending-issues/to-zitima-twn-kamerwn-foritwn-kai-swmatos-poy-feroun-oi-monades-apokatastaseos-tis-taxis-mat-tis-ellhnikhs-astynomias/#_ftn1

https://www.dpa.gr/sites/default/files/2020-07/gnomodotisi%203_2020.pdf

https://www.dpa.gr/sites/default/files/2020-07/gnomodotisi%203_2020.pdf

https://www.intellinews.com/serbia-reports-massive-cyberattack-on-interior-ministry-266192/

https://www.frontex.europa.eu/media-centre/news/news-release/frontex-launches-joint-operation-in-north-macedonia-U4I3Iv

https://data.consilium.europa.eu/doc/document/ST-12896-2022-INIT/en/pdf

https://frontline.mk/2023/06/29/fronteks-i-makedonskite-pogranichni-vlasti-so-rezultati-25-pomalku-migranti-vo-prvite-5-meseci-od-godinata/

https://homodigitalis.gr/posts/4048/

https://www.aljazeera.com/features/2022/2/18/serbia-hungary-asylum-seekers-violent-pushback

https://www.hrw.org/news/2023/05/03/croatia-ongoing-violent-border-pushbacks https://www.srbija.gov.rs/vest/en/208530/serbia-hungary-sign-several-agreements-aimed-at-strengthening-cooperation.php

https://www.reuters.com/world/europe/serbia-hungary-austria-agree-bolster-fight-against-illegal-migrations-2022-11-16/

https://medical-volunteers.org/Northern_Serbia_Advocacy_Report_DecJan_vFinal.pdf

https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

https://pers.11.be/translation-over-200000-illegal-pushbacks-at-eus-external-borders-in-2022

https://www.longroadmag.com/features/ongreeceslandborderlawlessness/

https://balkaninsight.com/2022/09/09/asylum-surveillance-systems-launched-in-greece-without-data-safeguards/

https://balkaninsight.com/2021/09/21/hate-lies-and-vigilantes-serbian-anti-vaxxer-brigade-plays-with-fire/

https://www.masina.rs/clan-levijatana-automobilom-upao-u-migrantski-prihvatni-centar-u-obrenovcu/

https://balkaninsight.com/2020/03/17/serbia-restricts-movement-for-migrants-asylum-seekers/

https://www.a11initiative.org/wp-content/uploads/2020/10/Deprivation-of-liberty-of-refugees-asylum-seekers-and-migrants-in-the-Republic-of-Serbia…_final-ENG-1.pdf

https://balkaninsight.com/2020/03/09/serbian-anti-migrant-protest-condemned-as-disgrace/

https://sitel.com.mk/na-makedonija-i-prestoi-opasnost-od-migrantite-za-eden-mesec-od-sega-se-ochekuvaat-po-5000-na-den

https://civicamobilitas.mk/wp-content/uploads/2018/02/radikalnata-desnica-vo-makedonija-1.pdf

https://m.mkd.mk/node/478550

https://twitter.com/giorgoschris2/status/1233905079222243328

https://www.youtube.com/@LathroGR

https://www.phorum.com.gr/viewtopic.php?f=92&t=50035

https://issuu.com/xagr/docs/1084

https://www.codastory.com/disinformation/disinformation-greece-wildfires-migrants/

https://www.milletnews.com/greece/mitsotakis-blames-migrants-for-forest-fires

https://www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back/

http://www.mup.gov.rs/wps/wcm/connect/4ceb4620-bcb6-4370-b55a-8f9dbb6f558d/НАЦРТ+ЗАКОНА+О+УНУТРАШЊИМ+ПОСЛОВИМА.pdf?MOD=AJPERES&CVID=ojJiNDS

https://eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state

https://irl.mk/shpionskiot-softver-predator-nelegalno-se-pravel-vo-skop-e-dodeka-nadlezhnite-zamizhuvale/

https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

https://www.hrw.org/el/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

https://algorithmwatch.org/en/greece-plans-automated-drones/

https://balkaninsight.com/2022/09/09/asylum-surveillance-systems-launched-in-greece-without-data-safeguards/

