LIBERTIES ONLINE CIVIC SPACE REPORT

The Civil Liberties Union For Europe

November, 2023

CIVIL LIBERTIES UNION FOR EUROPE

civitates

Table of contents

Executive Summary

The Liberties Online Civic Space Report is the first report specifically focusing on the state of the online civic space in the European Union (EU). It offers a comprehensive overview of the most striking developments within the past five years concerning the online civic space in 11 countries across the EU. The report, drafted by the Civil Liberties Union for Europe (Liberties) with input from member and partner organisations, lays out the myriad of threats and challenges civil society organisations (CSOs), journalists, activists, and other human rights defenders face in the digital space.

A safe and free online civic space is crucial for the proper functioning of our democracy. It ensures that citizens can freely exercise their fundamental rights, including the freedoms of expression, assembly, and association. It is a key enabler to public participation, allowing people to share and receive information, organise and mobilise around issues that matter to them. However, censorship, surveillance and repression by governments, coupled with other digital threats, such as misinformation and disinformation, pose a great threat to the online civic space. Ahead of the 2024 EU Parliament elections, it is imperative that we defend a free and safe online civic space.

The issues covered in the report include online smear and disinformation campaigns, attacks, threats, harassment, doxing and hate speech, digital surveillance, data protection and privacy issues, challenges connected to online fundraising, online censorship and other means of restricting freedom of expression online, such as abusive lawsuits (SLAPPs), cyberattacks, regulatory hurdles and (in)action by law enforcement.

The findings from this report show that the EU and its member states have not been able to fulfil their obligation to protect and enable citizens to freely exercise their fundamental rights in the digital space. Instead of establishing clear rules that ensure a safe online space, they have left big corporations with the power to decide what can be posted and what cannot.

The result: civil society actors are increasingly targeted by populist authoritarians with smear and disinformation campaigns; civil society actors, particularly women and activists who work on sensitive issues, such as asylum and LGBTQI+ rights, continue to be exposed to online threats, harassment, doxing and hate speech; arbitrary decisions, whether by big online platforms or law enforcement authorities, have resulted in websites and social media accounts and pages of civil society actors being blocked; weak anti-SLAPP and whistleblowing laws have failed to protect those who report on abuses and unlawful activities; and to top it off, law enforcement authorities across the EU lack human and financial resources or the interest to investigate and safeguard victims of online attacks.

About this Report

This report offers a comprehensive overview of the most striking developments within the past five years concerning the online civic space in 11 countries across the EU, namely Belgium, Croatia, Czech Republic, France, Germany, Hungary, Italy, Poland, Slovakia, Spain and Sweden. It lays out the main threats and challenges CSOs, journalists and activists face in the online space.

The Civil Liberties Union for Europe (Liberties) is a Berlin-based non-governmental organisation (NGO) promoting human and digital rights across the EU. As an umbrella organisation, Liberties coordinates campaigns through its expanding network of national civil liberties NGOs. Currently, we have member organisations in 18 EU Member States including Belgium, Bulgaria, Croatia, the Czech Republic, Estonia, France, Germany, Hungary, Ireland, Italy, Lithuania, the Netherlands, Poland, Romania, Slovakia, Slovenia, Spain and Sweden. As an EU watchdog, Liberties closely follows the development of the EU Rule of Law Report, the Media Freedom Act, the Digital Services Act, the Proposal on Political Advertising & Transparency, the CSAM, the anti-SLAPP Proposal, the AI Act and frequently publishes reports on issues about privacy, surveillance, civic space and more.

The report brings together data from the following countries:

- BELGIUM
- CROATIA
- CZECH REPUBLIC
- FRANCE
- GERMANY
- HUNGARY
- ITALY
- POLAND
- SLOVAKIA
- SPAIN
- SWEDEN

Each country report reflects the information collected on the online space that civil society actors are working in. The areas reported on vary slightly from report to report, as some issues may be more relevant in one country than another.

The data used to produce the report was collected by the Civil Liberties Union for Europe with valuable input from the following organisations: Belgian League of Human Rights

(Belgium), the Center for Peace Studies (Croatia), Civil Rights Defenders (Sweden), Hungarian Civil Liberties Union (Hungary), the Italian Coalition for Civil Liberties and Rights (Italy), Glopolis and the League of Human Rights (Czech Republic,) the Polish Helsinki Foundation for Human Rights (Poland), Rights International Spain (Spain), Vox Public (France) and VIA IURIS (Slovakia).

The report is made possible thanks to financial support from Civitates.

What is Online Civic Space

Background

An essential element of any true democracy is the freedom of people to exercise certain fundamental rights. These rights include freedom of expression, freedom of association, and freedom of assembly. The "space" that allows people to freely exercise these rights – to say what's on their mind and converse with others, to protest against things that are not in their best interest, to join together in citizens' groups and other organisations – is referred to as "civic space."[1]

Civil society organisations (CSOs) are especially important in this space. They make democracy work by giving people a channel to communicate with their representatives. They keep people informed about how politicians are using the resources and powers given to them. And they make sure governments don't overstep the law and encroach on human rights. The more a government is accountable to the people, and the more involved people are in government, the more likely it is that politicians will act not in their own best interest but in the people's.

Unlike in the past, where civic space was largely limited to physical spaces, such as town halls, community centres, and public squares, the digital space is a vast and ever-changing landscape. Whether on social media, online forums, blogs, websites or other digital platforms, citizens can exercise their right to freedom of expression, assembly, and association. This has fostered political participation, enabling people to organise and mobilise around issues that matter to them, regardless of their background, location, ethnicity, religion or sexual orientation.

However, the internet also presents many challenges and threats that affect civil society actors. Mis- and disinformation makes it difficult for civil society actors to get their message out and engage with the public. Online harassment, hate speech and intimidation, including threats of doxing and trolling, can have a chilling effect on their work and discourage them from speaking out on important issues. Censorship, either by governments or by arbitrary decisions of online platforms, violate CSOs' right to freedom of expression. Cyberattacks, such as data theft, where personal information of staff or supporters are stolen, which can be used to blackmail, intimidate, damage the reputation of or harm civil society actors and their communities.

1 Civil Liberties Union for Europe, What is Civic Space? Why Is It a Keystone in Any Democratic Society? How Do We Protect It? https://www.liberties.eu/en/stories/civic-space/44189, May 9, 2022

Civil society actors give a vital contribution to the promotion and protection of our human rights and should be acknowledged and cherished as a key enabler of peace and unity. While the European Commission is increasingly recognising the importance of safeguarding civic space,[2] some EU governments still pay too little attention to supporting and strengthening civil society.

EU initiatives affecting online civic space

There are various EU laws and initiatives that, whether directly or indirectly, have an impact on the online civic space. The obvious one is the Digital Services Act (DSA), which will be discussed in further detail in this report. The EU Whistleblower Directive and the Anti-SLAPP Directive aim to protect journalists and human rights defenders, including from threats to their right to freedom of expression in the digital space. The currently discussed European Media Freedom Act will also significantly shape the online environment, including the controversial Article 17, referred to as the "media privilege", which divides both civil society actors as well as parliamentarians, as it may provide a loophole for disinformation content.[3]

The EU has also strengthened its support for CSOs through increased funding opportunities made available under the new Citizens, Equality, Rights and Values Programme and adopted a proposal to facilitate cross-border activities of non-profit organisations in the EU, which would enable CSOs to apply for the legal status of a European Association, which would provide some legal clarity and help mitigate the overall trend of shrinking civic space.[4]

Other measures taken by the EU that intend to enable citizens to exercise their rights freely in the digital space include the 2016 Code of Conduct on Online Hate Speech,[5] a proposal to extend EU crimes to include hate speech and hate crimes, which are often perpetrated online,[6] and the 2018 Code of Practice on Disinformation,[7] which was further strengthened in 2022.[8]

2 European Commission, EU Charter of Fundamental Rights: annual report looks at role of civil society and underlines need to increase support, https://ec.europa.eu/commission/presscorner/detail/e%20n/ip_22_7521, December 6, 2022

3 Théophane Hartmann, Oversight level for online media freedom set to divide EU parliamentarians, September 26, 2023

4 European Commission, Commission facilitates the activities of cross-border associations in the EU, September 5, 2023

5 European Commission, The EU Code of conduct on countering illegal hate speech online

6 European Commission, Extending EU crimes to hate speech and hate crime

7 European Commission, 2018 Code of Practice on Disinformation, June 16, 2022

8 European Commission, The 2022 Code of Practice on Disinformation

However, as stressed by the European Parliament,[9] the EU must not regard the protection and promotion of civic space at national and EU level as a completed task. Left without adequate support and protection against threats and attacks, the efforts of civil society cannot be sustained in the long term. The European Commission[10] and the Council of EU member states[11] officially acknowledged in 2022 that civil society is facing pressures, including in the digital space, and needs further support.

Protecting fundamental rights in the digital space

While the digital space can be an enabler for stronger public participation, it also presents many threats and challenges to citizens' fundamental rights, including the right to freedom of speech and expression, the right to free and fair elections, access to reliable information and the right to form associations.

Malign actors are using the internet to spread misinformation and disinformation. Given the vast amount of information that is found online, it is impossible to verify the accuracy. This undermines the access to reliable information, obstructing constructive political debates. Attempts by EU member states to regulate and criminalise disinformation have raised questions about the implication on fundamental rights, especially the right to freedom of expression.[12]

Media freedom and the right to freedom of expression and right to access information are also undermined by attacks against those who speak up on matters of public interest, including journalists and civil society actors. They include hate speech, online harassment, intimidation and smear campaigns, which affect the victim's mental health and have a chilling effect. In addition, restrictive legislation may censor legitimate content, undermining freedom of expression, which can have a particularly serious impact on online debate. Furthermore, online debates are often not representative of the debates in our society, as people with more extreme opinions tend to be disproportionately active and hence more visible,[13] contributing to a more polarised society.

Another challenge is the lack of tools many targets of online attacks have: low digital literacy among the general public and weak digital security skills can make them easy prey for ill-intentioned people.

9 European Parliament, Civil society: Parliament calls for EU rules and strategy to counter threats, March 8, 2022

10 European Commission, EU Charter of Fundamental Rights: annual report

11 Council of the European Union, Council Conclusions on the application of the EU Charter of Fundamental Rights; The role of the civic space in protecting and promoting fundamental rights in the EU, February 24, 2023

12 Ó Fathaigh, R. & Helberger, N. & Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, 10(4). https://doi.org/10.14763/2021.4.1584

13 Gaisbauer et al, Ideological differences in engagement in public debate on Twitter, Marc 25, 2021

A serious issue concerning citizens' freedom of expression and access to information is also that non-democratically elected social media platforms have been acting as the gatekeepers, deciding what can and cannot be said and published. Until now, content moderation has been unreliable. Online platforms are regularly failing to remove illegal content and instead have been censoring harmless content, seriously undermining the right to freedom of expression.

Transparency has not been a strength of social media platforms. More than once, platforms shut down research projects, threatening legal action, including a research project on hate speech on Twitter[14] and an Instagram monitoring project.[15] Big platforms' own research, suggesting that social media is damaging people's mental health, remained hidden.[16]

Online platforms and the Digital Services Act

Today, the enormous power of very large online platforms (VLOPs) and very large online search engines (VLOSEs), classified by the EU as platforms that have more than 45 million users per month,[17] presents a key threat to online civic space and democracy as a whole. From manipulation by political actors[18] to growing polarisation and decline in political trust, studies have shown that digital media can play an important part in eroding democracy.[19]

EU legislators have been stepping up. On November 16, 2022, the Digital Services Act (DSA) entered into force.[20] The DSA intends to harmonise the rules for online service providers across the EU and create a strong transparency and accountability framework. It also aims to address the power imbalance between platforms and their users, currently clearly favouring the former, and establish a safe online environment.

14 David Klepper, Musk threatens to sue researchers who documented the rise in hateful tweets, August 01, 2023

15 Nicolas Kayser-Bril, AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook, August 31, 2021

16 Damien Gayle, Facebook aware of Instagram's harmful effect on teenage girls, leak reveals, September 14, 2021

17 European Commission, DSA: Very large online platforms and search engines

18 Carole Cadwalladr and Emma Graham-Harrison, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, March 17, 2018

19 Lorenz-Spreen, P., Oswald, L., Lewandowsky, S. et al. A systematic review of worldwide causal and correlational evidence on digital media and democracy. *Nat Hum Behav* 7, 74–101 (2023).

20 European Commission, Digital Services Act: EU's landmark rules for online platforms enter into force, November 16, 2022

There are a total of 19 VLOPs and VLOSEs affected by the DSA, including Facebook, Instagram, TikTok, X (formerly Twitter), YouTube, Snapchat, LinkedIn, Pinterest, Amazon, Booking, AliExpress, Zalando (which contested the decision),[21] Google Shopping, as well as Wikipedia, Google Maps and Google Search.

These companies must now comply with a new series of rules. They have to block without undue delay illegal content, such as defamation, hate speech, calls for violence, death threats or photos of child sexual abuse. The DSA also prohibits dark patterns that trick users into sharing their personal data and obliges online platforms to be more transparent about their recommender systems.

The DSA also aims to rebalance the power relationship between platforms and their users. Platforms must, for example, make the "Terms and Services" easier to read, and provide adequate explanation when they remove and block content, profiles and pages. Users will have new rights to challenge content moderation decisions, including seeking out-of-court settlements if necessary.[22]

The DSA also includes a data access provision, providing a huge opportunity for researchers and regulators to understand and scrutinise governance of online platforms and the impact they have on our societies.[23]

The EU has stressed its seriousness to make platforms obey the rules, even threatening social media shutdowns, as have happened in other countries across the world,[24] in case the platforms don't address problematic content.[25]

However, whether the DSA will actually create a safe(r) digital space remains to be seen. Much of it will depend on the regulators' ability to enforce the rules while fully upholding the rights to freedom of expression and of information.

21 Zalando, Zalando files legal action against the European Commission to contest its designation as a "Very Large Online Platform" as defined by the Digital Services Act, June 27, 2023

22 John Albert, A guide to the Digital Services Act, the EU's new law to rein in Big Tech

23 Julian Jaursch, Philipp Lorenz-Spreen, Researcher access to platform data under the DSA: Questions and answers, August 2023

24 https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent

25 Clothilde Goujourad, Nicolas Camut, Social media riot shutdowns possible under EU content law, top official says, July 10, 2023

Trends

Online smear and disinformation campaigns

CSOs, activists and journalists, who inform the public about government corruption or the harmful actions of corporations, are increasingly being targeted by public and personal attacks against their character and work.

Smear and disinformation campaigns are being used by populist authoritarians to damage the reputation of civil society, to undermine their credibility and the public's trust in them, to intimidate them or even to silence their work altogether. They are also often used as a tool to divert attention, a common feature for attacks launched against investigative journalists for example.

In Hungary and Poland, government officials and politicians are using online smear campaigns against journalists and CSOs who oppose their autocratic regime. They sometimes resort to dishonest and deceiving methods, for example by fabricating evidence to discredit journalists, or try to label critical voices, including politicians, CSOs and journalists, as "Russian agents".

Disinformation campaigns with a pro-Russian narrative have spread in several countries, including Slovakia and Sweden. In the former, the National Security Office went as far as to block websites deemed to contain disinformation.

In France and Italy, sea rescue organisations helping migrants in the Mediterranean Sea have been targeted by far-right politicians with online smear and disinformation campaigns that linked the organisations' humanitarian effort to the activity of smugglers. Disinformation is also commonly used to spread hate against minorities, such as the Muslim community in Sweden.

In Germany, disinformation increased significantly during the coronavirus pandemic. Supporters of the right-wing Alternative für Deutschland (AfD) party and conspiracy theorists accused the media and NGOs of lying and manipulating data to exaggerate the severity of the pandemic and thus justify restrictions. In both Germany and France, the last federal elections were plagued by a voter-fraud narrative used by the Republican Party in the United States.

As governments are struggling to combat disinformation, nonprofits and CSOs, including the EU Disinfo Lab, EDMO BeLux, Faktograf, Czech Elves, Italian Digital Media Observatory or Konspiratori.sk, have been stepping up, monitoring, flagging and/or debunking disinformation.

Resource: Liberties has published a guide[26] on how activists working for progressive causes can counter smear campaigns. It's actually not much more complicated than following a basic messaging structure – as long as you also keep in mind several important things that are particular to dealing with smear campaigns. The key points in a nutshell:

1) never repeat your opponent's smear, it cements the most emotive words in your audience's mind,

2) no myth-busting and no direct contradictions,

3) careful to not co-opt your opponent's message, and finally

4) don't use overly technical language.

Attacks, threats and hate speech online

There is a worrying trend of increasing violence against journalists and human rights defenders across the EU, both offline and online.[27] This is the case for almost all countries included in this report, including **Croatia, the Czech Republic, Germany, Hungary, Italy, Poland, Spain and Slovakia**. For many activists, these attacks have an important psychological impact and may lead to changes in career plans. In many cases, online threats and hate speech have served as a precursor to physical violence.

Oftentimes, the attacks come from government officials and religious leaders, such as in **Poland** and **Hungary**. In several EU member states, including **Belgium, Germany, Hungary, Spain** and **Sweden**, women are particularly targeted with online threats, hate speech and harassment. Other targets are activists and CSOs who defend the rights of minorities. In the **Czech Republic, Germany, Hungary** and **Poland**, for example, LGBTQ activists are particularly targeted. In **Italy, Poland** and **Sweden**, activists who work on immigration and asylum issues, and work with and for ethnic and religious minorities are the victims of attacks.

Surveys are providing facts supporting these trends. In **Slovakia**, two-thirds of media workers have experienced attacks on their character. In **Sweden**, a government survey found that 67 percent of female journalists and 41 percent of male journalists were victims of online attacks.

The way courts rule on hate speech cases varies significantly from country to country. While in the **Czech Republic** and **Germany**, more and more people are being punished and receive prison sentences and, in the case of **Germany**, there are regular house searches, the Supreme

26 Israel Butler, How to talk about civic space: a guide for progressive civil society facing smear campaigns, December 2021

27 Civil Liberties Union for Europe, Rule of Law Report 2023, March 2023

Court in **Poland**, known for its lack of independence, applies rules rather arbitrarily.

The encrypted messaging service Telegram is particularly popular among conspiracy theorists, anti-vaccine influencers and extremists. Germany even considered banning the company for its failure to rein in conspiracy theories and hate speech. In several countries, including the **Czech Republic, France, Germany, Poland, Italy** and **Spain**, Telegram is being used to promote pro-Russian propaganda.

Doxing

One form of online threats that is less covered in the media is so-called doxing, the practice of publishing personal identifiable data of people on the internet, without their permission. This includes names, phone numbers, home addresses, private photos and other personal information. While human rights defenders and journalists are not the only victims, the disproportionate amount of hate speech and harassment they face makes them also more vulnerable to verbal and physical attacks as a result of doxing.

In **Germany**, far-right groups keep "enemy lists" that contain personal information of activists, journalists, and artists. The government in 2021 amended the criminal code to punish doxing and the publication of enemy lists. In **France**, the tragic murder of Samuel Paty prompted the government to criminalise doxing. Similarly, in **Belgium**, the government reformed its criminal code to include online harassment and doxing.

In **Hungary**, the personal data of a journalist who conducted investigations on corruption cases of high-ranking government officials was leaked and a magazine with links to the government published a list of persons considered "enemies of the state". In **Spain** too, most victims of doxing - which is a punishable offence in the criminal code since 2015 - are journalists. In 2021, the far-right party Vox threatened and published the name and photograph of the editor of a satirical magazine, as well as the city and street location of the magazine's office.

Digital surveillance

Digital surveillance in the online civic space can have a chilling effect on freedom of expression, lead to discrimination and targeting, and undermine democracy. And in several countries of the EU, governments have been illegally spying on their constituents.

In **Hungary**, state-administered digital surveillance has been increasing. The Orbán regime has been using the Pegasus spyware to monitor hundreds of people, including journalists and activists. Once the scandal was revealed, the government attempted to justify the covert surveillance by labelling the local NGOs as "foreign agents".

Pegasus has also been used in **Poland**, where political opponents and critics of the governments were systematically surveilled, and in **Spain**, where the government used surveillance software to spy on journalists, lawyers, human

rights defenders and political representatives from Catalonia and the Basque country.

Meanwhile, there is an increasing normalisation of citizens' surveillance in certain countries in the EU. In **France**, for example, the fear of terrorism has set the scene for a wider acceptance of surveillance for purposes of national security, and the upcoming 2024 Olympic Games are providing a great opportunity for proponents of increased surveillance.

Online censorship

Restrictions to the right to freedom of expression remain an important issue within the EU. In **Poland**, a party of the ruling coalition submitted a draft law that would tighten the existing blasphemy law, criminalising, among other things, insults to the church. In 2021, the **Hungarian** government banned the sharing of information that could encourage homosexuality or gender transition of under eighteen-year-olds, violating the right to access to information and freedom of expression.

Having an online presence is practically a must for any organisation today. For some, their biggest strength is a large online follower base to which they can only communicate via their website or their social media channels. So when this resource is cut off, the very existence of their organisation is at play.