https://www.europarl.europa.eu/doceo/document/E-9-2022-003094_EN.html

https://www.yucom.org.rs/wp-content/uploads/2022/09/Sloboda-izrazavanja-u-digitalnom-prostoru.pdf

https://www.bazenuns.rs/srpski/napadi-na-novinare https://www.article19.org/resources/serbia-harassment-journalists-action-needed/

https://www.cenzolovka.rs/pritisci-i-napadi/sapiceva-monstruozna-pretnja-iscupacu-mu-srce/

https://www.slavkocuruvijafondacija.rs/en/podcast-authors-targeted-by-pro-state-media-and-threatened-on-social-media/

https://nova.rs/vesti/hronika/sapic-pretio-vidojkovicu-cupanjem-srca-tuzilastvo-odbacilo-prijavu/

https://n1info.rs/vesti/nuns-zabrinutost-zbog-talasa-slapp-tuzbi-protiv-medija-novinara-i-aktivista/

https://www.article19.org/resources/serbia-lawsuits-against-investigative-portal-chills-media-freedom/

https://www.slobodnaevropa.org/a/28604305.html

https://www.krik.rs/en/kriks-journalist-apartment-broken/

https://civilmedia.mk/tsivil-zaedno-so-gragankite-i-graganite-vo-aktsija-protiv-govorot-na-omrazata-1-del/

https://meduza.mk/fem-101/da-se-bide-zhrtva-na-govor-na-omraza/

https://24.mk/details/mvr-go-istrazhuva-govorot-na-omraza-na-socijalnite-mrezhi

https://mvr.gov.mk/vest/7219

https://a1on.mk/macedonia/helsinshki-tolerancija-na-govorot-na-omraza-vodi-kon-dela-od-omraza/

https://360stepeni.mk/video-koga-institutsiite-promoviraat-tolerantsija-no-na-govorot-na-omraza/

https://ecre.org/greece-government-takes-another-crack-at-preventing-free-press-reports-of-pushbacks-and-non-response-continue/

https://www.theguardian.com/global-development/2022/sep/01/speak-out-against-pushbacks-youre-an-enemy-of-greece-says-refugee-hero

https://www.capital.gr/epikairotita/3739461/sti-fulaxi-vip-stoxon-15-000-astunomikoi-oi-uperboles-oi-epixeirimaties-kai-ta-astunomika-tmimata-prostasias/

https://vreme.com/komentar/slucaj-nuklearne-inzenjerke-otkaz-zbog-politicki-nepodobnih-tvitova/

https://www.aljazeera.com/news/2023/5/7/normalisation-of-violence-what-led-to-serbia-mass-shootings

https://freedomhouse.org/country/serbia/freedom-net/2022#footnote7_tidhhjn

https://soinfo.org/vesti/vest/26608/prekrsajne-prijave-protiv-novinara-i-aktiviste/

https://n1info.rs/vesti/aktivista-iz-nisa-policija-me-probudila-u-7h-zbog-poziva-na-protest-na-fejsbuku/

https://safejournalists.net/safejournalists-index-skopje/

https://cpj.org/2022/10/in-greece-reporters-killings-unsolved-critical-journalists-complain-of-growing-threats/

https://www.ecpmf.eu/greece-full-scale-of-surveillance-on-journalists-must-be-unearthed/

https://vss.sud.rs/sites/default/files/attachments/Етички%20аспекти%20употребе%20друштвених%20мрежа%20-%20Водич%20за%20судије%20и%20тужиоце.pdf