Several CSOs have seen their websites or social media platforms been taken down. In **Germany**, the Facebook account of one NGO was blocked and another deleted in the company's content moderation decisions that were criticised for their arbitrariness and lack of transparency. Similarly, Facebook removed fan pages and groups belonging to an NGO in **Poland**, allegedly because the NGO violated the company's community standards. Facebook did not provide any warning or explanation.

While it's mostly social media platforms who take down pages, sometimes law enforcement authorities take that role. In **Germany**, for example, a regional police confiscated the website of a climate activist group noting that it is a criminal organisation, without having the actual competence of making such a decision.

Strategic Lawsuits Against Public Participation (SLAPPs)

Strategic lawsuits against public participation (SLAPPs) are a serious hindrance to the democratic process. Journalists, bloggers, online media portals and human rights defenders are being silenced by powerful people who seek to suppress the truth with disingenuous lawsuits. The activists often decide to shut down their investigation for fear of facing exorbitant legal fees. Often overlooked is that victims of SLAPPs are also facing harassment and hate

speech online, which places additional burden on the already difficult situation.[28]

Across the EU, legal safeguards against SLAPPs are almost completely lacking and the number of SLAPP cases recorded have drastically increased within the last several years.[29] The individuals behind the SLAPPs have different backgrounds, from powerful business people, to politicians, police officers and lawyers. Most SLAPPs are framed as defamation or data protection cases.

In **Croatia**, the situation is particularly grim, with close to a thousand active lawsuits against media outlets and journalists. In **Poland** too, media actors are bombarded with abusive lawsuits, in particular the newspaper Gazeta Wyborcza, which faced approximately 90 SLAPPs in 2022. In **Italy**, SLAPPs have increased since the start of the leadership of Prime Minister Giorgia Meloni, with the journalist Federica Angeli collecting more than a hundred lawsuits by herself.

> Initiative: The Coalition Against SLAPPs in Europe (CASE) is a coalition of non-governmental organisations from across Europe united in recognition of the threat posed to public watchdogs by SLAPPs. This summer CASE released a new report, which contains an analysis of over 200 abusive lawsuits in 35 different countries.[30]

Law enforcement capacity to investigate online attacks

The capacity of law enforcement authorities to investigate online attacks is very limited. Oftentimes, authorities lack resources and officers don't receive the necessary training. But in some cases, it's also just not a priority. In **Croatia** and **Germany**, for example, authorities are not taking hate speech against journalists too seriously. In **Hungary**, the government has taken measures to combat hate speech online, but they remain cosmetic fixes and most cases are unresolved.

However, there are also positive developments. In the **Czech Republic**, police investigations of online hate speech have been increasing. In **Sweden**, the government established a new agency to combat disinformation and propaganda.

Other measures are more controversial, as they conflict with the right to freedom of expression. Following the Russian invasion of Ukraine, the government in **Slovakia** granted the National Security Office temporary permission to block online content under reasons to minimise radicalisation, political destabilisation and threats to democratic institutions.

28 A. Jedrejcyk, Bart Staszewski: You're suddenly attacked by anonymous trolls, August 5, 2021

29 https://www.the-case.eu/slapps/

30 CASE, How SLAPPs increasingly threaten democracy in Europe – new CASE report, August 23, 2023

Recommendations to the EU

Creating a safe digital environment

- The EU should enhance and expand its monitoring and reporting of challenges affecting activists and other civil society actors in the online space within its annual rule of law audit and use enforcement powers against restrictive laws breaching EU rules.

- The EU should ensure that member states who have taken steps to prohibit hate speech, incitement to violence and the spread of disinformation are not using them as an excuse to curb free speech.

- The EU should protect civil society actors from undue digital surveillance and violations of privacy, including in the context of regulatory efforts such as the EMFA and the AI Act.

Establishing an enabling regulatory framework

- The EU should further support civil society's fight against disinformation, including in their fact-checking efforts, and require online platforms to not only make data available to researchers but to encourage and assist them in better understanding the effects of disinformation, including its influence on local, national and European elections.

- The EU should support member states in creating independent, transparent and accountable regulators who ensure online platforms' compliance with the DSA, in full respect of freedom of expression and information.[31]

Building capacity and resilience of civil society actors facing online threats

- The EU should support CSOs to communicate more effectively so they can build greater understanding and public support for the work they do. The EU should also invest more into digital literacy to ensure that the public has better tools to deal with online threats, such as disinformation, and learn to critically evaluate internet sources.

31 Julian Jaursch, Platform oversight: Here is what a strong Digital Services Coordinator should look like, October 13, 2022

- The EU should urge governments to improve the financing landscape for civil society actors, and devise ways to make EU funding more accessible and beneficial for grassroots civil society actors. The EU should focus its funding in particular on supporting CSOs' capacity building on digital security to enable them to protect themselves from online threats.

Country Reports

BELGIUM

Key Findings:

- Nine out of ten Belgians think that mis- and disinformation is an issue for society. Investigations have shown that they have a considerable impact on public perception of immigrants and asylum seekers.
- Due to their relation and closeness, Belgium is frequently impacted by social issues emerging in France, such as the doxxing regulation (following the Samuel Paty case) or online fundraising rules.
- Over the last few years, Belgium's national data protection authority (APD) has been criticised for its lack of transparency and conflicts of interest. In 2022, two whistleblowers exposed the toxic environment, plunging the institution into a crisis.

Online smear and disinformation campaigns

Online disinformation campaigns are a recurring theme in the Belgian national discourse since 2018.[32] A poll conducted by the media companies VRT and RTBF attested that nine out of ten Belgians think that disinformation is an issue for society.[33]

In October 2021, as part of the European Digital Media Observatory network funded by the European Commission, EDMO Belux was launched, an online platform in five languages that aims to monitor and fight disinformation, in partnership with Belgian media such as RTBF or universities such as UCLouvain.

The spread of misinformation has an impact on the work of associations such as the Fedasil refugees centre.[34] In 2021, la Libre Belgique and De Morgen reported the results of a survey conducted by local officials and the Secretary of State for Asylum and Migration. The results showed that fake news circulating on social media strengthened the reluctance

32 Ministre de l'Agenda numérique, des Télécommunications et de la Poste, Rapport du groupe d'experts belge sur les fausses informations et la désinformation, July 2018

33 Ryckmans G., Près de neuf Belges sur dix estiment que la diffusion de fausses infos est un problème pour notre société, April 1st, 2022

34 RTBF with Belga, Asile et Migration : les fake news sont un frein majeur à l'ouverture des centres d'accueil, November 26, 2021

of inhabitants to have a refugee centre in their vicinity.

Attacks, threats and hate speech online

Attacks, threats and hate speech online are widespread in Belgium and usually target media professionals. According to the annual Media Freedom Monitoring Report,[35] 18 alerts were reported in 2022, involving 23 Belgian journalists and media outlets. Like its neighbours, France and Germany, Belgium media professionals were often the targets of strong opponents to government measures to fight the spread of Covid-19.

Therefore, and despite a relatively high level of trust in the press, Belgian journalists face frequent online threats, especially women,[36] with 11 serious cases reported in 2022. Indeed, six out of ten women aged 15-25 have experienced online harassment, according to the organisation Plan International. Samira Atillah (De Morgen), Myriam Leroy, Safia Kessas, Mryriam Leroy,[37] Cécile Djunga[38] or Johanne Montay[39] (all from RTBF) were the victims of racist or misogynist attacks, death threats, and hate speech online. Men adopting a feminist journalistic angle are also targets of online attacks, as illustrated by Julien Vlassenbroek.[40]

Digital surveillance

Established in 2017 and replacing the Privacy Commission, the Belgian Data Protection Authority or APD (Autorité de Protection des Données) is responsible for monitoring compliance with the basic principles of the protection of personal data,[41] especially when citizens might be under surveillance.

In January 2022, the APD issued a fine against the NGO EU DisinfoLab and one of its researchers[42] for violating the GDPR by collecting sensitive data on political and religious beliefs, ethnic origin, or sexual orientations. The ADP observed a breach of the GDPR related to a massive collection of data, as part of a study aimed at identifying the political orientation of the people at the origin of tweets in the "Benalla affair" in France.

35 Mapping Media Freedom, Monitoring Report 2022, 2023

36 www.rsf.org/fr/pays/belgique

37 Fievet V., L'auteur de harcèlement contre Myriam Leroy, condamné à 10 mois de prison avec sursis, 21 décembre 2021

38 Adam A., Condamnation pour incitation à la haine raciale envers l'animatrice et humoriste Cécile Djunga, April 15th, 2021

39 Keszei N., Johanne Montay harcelée sur Twitter: le RTBF exige des noms, June 17th, 2022

40 Englebert, Injurier par messagerie privée un journaliste relève du harcèlement, June 16th, 2021

41 OneTrust Data Guidance, Belgium - Data Protection Overview, November 2022

42 CNIL, Profilage politique : l'Autorité belge de protection des données prononce deux sanctions après saisine de la CNIL, January 27th, 2022

Data protection and privacy issues

Even though the Belgian government and its agencies are supposed to be the safekeeper of citizens' right to privacy, the APD has recently been under fire for its internal problems, from conflicts of interest to lack of transparency.[43]

In September 2022, two APD directors, Alexandra Jaspar and Charlotte Dereppe, sent a ten-page letter to the Belgian Parliament, stating that the institution had become "unworkable" and "is no longer able to fulfil its mission independently" due to "serious" actions of its president, David Stevens, who was part of the Data Against Corona Taskforce. Under normal circumstances, the decisions of this task force had to be submitted to the opinion of the APD. Jaspar and Dereppe argued that this placed the APD "in an obvious situation of conflict of interest". The two directors made two recommendations: they asked the Parliament to remove the mandate of Stevens and advised the conduct of external audits.

Following this leak, Charlotte Dereppe was put under investigation by the Justice Commission of the Belgian Parliament. Consequently, the Maison des Lanceurs d'Alerte[44] and the European Commission[45] voiced their concerns about how the Parliament treated Charlotte Dereppe.

Doxing

The practice of doxing (the act of publicly divulging personal information about a person - without their consent - on the Internet), has been heavily reported in the Belgian news due to the Samuel Paty case occurring in France in 2020. The infamous case where a teacher in France was brutally murdered, because of an online hate campaign, led to serious discussions in Belgium.

Consequently, Belgium reformed its criminal code to include online harassment[46] in 2021. Therefore, practices such as harassment, sending unwanted explicit photos or doxxing will have the same penalties as offline harassment. This reform follows the EU-wide initiatives implemented from the EU Digital Services Act.

Political advertising

The 2019 elections saw an increasing use of social media by political parties, compared to newspaper advertising. Compared to other

43 Civil Liberties Union for Europe, A bittersweet victory for human rights?, May 2021

44 La Maison des Lanceurs d'Alerte, Conflits d'intérêts au sein de l'Autorité de Protection des Données : la lanceuse d'alerte Charlotte Dereppe écartée par le Parlement belge, July 12th, 2022

45 Benayad M., La Belgique à nouveau épinglée par l'Europe dans le dossier de l'Autorité de protection des données, January 29th, 2023

46 The Brussels Times, Sending unwanted sexually explicit photos now punishable in Belgium, November 25th, 2022

European countries where political advertising starts six months before the general elections, in Belgium, politicians are constantly campaigning online.[47] The Adlens group released in 2020 a report detailing the total expenses of political parties on advertising, and Facebook remains the strong fort where campaign finances are allocated for political ads.[48]

Strategic Litigation Against Public Participation (SLAPPs)

Also called "poursuites-baillons" in French, SLAPPS (Strategic Litigation Against Public Participation) usually target journalists to prevent them from investigating or reporting a story in the public space. De Juristenkrant reported three significant cases in 2022 involving leaders of anti-vax organisations who sued a journalist and two professors over comments on TV.[49]

Cyberattacks

The Federal Cyber Emergency Team (CERT) and the Centre for Cybersecurity (CCB) are the authority in charge of investigating online threats and attacks in Belgium. According to a poll by the organisation Avantdecliquer, Belgian organisations are the number one target of cyberattacks[50] in Europe: the number of cyberattacks in Belgium tripled from 2018 to 2019.

More and more, the insurance market has developed guarantees to associations and public institutions to cover their risks in case of ransomware. Ethias Cyber Security is one of them, working with associations and protecting them from cyberattacks.[51]

In 2022, an association of ethical hackers, BeHack, was launched in Belgium in order to help counter cyberattacks.[52]

Whistleblowers

Since January 2023, whistleblowers in corporations and public institutions are protected by the Belgian law thanks to the transposition of the European directive (2019/1937).[53] Both Acts of November 28th, 2022 (private sector) and of December 8th, 2022 (public sector) will

47 Régulation, En Belgique, les partis sont en campagne permanente sur les réseaux sociaux, July 8th, 2022

48 Touriel A., En Belgique, quels partis politiques ont dépensé le plus en publicités Facebook en 2020?, December 9th, 2021

49 Voorhoof D., Anti-SLAPP: Professor goes free after vexatious and frivolous suit, January 6th, 2022

50 AvantdeCliquer.com, La Belgique, championne européenne des cyberattaques

51 Noulet J-F. with Brichard D. and Hupin B., Après une cyberattaque, comment les entreprises ou collectivités visées sortent-elles du pétrin?, May 16th, 2022

52 Pall E., Une association de hackers éthiques voit le jour à Tournai, en Belgique, September 12th, 2022

53 L'Écho, Les lanceurs d'alerte désormais protégés en entreprise, February 15th, 2023

protect whistleblowers from public disclosure pursued in the public interest. The new rule is timely due to the APD scandal.

Online platforms connected issues

In November 2015, the APD won a lawsuit against Facebook because of the platform's abusive tracking practices.[54] The Belgian authority sued the Internet giant in June 2015 for tracking Belgian users and storing their personal data without their consent. The practices violated Belgian and EU data protection legislation. In February 2015, researchers from the University of Leuven and the Vrije Universiteit Brussel first detected the illegal digital tracking operated by Facebook with specific cookies called "datr".

In Belgium, online fundraising is regulated exclusively by online platforms such as Leetchi or Ulule (platforms also used by the French public). The lack of strict rules or oversight on the platforms has given way to fundraising campaigns deemed controversial. In 2020, the Belgian conspiracy documentary "Hold-Up", claiming to hold the truth about Covid-19, was financed thanks to two fundraising campaigns on Ulule.[55] Alexandre Boucherot, co-founder of Ulule, explained how the documentary producers softened the pitch in order to get the fundraising campaigns validated by the platform. Regulating campaigns deemed controversial might be difficult for the platforms, which received a percentage for each fundraising completed: Ulule received for example 10% of the "Hold Up" fundraising and refused to suspend or cancel it, fearing censorship accusations.

54 Hérard P., Belgique : Facebook condamné pour traque illégale, et ensuite?, November 10th, 2015

55 Laloux P., Sur les sites de crowdfunding, le complot, ça rapporte, November 18th, 2020

CROATIA

Key Findings:

- Croatian SLAPPs cases are an ever-growing challenge. In 2020, there were at least 900 active lawsuits against journalists and media outlets. In recent years, journalists have been under fire for publications posted online, experiencing long SLAPP cases with high court fees.
- The Electronic Media Act was recently established to make users liable for comments or content published online that incites hatred.
- Faktograf is the only fact-checking institute and NGO combating disinformation in Croatia. However, the organisation is under constant attack, experiencing online threats and hacking attacks with no help from Croatian authorities.
- Online threats and attacks are prevalent on social media platforms. Several journalists are subject to harassment, verbal attacks and death threats as a result of their work.

Disinformation

Faktograf is the first and only media fact-checking institute, combatting disinformation in Croatia.[56] The NGO investigates and reports on the credibility of articles published online, measured with objectivity. Faktograf supplies sources for the truthful status of these articles using tools including data collected by civil society, scientific research, expert opinions and official PR statements.

Online smear campaigns

Journalist Anja Kožul of Novosti was the target of a smear campaign and several threats after she published her article, "Islamophobe to state official".[57] The article discussed Arnaud Gouillon, an advocate well known in Serbia for his support of Kosovo Serbs, and his newly awarded position as head of the Directorate for Cooperation with the Diaspora and Serbs. As a result, Kožul received threatening messages on social media platforms, including those from other media outlets and Serbian paramilitary group, the "White Eagles".

56 Šimundić, D., Faktograf: The croatian weapon against fake news, March 17, 2023

57 International Press Institute, Protection needed following smear campaign journalist in Croatia, December 9, 2020

Attacks, threats and hate speech online

Croatian NGOs and journalists have been victim to many threats online. For example, journalist Marcello Rosanda of Glas Istre was the target of insults and death threats on his Facebook page in 2022 as a result of publishing an article that criticised a business.[58] NGO Faktograf has been victim to a multitude of attacks and threats online for ongoing years. The organisation has regularly received threats sent by email, direct messages and social media platforms, none of which have resulted in action being taken against them by Croatian authorities.

Journalist Goran Latković of RTL, who was physically assaulted while reporting on a COVID-19 related protest, was shortly thereafter the victim of multiple online attacks on social media platforms.[59] This came after he reported online about his violent experience at the protest. Because he did not supply video footage, or was able to properly identify his attacks since he was struck from behind, online users accused him of fabricating the story.

Online censorship

The *Electronic Media Act* regulates content issued by users on online platforms.[60] It establishes that those who publish hate related comments under social media posts, for example, are legally responsible for the comments, not the publisher of the platform. The law is aimed at combating hate speech online, allowing the distribution of fines to prevent such comments from happening.[61]

In 2019, Gordan Duhaček of Index.hr was arrested for a satirical post he made on Twitter stating "ACAB", meaning "all cops are bastards."[62] As a result, Duhaček was detained and fined a total of 700 kunas. The Ministry of Interior claimed that this was not a simple case of violating freedom of expression, but rather insulting police officers.

In 2021, the court barred journalists from the online newslite H-Alter from reporting on a public childcare clinic for 30 days.[63] The initial complaint and injunction was filed by Gordana Buljan Flander, who was director of the Polyclinic for Child and Youth Protection of the

58 Hrvatsko novinarkso društvo, Najoštrije osuđujemo prijetnje i uvrede upućene kolegi marcellu rosandi, September 9, 2022

59 Jakubin, H, Reporteru RTL-a sad prijete i smrću: 'Go**o novinarsko, bolje ti je da ne izlaziš iz kuće', November 22, 2021

60 Narodne Novine, Electronic Media Act, https://narodne-novine.nn.hr/clanci/sluzbeni/2021_10_111_1942.html October 14, 2021

61 Freedom House, Croatia: Nations in transit 2022, 2022

62 Committee to Protect Journalists, Croatian journalist detained and fined for satirical tweet, September 23, 2019

63 Committee to Protect Journalists, Croatian court injunction blocks news website H-alter from reporting on public childcare clini, October 8, 2021

City of Zagreb. Flander claimed that H-Alter had previously damaged the institute's reputation. However, the mayor dissolved the clinic's entire board, as they felt it was not appropriate for the institute to request a gag order on a media source. The same day, Flander resigned.

Strategic Litigation Against Public Participation (SLAPPs)

SLAPPs cases in Croatia are a rising concern. In 2020, there were at least 900 active SLAPPs lawsuits against media outlets and journalists, demanding millions of Euros.[64] The majority of these lawsuits are brought forth by politicians, former officials, businesspersons and judges. For example, former agriculture minister Tomislav Tolušić, issued 11 lawsuits against websites Telegram.hr, Index.hr and VIrovitica.net. Tolušić sued these platforms for reporting that the National Conflicts of Interest Prevention Commission was attempting to sue Tolušić for not properly reporting the size of his property. As a result, Telegram.hr was ordered by the court to pay him €4,000 for damaging his reputation.[65]

In 2022, journalist Dražen Ciglenečki of Nova List was convicted in a non-final verdict of damaging judge Ivan Turudić's reputation and was sentenced to pay a fine of 1000 kuna.[66] The case began in 2014 when Ciglenečki wrote an article expressing his opinion that publicly disclosed assessments made by judges have a more damaging impact on the public in comparison to statements made by war criminals. As a result, Turudić sued Ciglenečki for libel. The journalist had to attend trial on three occasions for the case. If the conviction is ultimately finalised, Ciglenečki will be required to pay for the court proceedings and Turudić's court expenses, including his lawyer.

In another instance, businessman Josip Stojanović Jolly issued three lawsuits demanding 6.2 million euros to Telegram.hr, Šibenik In, Šibenik News, and Šibenski Portal, for damaging his reputation.[67] This comes after Telegram.hr published Stojanović's non-final court verdict on their platform, which was then distributed through Šibenik's platforms.