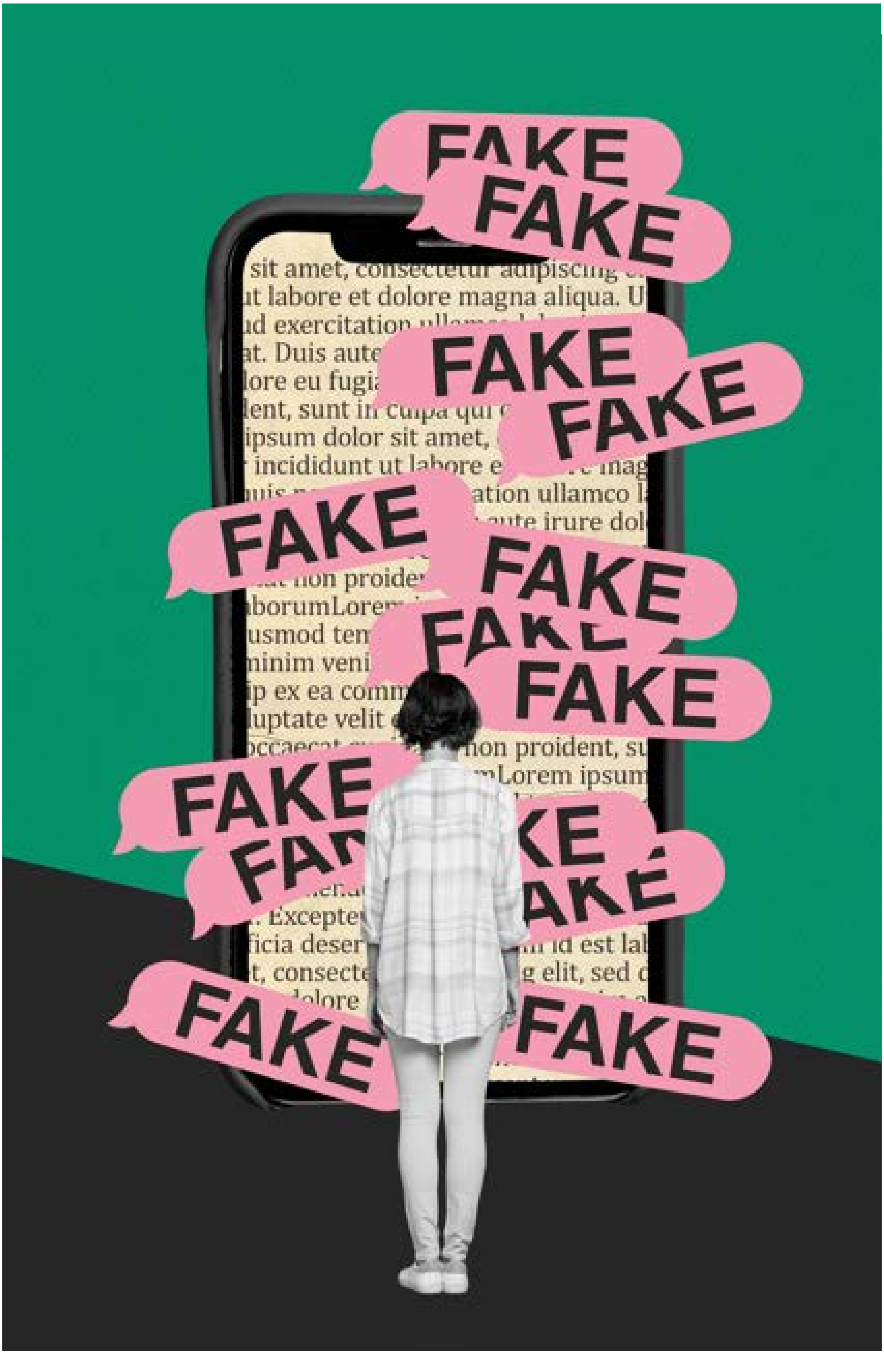
https://www.yucom.org.rs/wp-content/uploads/2022/09/Sloboda-izrazavanja-u-digitalnom-prostoru.pdf

https://tpson.portal.sud.rs/tposvs/

http://tpvks.portal.sud.rs:8080/SAPSPortal/select.do?court_id=VKS

http://www.ustavni.sud.rs/eSud/StatusPredmeta

http://www.solon.gov.gr



FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE
FAKE

THE GREENS/EFA
in the European Parliament

60 rue Wiertz/Wiertzstraat
60 1047 Brussels, Belgium
www.greens-efa.eu
contactgreens@ep.europa.eu