Cyber attacks to IT infrastructure

In 2022, newspaper Daily Slobodna Dalmacija was targeted by a cyberattack. The hackers had reportedly been deleting old articles and replacing them with new articles promoting Russia's invasion of Ukraine.[68]

64 Prtoric, J., Vexatious lawsuits a SLAPP in the face for journalists in Croatia, November 11, 2020
65 Prtoric, J., Vexatious lawsuits a SLAPP in the face for journalists in Croatia, November 11, 2020
66 Croatian Journalists' Association, CJA: Stop the prosecution of journalists, February 4, 2022
67 Total Croatia, HND says HRK 6.2m claim for damages against news portal scandalous, May 11, 2023
68 Slobodna Dalmacija, Izvanredne vijest: izvršen je hakerski napad na portal Slobodne Dalmacije, u naš sustav ubačeni su i objavljeni članci koji šire rusku propagandu, March 22, 2022

In 2021, Faktograf was the target of a DDos hacking attack after entrepreneur and Faktograf critic, Nenad Bakić, started a smear campaign against the NGO. Bakić accused Faktograf of illegal activity and initiated an effort online to fund a lawsuit against the organisation, which stimulated further harassment and more than 27 million attempts to log into Faktograf's portal.[69]

Law enforcement capacity to investigate online threats and attacks

Croatian authorities have been increasingly silent or dismissive about hate speech against journalists in recent years. In one instance in 2018, the District Attorney of Split rejected charges made against an individual who posted death threats under an Index.hr journalist's Facebook post. According to the attorney, the perpetrator was a well known veteran and had made this comment after celebrating his birthday, so he was "taken by emotions".[70]

Whistleblower protection

In 2022, the new *Protection of Reporters of Irregularities Act*, was brought in to ensure whistleblower protection.[71] Although Croatia already had a protection law for reporters in 2019, significant amendments were made to the 2022 act to go beyond the minimum standards.[72] The act now ensures the legal protection of those who report on concepts such as government corruption, privacy and data protection, and money laundering.[73]

69 SEE Check, SEE Check with Faktograf: No public smear campaigns or hacker attacks can intimidate us, December 14, 2021

70 European Federation of Journalists, Croatia: Court rejects charges for death threats against journalists, 2018

71 Civil Liberties Union for Europe, Liberties of Rule Law Report 2023, 2023

72 EU Whistleblowing Monitor, Croatia adopts new whistleblowing law, 2022

73 Narodne Novine, Protection of Reporters of Irregularities Act, April 15, 2022

CZECH REPUBLIC

Key Findings:

- The government plans to criminalise disinformation and financially support media and NGOs who fight disinformation.
- Investigative journalists and activists, particularly those defending LGBTQI+ related causes, face smear campaigns, hate speech, online harassment and online threats.
- Law enforcement has been taking these issues more seriously, as illustrated by a significant increase in investigations and police actions. Many individuals have been charged for supporting the Russian aggression in Ukraine.
- Authorities have blocked several websites that disseminated pro-Russian disinformation. The messenger service Telegram is particularly popular among those spreading pro-Russian narratives and conspiracy theories.

Disinformation

Despite its promises, the Czech government has yet to establish a national legislation to fight disinformation.[74] In 2022, the Interior Ministry drafted a bill that would allow authorities to block disinformation that is deemed to have been intentionally spread and is found to be a threat to security. However, a timeframe on the release or implementation of such a bill has not yet been disclosed, nor has the draft been made public. The implication of the phrase "a threat to security" also remains unclear.[75] This bill has the potential to prevent the spread of disinformation and benefit civil society and the media, as the plan further suggests the allocation of EUR 2 million to NGOs fighting disinformation and EUR 4 million to Czech media.

NGOs are supporting the government in combating disinformation. The organisation, the Czech Elves, for example, are monitoring the media to find hostile influences[76] and have proposed working alongside social media networks to slow the spread of disinformation.[77] The data they are collecting is made available to both authorities and other NGOs.

74 Gosling, T., Czech war on disinformation is still mostly talk, November 9, 2022
75 Zachová, A., Czechia mulls criminalising disinformation, February 6, 2023
76 Kleckova, A. and Nauman, F., Explaining Czech Elves, August 16, 201
77 Gosling, T., Czech war on disinformation is still mostly talk, November 9, 2022

Online smear campaigns

There are several cases of Czech journalists facing smear campaigns, including from politicians. In particular, former Prime Minister Andrej Babiš, owner of the largest media house, has a history of using smear campaigns against journalists.[78] In April 2022, Babiš harassed and attempted to discredit the work of a Czech investigative reporter, Pavla Holcová, by way of claiming she fabricated false Whatsapp messages about his political party. This followed Holcová's reports that Babiš had purchased property in France using offshore accounts, which is currently under a money laundering operation investigation.[79] Once more in September 2022, Babiš continued spreading disinformation in the media when he appeared in newspapers (which he owns) with the caption "Do you believe the media?", in an attempt to build public beliefs that journalists are spreading incorrect information.[80]

Online censorship

Leaked documents listed Czech software supplier company, Jetbrains, as providing censorship services to Russian media monitor, Roskomnadzor (RKM).[81] RKM is Russia's federal agency in charge of controlling and censoring any Russian-language media criticising Putin, the war in Ukraine, corruption investigations and additional information that reflects poorly on the Russian government. Although Russia-based, RKM also monitors individuals of Russian opposition that reside in the Czech Republic - for example, volunteers in Alexei Navalny's team, as well as members of the Prague Russian Anti-War Committee.

Attacks, threats and hate speech online

Online harassment and death threats, particularly aimed at activists and NGOs, have been increasing.[82] In particular, organisations working for the benefit of those in the LGBTQI+ community have faced online hate speech. For example, government officials have suggested that these organisations should not have a right to participate in public debates. They claimed that the community they represent is a danger to society.[83]

78 Oniang'o, M., "If we explain to our readers that we work for them, they'll stand up for us in case of need", January 24, 2023

79 Mapping Media Freedom, Journalist victim of smear campaign.

80 International Press Institute, Czech Republic: The would-be president and the press (that he owns), January 25, 2023

81 Investigace.cz, The Russian censorship office bans words and also blocks Czech media: It is helped by the software of a Czech company, February 23, 2023

82 European Civic Forum, https://civicspacewatch.eu/wp-content/uploads/2022/01/Czech-Republic.pdf, 2022

83 Glopolis, European Civic Forum, Civic Space Watch, Civic Space Report 2023

Hate speech against minority groups online have caught more attention by authorities in recent years. In early 2022, the Czech Supreme Court sentenced an individual to 16 months in prison for writing a hate speech comment online under a photo of children primarily of Roma and Arab descent.[84] The constitutional court stated, "Hate speech on the Internet, as one of the types of hate speech, must be combated in a democratic society, and in serious cases also through the norms of criminal law."[85]

Law enforcement capacity to investigate online threats and attacks

In 2022, police involvement in investigations of online hate speech increased.[86] That year alone, police registered reports of about 700 cases of hate speech on social networks, including the approval of Russian aggression and spreading pro-Russian narratives, such as speaking highly of Russian troops in Ukraine or war crimes.[87] At least 18 individuals were prosecuted for their posts.

Data protection and privacy issues

In 2021, the Czech organisation Iuridicum Remedium criticised the Ministry of Health in an open letter for using Google Analytics on its website. The Ministry decided to switch to a more privacy-friendly tool, Matomo, as a result.[88] Several other government websites followed this example and terminated the use of Google Analytics.

Whistleblower protection

The organisations Transparency International, Rekonstrukce Státu, and Oživení, criticised in a joint statement the first draft law on the protection of whistleblowers, approved by the government in November 2022.[89] According to the organisations, the proposed law has a number of shortcomings, including limitations as to the anonymity of whistleblowers and what type of content can be reported, making it significantly more difficult and dangerous for whistleblowers to expose corruption and fraud. In February 2023, the European Commission announced that it would refer the Czech

84 https://nalus.usoud.cz/Search/GetText.aspx?sz=3-2696-21_1

85 Seznam zpravy, Nenávistné projevy na internetu je třeba potírat, uvedl Ústavní soud, April 1, 2022

86 Glopolis, European Civic Forum, Civic Space Watch, Civic Space Report 2023

87 iRoshlas, Za schvalování ruské agrese si vyslechlo obvinění již 18 lidí. Policie eviduje na 700 oznámení, April 21, 2022

88 EDRi, Czech online state services without Google Analytics: thanks to IuRe, March 1, 2023

89 Rekonstrukce statu, Vláda Petra Fialy (ODS) schválila návrh zákona o ochraně oznamovatelů, který jde naproti korupci, November 23, 2023

Republic and seven other EU member states to the Court of Justice for failing to transpose the European Whistleblower Directive.

Online platforms connected issues

Recent developments in the suspension of online content have created new concerns for overstepping the freedom of expression online. Although formal measures are not yet in place, the National Cyber Operations Centre of the Military Intelligence of the Ministry of Defence had issued a request to unplug several internet service providers that use Czech domains, blocking a series of websites providing pro-Russian disinformation on the war in Ukraine, without legal justification in 2022.[90] The NGOs H21 and Open Society reacted with a joint lawsuit for illegally interfering with disinformation websites. Reasons for this include violations of freedom of thought, freedom of expression, the rule of law and the right to receive information. As a result, a law is now being drafted to clarify constitutional limits for removing websites maintaining disinformation.[91]

Telegram has seen a great rise in accounts spreading disinformation including pro-Russian rhetoric, conspiracy theories and extremist views.[92] The platform has also been used by a variety of politicians, such as a candidate for leadership of Bratislava, Miroslav Heredoš, who is using Telegram to promote the Russian narrative on the war in Ukraine. Radical politician, Lubomír Volný, who was blocked from Facebook for his extremist posts, moved his activities to Telegram.[93] Because Telegram offers similar features, such as public channels and public and private group chats, the platform has attracted many extremists and conspiracy theorist groups.

90 Root.cz, CZ.NIC zablokoval osm domén dezinformačních webů, February 25, 2022

91 Institut H21, Tisková zpráva: Institute H21 a Otevřená společnost žalují ministerstvo za postup při zásahu proti dezinformačním webům, June 7, 2022

92 Investigace.cz, Extremisté na Telegramu posilují. Včetně těch, co propagují invazi na Ukrajinu, March 14, 2022

93 Investigace.cz, Český a slovenský Telegram: Konspirační a extremistická bažina, July 16, 2021

FRANCE

Key findings:

- In 2023, France faced a political and social crisis that started with President Emmanuel Macron's pension reform. The reform, which pushes back the retirement age to 64, caused a national uproar, leading to massive protests. The political crisis reached its peak when the government used Article 49.3 of the Constitution to force the adoption of the pension reform, without a parliamentary vote. Since then, France is facing a democratic crisis as people argue that the Constitution has been misused.

- Since the first election of Emmanuel Macron in 2017, the far-right has risen in France, with chances for Marine Le Pen reaching the presidency in 2027 increasing. The bipolarization of French politics is shared between three forces: the alliance of left-leaning parties (also known as the NUPES), the right-leaning centre party of President Emmanuel Macron (Renaissance and before 2017, En Marche!), and the far-right (monopolised by Marine Le Pen, Rassemblement National, and to a lesser extent, Éric Zemmour's Reconquête). Ahead of 2027, a new force is trying to emerge on the right side: the former Prime Minister Édouard Philippe, with its party Horizons.

- In October 2020, the murder of Samuel Paty, a French secondary school teacher, made the news for several months. Teaching a class on freedom of expression, Samuel Paty showed his students Charlie Hebdo's cartoons depicting the Islamic prophet Muhammad. Some students started an online smear campaign against the teacher, leading to a massive leak of Samuel Paty's personal information online. Following this hate campaign, the professor was killed and beheaded by an Islamic terrorist. The attack awakened Islamic extremism in France, which has experienced similar attacks since 2015 due to the same cartoons. The Samuel Paty case also relaunched the discussion on surveillance, doxxing, and hate speech online.

Online smear and disinformation campaigns

Over the last few years, disinformation campaigns in France focused on Covid-19 and elections. If 2021 was the year of vaccine

disinformation, 2022 was overwhelmed by election fake news.[94] Six French fact-checking organisations reported 169 disinformation (mostly visual) items circulating in France from January 1st to April 30th 2022, the last four months of the French presidential election. The most widespread items were about polarising issues such as immigration, security, and the economic crisis.

Disinformation undermined public confidence in the electoral process and might have affected its outcome. Disinformation had an impact on the online discourse, engorged by fake news. The most notable examples included the claim that 2 million votes for the far-right candidate Marine le Pen had disappeared; the rumour that Yellow Vests were deprived of the right to vote by a 2020 law; or that the QR code on the new voter cards allowed the government to track voters or rig the results. Disinformation around the French elections spread to neighbouring countries (Spain, Germany, and Italy).

Besides the elections, NGOs were also the target of disinformation in 2022, especially organisations helping migrants in the Mediterranean Sea. The likes of the Italian minister Matteo Salvini, France's far-right leader Marine Le Pen and her supporters started online smear and disinformation campaigns by linking the NGOs' humanitarian effort to the activity of smugglers. The disinformation gained momentum when the French Interior Minister Christophe Castaner alluded to the idea that NGOs were even accomplices to smugglers.[95]

Attacks, threats and hate speech online

Hate speech online was heavily discussed in France when the French Parliament decided to regulate "online misdemeanours" from attacks to threats made on the Internet. In 2020, the National Assembly passed the Avia bill,[96] also called the "law against hateful content online." Its goal is to allow social media, the government, and the Regulatory Authority for Audiovisual and Digital Communication (ARCOM) to regulate, counter, and educate together on the topic of hate speech online. In an attempt to strike a balance between freedom of expression and addressing hate speech, legislators chose an overly narrow definition of "online hate speech". The consequence is that a lot of hateful content falls outside the legislative scope, or in the purview of the law.

94 EU Disinfo Lab, What did disinformation look like during the 2022 French presidential election? An overview based on fact-checking articles, June 28, 2022

95 Le Point with AFP, ONG "complices des passeurs": le RN revendique l'antériorité des propos de Castaner, April 7, 2019

96 Vie publique, Loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet, June 29, 2020

Digital surveillance

The extent of this online surveillance is often the subject of public debate, as it might infringe on citizens' right to privacy and personal data protection. In 2021, the advocacy group "la Quadrature du Net" sued - on behalf of 15,000 French citizens - the Ministry of Interior over extensive surveillance.[97]

The normalisation of online surveillance also translates into the real world. LaQuadrature du Net has highlighted the extensive offline and online means of digital surveillance in France: electronic surveillance via street cameras or metadata analysis. With so much power, the French government could use digital surveillance beyond proportion and even justify the mutualization of databases, despite the infringement on the right to privacy.

Data protection and privacy issues

In France,[98] data protection is the competency of the CNIL ("Commission Nationale de l'Informatique et des Libertés"), an authority created in 1978 to address privacy issues. The CNIL's role has been expanded several times, notably in 2018 to incorporate the EU General Data Protection Regulation (GDPR).

Mainly covering the data protection of citizens, the CNIL recently expanded its purview to protect NGOs or associations. In 2021, the CNIL published guidelines regarding data protection and privacy issues for associations,[99] especially regarding their databases.

Doxing

Doxing first emerged in France[100] when grocery store owners disclosed in 2015 the identity of shoplifters online. It has been under scrutiny since 2020, in the aftermath of the Samuel Paty case. Samuel Paty was a French teacher cruelly killed and beheaded for showing Muhammad cartoons in a class on freedom of speech. The murderers were able to track the late teacher because his name and address were uploaded online as part of an online hate campaign. In the aftermath of the case, lawmakers decided to include doxing as a new offence in the law against separatism. Under the "Samuel Paty amendment", doxing is punishable up to three years in prison and a €45,000 fine (art. 223-1-1 of the Criminal Code).

97 Vitard A., Plus de 15 000 personnes poursuivent le ministère de l'intérieur pour surveillance généralisée, September 26, 2022.

98 Cissé S. and Richard C., France - Data Protection Overview, January 2023

99 CNIL, Guide de sensibilisation au RGPD pour les associations, Novembre 10, 2021

100 Péault E., Diffuser les images d'un individu afin de lui nuire : le "doxxing", une pratique qui vient des États-Unis, April 1, 2022

Online campaigning

In 2023, the EU Parliament[101] adopted a position on political advertising regulation, a subject heavily scrutinised in the 2022 presidential election in France. Even though the Internet has been used in French elections since 2007, the Constitutional Council reminded the public[102] of the rules of online campaigning ahead of the 2022 presidential election, where political advertising took over social media platforms and apps (such as ELYZE). The general rule is that both candidates and/or voters are forbidden to campaign online on election day and the day before (campaigning includes sharing polls, political ads, or smearing other candidates).

A notable example during the last presidential election was the use of Facebook by the far-right candidate Eric Zemmour to launch a massive campaign of political ads.[103] The ads were not only against French laws (article L. 52-1 of the Electoral Code) but also against the platform rules[104] because they did not clearly mention the disclaimer "paid by".

Strategic Litigation Against Public Participation (SLAPPs)

The use of strategic litigation against public participation (SLAPPs) is not new in France. The French media mogul, Vincent Bolloré, chairman and CEO of Bolloré Group, has used its influence many times to silence journalists or associations conducting investigations on its businesses. Bolloré extensively relied on SLAPPs to silence the Inrocks for Bolloré's role in the Sarkozy-Kadhafi scandal[105] or the journalist Nicolas Vescovacci for his book criticising Bolloré's business in Africa.[106] Within the last eleven years, Vincent Bolloré has been sanctioned numerous times by French courts for using abusive lawsuits against civil society actors.[107]

Online fundraising

The Autorité des Marchés Financiers (AMF) is the agency responsible for the oversight of crowdfunding activities[108] carried by platforms such as Lydia or Leetchi, the most popular crowdfunding apps in France. But the platforms remain the principal regulators,

101 Killeen M., EU Parliament adopts position on political advertising regulation, February 3, 2023
102 Conseil constitutionnel, La campagne sur Internet
103 Numerama, Les pubs politiques du parti d'Éric Zemmour sur Facebook sont-elles légales?, December 23, 2021
104 Facebook, Introduction aux standards publicitaires
105 On ne se taira pas, Défaite pour la société Bolloré suite à l'action en diffamation engagée contre les Inrocks, September 11, 2020
106 On ne se taira pas, Condamné par trois fois pour procédures abusives, Bolloré ne lâche rien, May 17, 2019
107 Aveline P., Bolloré contre le journalisme : 11 ans de procédures baîllons, March 1, 2021
108 Planet compliance, An overview of the French crowdfunding regulation

with the power to suspend illegal or immoral fundraisings.

In 2019, a controversial fundraising started in Leetchi to support Christophe Dettinger, a boxer who violently beat down two police officers during a Yellow Jacket protest[109] in Paris. Leetchi suspended the fundraising because of its controversial goal, but the platform did not cancel it at the time. Platforms such as Lydia or Leetchi are always cautious of accusations of restricting users' freedom of expression. In the end, the Paris court cancelled the boxer's fundraising page because it was contrary to the public order.

Cyberattacks, including attacks to IT infrastructure, DDoS, malware, phishing and data or identity theft

NGOs' IT infrastructures are targeted by cyberattacks as much as private firms. The Parisian cybersecurity firm Blue Secure[110] works with major French associations (Médecins sans Frontières, Terre Solidaire, or abej SOLIDARITE) to protect them from ransomware or any type of digital attacks such as hacking.

Digital attacks against associations usually target emails and members list, a useful resource also found in other types of organisations, such as political parties. In 2017, the political party of Emmanuel Macron was the target of a cyberattack during the French presidential election.[111] Thousands of the party's emails were leaked just before the second round of the election in order to undermine the nature of the electoral process. The investigation conducted jointly by France and the US pointed to (without confirmation) Russia's role in the "Macronleaks" due to similarities with the hacks which targeted the 2016 US presidential election.

Besides political parties, associations are also the target of cyberattacks. In 2022, the International Committee of the Red Cross servers were targeted by a digital attack compromising the personal data of 515,000 persons around the world.[112] Moreover, in January 2023, the association Appui Santé Nord Finistère was the victim of a digital attack from an unknown perpetrator, preventing it from accessing its archived data and its accounting system.[113] On top of that, all data has been encrypted and some archives deleted, but the attack had no impact on the continuity of the organisation's activity.

109 Le Point with AFP, La cagnotte Leetchi de l'ex-boxeur Gilet jaune Dettinger annulée par la justice, January 6, 2021

110 Blue Digital, À propos

111 Alonso P. and Guiton A., "MacronLeaks", pollution hackeuse, May 7, 2017

112 CICR, "Cyberattaque contre le CICR: le point sur ce que nous savons", February 16, 2022

113 ARS, Cyberattaque de l'Association Appui Santé Nord Finistère : Point de situation, January 30, 2023

Law enforcement capacity to investigate online threats and attacks

Shifting from traditional law enforcement capacity, French police forces embraced the Internet to better regulate it with the most appropriate agencies. Created in 2009, Pharos[114] is the police department in charge of investigating online threats and attacks in France. Recently, Pharos were the focus of public attention following the Samuel Paty case. Before the murder, Pharos received a report that the online campaign started against the teacher.[115] Despite this initial report, Pharos was unable to detect and shut down the litigious online campaign on time, missing the potential chance to prevent the murder.

Pharos is often criticised for its understaffing and inability to fight online hate speech. Pharos received more than 228,545 complaints in 2019, of which more than 25 percent are about terrorist attacks, and 50 percent cover online scamming. Moreover, Pharos has to work hand-in-hand with platforms such as Facebook, Twitter, or Snapchat: therefore, it is difficult to delete hateful content online without the approval of the social media platform.

Whistleblower protection

The EU Whistleblower Directive was transposed into French law in 2022. While the directive does a good job at protecting whistleblowers from exposing corruption and fraud on corporations, there are less safeguards when it comes to exposing state secrets. In 2020, the whistleblower Benoît Muracciole was auditioned by the DGSI, the authority of internal security in France.[116] The president of the association "Action Sécurité Éthique Républicaine" (ASER), Muracciole leaked an internal note regarding the export of French arms to Yemen. The case highlighted the ambiguous stance of France regarding its military industry with ambivalent foreign countries. Whistleblowers are sometimes interrogated and watched by French secret services when they feel that the national interest is in danger.

New security measures that may affect civil society actors

Traumatised by the multiple attacks the city suffered in 2015 and 2016, Paris never lowered its security levels it built after the Bataclan terrorist attacks.

Therefore, the Olympic Games in 2024 will be the subject of a new type of surveillance, justified by the fear of potential terrorism in Paris. The minister of sports, Amélie Oudéa-Castéra,

114 Rousset A., Haine en ligne : la plateforme de signalement Pharos en cinq questions, October 20, 2020
115 Le Point, Le compte Twitter du meurtrier de Samuel Paty signalé à plusieurs reprises, October 23, 2020
116 Le Média, Lanceur d'alerte: menacé par les services secrets, February 26, 2020

proposed a security/anti-terrorist bill in December 2022 to use increased and improved digital surveillance (or algorithmic surveillance) for the 2024 Olympic Games. Algorithmic surveillance aims to analyse images and crowds by machine and not by humans. The human eye is replaced by algorithms in charge of detecting any alarming situation, prompting a police intervention.

Defending the nature of this new digital surveillance, the minister reassured that the technologies will be temporary, but some already fear that measures could become permanent once the Olympics are over, or start being used well before 2024.[117] The National Assembly adopted the bill in March 2023 and the Constitutional Council confirmed this bill in May 2023.

Online platforms connected issues

Social media platforms regularly ban or censor content they deem illegal. In 2021, the French city of Bitche's Facebook page was suspended because it was confused with the English derogatory word bitch.[118] While this might generate a few laughs, some arbitrary bans target freelance journalists or independent media because of the nature of their content. In April 2021, "Cerveaux Non Disponibles" and "La Relève et la Peste" accounts were suspended because both media shared political content and actions from activists (feminist protests in Mexico).[119] Facebook never explained why the accounts were suspended, even though they did not violate Facebook's terms of use on terrorist or dangerous and illegal content. What is more, the Extinction Rebellion France, an environmental group using civil disobedience as means of protest, suffered the same fate in 2020. In 2016, the antiracist collective the "Collectif contre l'islamophobie en France" (CCIF) had already been banned.[120]

117 France info, Vidéosurveillance, scanners corporels, contrôles antidopage génétiques… Ce que contient le projet de loi JO 2024, January 1, 2023

118 Le Point with AFP, Moselle : une ville censurée par Facebook à cause… de son nom!, April 13, 2021

119 Debove L., Facebook censure petit à petit les médias indépendants, une menace pour la démocratie, June 16, 2021

120 La Quadrature du Net, Sur Facebook, les militant.e.s antiracistes victimes de censure, September 5, 2016

GERMANY

Key findings:

- Right-wing populists and extremists engage in attacks and disinformation campaigns against civil society organisations (CSOs), discrediting them through conspiracy theories and right-wing ideologies on social media. During the Corona pandemic and German federal elections, CSOs faced false accusations and mischaracterization, contributing to the erosion of trust in the electoral process.
- Germany has implemented laws such as the Network Enforcement Act (NetzDG) to regulate online violence and hate speech, with hefty fines for online platforms for non-compliance. However, investigations are rare.
- German authorities possess spyware like Pegasus, but there are no reported cases of state surveillance on civil society organisations, journalists, or activists.
- Far-right groups maintain "enemy lists" targeting activists, journalists, and artists, prompting legal amendments to punish doxing and the publication of such lists. However, challenges persist in investigations, prosecutions, and accountability due to reliance on law enforcement data and anonymous social media accounts.
- There have been isolated cases of arbitrary online censorship by law enforcement authorities.
- While there is a strong legal framework to combat online hate, enforcement is lacking, with investigations and prosecutions remaining exceptions. Law enforcement authorities are inadequately trained in media skills, lack awareness of digital violence, and often do not consider online violence a serious issue.
- Challenges and controversies in regulating online platforms persist. The NetzDG has been criticised over its impact on free speech. Social media platforms, such as Meta, Twitter and TikTok, are struggling with disinformation, moderation practices, and transparency concerns.

Online smear and disinformation campaigns

Civil society organisations (CSOs) are regularly attacked, smeared and defamed by right-wing populists and extremists, who promulgate conspiracy theories and right-wing ideologies on blogs and social media platforms. Disinformation campaigns targeted at CSOs with

different opinions serve to discredit, stigmatise and question their entitlement to public funds.

In particular during the Corona pandemic, floods of false information entered the German digital space. The anti-lockdown movement, fuelled by the right-wing Alternative für Deutschland (AfD) party, accused the media and NGOs of lying and the government of manipulating COVID-19 data to exaggerate the severity of the pandemic and justify restrictions.[121]

Online disinformation was also an issue throughout the German federal elections of September 2021. Parties' programs were mischaracterized, and candidates intentionally misquoted.[122] The AfD also copied the voter fraud narrative utilised by the Republican party in the United States during the 2020 elections. And, as Julian Jaursch from the think tank Stiftung Neue Verantwortung notes, even if it had little success, it contributed to undermining the trust in the electoral process.[123]

Another notable example was a disinformation campaign against the anti-racist organisation Amadeu Antonio Foundation in 2019. The foundation was accused of being a left-wing extremist organisation and promoting censorship of conservative voices.[124]

Attacks, threats and hate speech online

Online violence in Germany is regulated by a series of laws. The most relevant is the Network Enforcement Act (NetzDG), which came into effect in October 2017. The NetzDG requires social media platforms with more than two million registered users to remove "obviously illegal" content within 24 hours of being notified. This includes hate speech, defamation, and incitement to violence. Failure to comply with the NetzDG can result in hefty fines of up to €50 million.

Furthermore, section 130 of the German Criminal Code, applicable both offline and online, prohibits inciting hatred against a group based on national, racial, religious, or ethnic identity. It also forbids insulting, ridiculing, or defaming such groups in a manner that could cause social unrest.

For a very long time, victims of violent and hateful comments were left alone by authorities. For example, the application in September 2019 by the politician Renate Künast to a Berlin district court to release the data of people who threatened her on social media was initially rejected, causing a stir at the time.[125]

121 Joswig, G. Wenn die AfD über Leichen geht, https://taz.de/Desinformation-in-der-Coronakrise/!5824346/ December 29, 2021

122 Wipfler F. #Faktenfuchs: Falsches Laschet-Zitat kursiert auf Twitter, July 6, 2021

123 Jaursch J. Disinformation in the 2021 German Federal Elections: What Did and Did Not Occur, October 5, 2021

124 Reinfrank T. and Lüdecke R. Civil society demonised May 28, 2019

125 Renate Künast later won the appeal, with the help from HateAid

Online threats and hate speech also sometimes serve as a precursor to physical hate crimes. In an event that shocked the nation, local politician Walter Lübke was murdered in 2019 by a neo-Nazi, presumably because of his support for refugees and immigrants. Hate-filled content targeted at the politician had previously circulated on right-wing online forums.

In 2021, as a result of these (and other) events, the government took new measures to fight hate speech, by tightening penalties and forcing social media platforms to report serious hate crimes to the Federal Criminal Police Office, which should lead to faster and more effective investigations.[126]

To this date, there are many people who have been fined for posting illegal content online, including public calls for crimes, incitement to hatred, depiction of violence, insults or slander.[127] Hostile narratives against the LGBTQI+ community and immigrants remain the main topic in right-wing online groups, with numerous memes and hate messages circulating uncommented on the net.

Civil society in Germany plays a big role, helping victims of hate speech, monitoring the web for attacks and threats, reporting them to law enforcement authorities and educating people about hate speech and how to protect themselves from it.[128]

However, despite increased awareness, digital violence and hate speech is only rarely investigated. People often don't know about legal measures or lack trust in authorities.

Digital surveillance

While German law enforcement authorities are in possession of spyware, such as Pegasus, there are no reports of state surveillance into CSOs, journalists or activists. However, German authorities do use their tools for other purposes.

Following a complaint by a group of civil society and media organisations at the Federal Constitutional Court, the latter declared that the Federal Intelligence Service's (BND) practice of monitoring worldwide internet traffic violates the fundamental right to privacy of telecommunications, protected by the German Constitution. The BND law lacks sufficient protection for vulnerable groups such as journalists and does not set high enough hurdles for targeted surveillance of individuals abroad.[129]

During online exams, the University of Erfurt, like many other universities, uses automated face recognition and spyware to monitor the participants' computers. An affected student, together with the GFF and the Free

126 Bundesministerium der Justiz, Gesetzespaket gegen Hass und Hetze ist in Kraft getreten, April 1, 2021
127 No Hate Speech Movement
128 Klicksafe
129 Gesellschaft für Freiheitsrechte, BND law on worldwide mass surveillance

Association of Student Unions (FZS), is suing against this so-called proctoring software.[130]

Doxing

In 2019, personal data of hundreds of German politicians, journalists and celebrities were leaked on Twitter.[131] The leaked content included private information such as email exchanges, holiday pictures, telephone numbers, bank statements and credit card details. The police arrested the person behind the leaks,[132] and he was sentenced to nine months of youth imprisonment on probation. His Twitter account was suspended.

Far-right groups, such as Nordkreuz, or the terror group NSU, have kept so-called "enemy lists" with tens of thousands of people, including addresses of activists, journalists and artists who are active against racism. Walter Lübcke was on such a list before he was murdered.

In 2021, the German Criminal Code was amended to punish doxing and the publication of enemy lists, containing potential targets. However, shortcomings remain. Enemy lists are often relying on data provided by law enforcement, and investigations into right-wing networks are lacking. Prosecutions for sharing private data and enemy lists remain inadequate. Furthermore, anonymous social media accounts make it challenging to hold doxers accountable due to legal constraints.

Online censorship

In March 2023, the far-left media platform linksunten.indymedia, which was banned in 2017 by the Federal Interior Ministry for its extremist content, lost a five-year-long legal battle[133] as the Federal Constitutional Court (BVerfG) did not accept its complaints.[134]

A few months earlier, in January 2023, the police raided the homes of two journalists and the office of the independent non-profit radio station Radio Dreyeckland because they had published an article in summer 2022 which covered the legal proceedings against linksunten.indymedia and contained a link that led to the website of the platform.[135] A regional court later decided that the linking was part of the journalistic task and did not constitute criminal support. It declared the searches unlawful and ordered the police to delete the seized data carriers.

130 Fuest P., Gemeinsame Klage gegen Gesichtserkennung an der Uni Erfurt, October 20, 2022

131 Steinlechner P., Persönliche Daten Hunderter Politiker offen im Netz, January 4, 2019

132 Bundeskriminalamt, Festnahme eines Tatverdächtigen im Ermittlungsverfahren wegen des Verdachts des Ausspähens und der unberechtigten Veröffentlichung personenbezogener Daten, 2302 January 8, 2019

133 Nowak P., Indymedia Verfahren eingestellt, August, 1, 2022

134 Nowak P., Indymedia vor Gericht gescheitert, March 21, 2023

135 Committee to Protect Journalists, German police search office of independent broadcaster and 2 journalists' homes, seize equipment and documents, January 19, 2023

In May 2023, the Bavarian State Criminal Police Office (LKA) confiscated the website of the climate activist group "Letzte Generation" and redirected it to a website of the Bavarian police, on which a notice was displayed saying that the Letzte Generation is a criminal organisation. The LKA later admitted to having made a mistake in seizing the domain of "Letzte Generation". It also apologised for calling the group a "criminal organisation", which is the competence of the General Prosecutor, not the police.

Digital attacks to IT infrastructure

The Federal Office for Information Security (BSI) is responsible for monitoring disinformation and cyber threats to national security. It operates a "situation centre" that monitors social media and other online sources for disinformation campaigns and works with other government agencies to develop countermeasures.

Law enforcement capacity to investigate online threats and attacks

There is a strong legal basis on which law enforcement authorities can act against online hate. The last federal government with the then Minister of Justice Christine Lambrecht pushed ahead with a large legislative package, where criminal offences such as threats of rape or so-called enemy lists were added.[136] However, enforcement of the law is lacking. There have been investigations and prosecutions, but they remain the exception.

In February 2022, after the violent murder of two police officers in Rhineland-Palatinate, the LKA set up its own "Hate Speech" investigation group, composed of 14 experts. The group identified 399 cases of online threats and hate speech against the police, of which 102 posts are criminally relevant. Investigators across the country regularly search the homes of suspects, confiscating data carriers such as smartphones, notebooks and other digital devices. A total of 150 suspects are currently being investigated in 172 criminally relevant cases.[137]

There are many initiatives[138] that have been set up by various stakeholders aimed at countering disinformation and online threats. The initiatives come from political parties, the government and public institutions, the media, civil society and also from big online platforms. For example, the NGO HateAid campaigns for the rights of those affected by digital violence

136 Linß V, Böttcher M., Ist das Netz ein rechtsfreier Raum?, November 12, 2022

137 Tagesschau, Bundesweite Razzien nach Hasskommentaren, June 20, 2022

138 Miguel R., The battle against disinformation in the upcoming federal election in Germany: actors, initiatives and tools, September 24, 2021

and has already supported lawsuits against major online platforms on several occasions.[139]

However, law enforcement authorities are still insufficiently trained in appropriate media skills and lack awareness of digital violence and the functioning of social media. There is a lack of resources to train law enforcement. A media report from May 2022 also shows that police officers often do not see online violence as a serious issue.[140]

Online platforms connected issues

In Germany, the primary law that regulates illegal content on online platforms is the Network Enforcement Act (NetzDG). It has been controversial since its introduction, as some argue that it threatens free speech and puts too much power in the hands of private companies.

The Federal Office of Justice (BfJ) is in charge of enforcing the NetzDG, which includes punishing those who violate its rules. In 2023, it initiated fine proceedings against Twitter for repeated failures to delete illegal content, despite numerous complaints by users of the social media platform.[141] The BfJ has also imposed a fine of more than five million Euro on the messaging app Telegram, because Telegram failed to create a means for users to report illegal content, and because the company did not have a representative office located in Germany to receive official communication.[142] Telegram is believed to be increasingly used as a medium for radicalization. As a reaction, Germany's Federal Criminal Police Office has created a task force[143] to investigate individuals suspected of committing crimes using Telegram.

Social media platforms play a major role in fighting disinformation online. In November 2022, the District Court of Frankfurt ruled that social media platforms such as Facebook and Twitter must take an active role in preventing the spread of false information and disinformation.[144]

During the 2021 federal elections, Facebook announced security measures to tackle disinformation.[145] TikTok on the other hand struggled to fight disinformation, failing to properly label political content, implement its

139 Hate Aid

140 ZDF Magazin Royale, Wo die deutsche Polizei bei der Verfolgung von Straftaten im Internet versagt, May 27, 2022

141 Reuters, Germany starts fine proceedings against Twitter over user complaints, April 4, 2023

142 Legal Tribune Online, 5,1 Millionen Euro Bußgeld gegen Telegram, October 17, 2022

143 Associated Press News, Germany: Telegram becoming a 'medium for radicalization', January 26, 2022

144 Leber S., Prozess um Hasskommentare auf Twitter, November 24, 2022

145 Cerulus L., Facebook promises to ramp up security for German election, May 10, 2021

fact checking project and delete or ban fake accounts.[146]

Facebook deleted nearly 150 accounts, pages and groups in September 2021 as a result of disinformation linked to the Corona pandemic.[147] It was a controversial move that drew criticism from digital activists, who believe that social media platforms should not have the power to censor citizens' voices, even those which are anti-democratic.[148]

The criticism is well-founded, as some actions by the social media giant are questionable, to say the least. For example, in December 2021, the Facebook account of the NGO Filmwerkstatt Düsseldorf was deleted, presumably due to the publication of a thumbnail for the documentary The Shaman and the Snake.[149] The picture shows several indigenous people wearing only loincloths (thus arguably violating anti-nudity rules). According to the Filmwerkstatt Düsseldorf, Facebook deleted the page without warning, and did not send the NGO a reason why their account was deleted. The NGO filed a lawsuit against Facebook for the deletion of its account, criticising the arbitrariness and lack of transparency in the company's moderation decisions.

In 2021, there was already a ruling of the Federal Court of Justice (BGH) which criticised Facebook for not informing users about the reason why their account was shut down or their post deleted.[150]

Properly understanding the impact social media platforms have on civic space is also made difficult because Facebook and other social media companies are opaque. In 2020, the Berliner NGO Algorithm Watch launched an Instagram monitoring project. People could voluntarily share their data to Algorithm Watch by installing a browser add-on that would scan their Instagram newsfeed. The purpose of the project was to see how politicians interact with people on Instagram and answer the question - do social media platforms polarise political discourse, promote disinformation and fuel hate speech? However, after Facebook, which owns Instagram, threatened legal action, the NGO had to shut down the project.[151]

In another case, Facebook blocked the page of the Hamburg-based NGO Goliathwatch in February 2022. The NGO campaigns for limiting the power of large corporations like Facebook. Facebook did not inform Goliathwatch in advance and the reasons for the block were vague: the company accused Goliathwatch of

146 Bösch M., Ricks B., Broken Promises: TikTok and the German Election, September 2021
147 Deutsche Welle, Facebook deletes accounts of German anti-lockdown group, September 16, 2021
148 Reuter M., Massenlöschungen sind kein Grund zum Jubeln, September 17, 2021
149 Rudl T., Filmwerkstatt Düsseldorf zieht gegen Facebook-Sperre vor Gericht, April 13, 2023
150 Busvine D., Top German court strikes down Facebook rules on hate speech, July 29, 2021
151 Kayser-Bril N., AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook, August 13, 2021

disseminating "fraudulent" and "misleading" information.[152] The NGO Gesellschaft für Freiheitsrechte (GFF) initiated legal protection procedures, resulting in the page being accessible again. However, the GFF, Goliathwatch, and the law firm Hausfeld are pursuing legal action to prevent arbitrary blocking in the future.[153]

The Hamburg Regional Court ruled that the blocking was unlawful, but denied future injunctions due to lack of specificity. However, the Hanseatic Higher Regional Court established that stringent requirements must be met before a page can be blocked, including a hearing, reasons for the block, and a factual and objectively verifiable justification. The court's decision is seen as a victory for freedom of expression and strengthens the rights of NGOs and companies against social networks. The court also stated that Facebook cannot avoid penalties by not providing reasons for the decision to block.

It's not just the big social media platforms that apply EU rules in a questionable manner. The NGO Netzpolitik analysed Germany's 100 most-visited websites for dark patterns and found that four out of five rely on manipulative cookie banners,[154] violating the GDPR.

152 Goliathwatch https://goliathwatch.de/facebooksperre/

153 Gesellschaft für Freiheitsrechte

154 Reuter M., Dachwitz I., Seifert T., Miese Tricks und fiese Klicks, September 1, 2022

HUNGARY

Key Findings:

- There is no legislation to limit political advertising in Hungary. Consequently, a third of the government's ad revenue is spent on political campaigning on Facebook.
- NGOs in Hungary are the subject of constant attacks and threats by Hungarian government actors. Multiple journalists and civil society organisations face smear campaigns, threats, harassment and doxing. Additionally, disinformation campaigns against women politicians advocating for democracy have been increasing.
- State administered surveillance has been increasing in Hungary. The Orbán regime used Pegasus spyware on hundreds of journalists' phone numbers for monitoring, accessing personal information such as emails, texts and photos.
- The State has controls, including censoring information online. In 2021, this included the ban of information pertaining to homosexuality or LGBT content in any advertising, films and sex education programs.

Disinformation

For many years, the public service media in Hungary has given up pretending to be unbiased, including in its coverage of the Russian war against Ukraine. In 2022, state-owned public service media, *Duna Média*, became a main source of pro-Russian propaganda.[155] Like many other state-owned media providers, *Duna Média* does not provide alternative viewpoints or context to the issues presented, neglecting to give viewers a properly informed report. Meanwhile, the Hungarian government has failed to place any sanctions on Russian sources or limit the spread of Russian narratives, while advertising and promoting conspiracy theories that minimise Russian aggression.[156]

Online smear campaigns

Online smear campaigns against journalists and civil society organisations (CSOs) have been increasingly used by government officials and politicians in Hungary in recent years. In 2022, a smear campaign against journalists

155 Hungarian Civil Liberties Union, Russian disinformation in hungarian public broadcast media: complaint to the european commission, March 29, 2022

156 Bayer, L., Hungary has become the EU home of Kremlin talking points, March 9, 2022

was published by a pro-government newspaper, *Magyar Nemzet*. The newspaper posted secret recordings of journalists' job interviews that had been spliced and edited to distort their conversations[157] and discredit the journalists.[158] Government spokesman Zoltan Kovacs then supported these fabricated videos on a government website. Additionally, Prime Minister Viktor Orbán responded to and endorsed the false conclusions made from these videos, and the Hungarian government later posted these distorted videos on YouTube.

In 2023, non-profit investigative media outlet Átlátszó was victim to an online smear campaign by pro-government news outlets run by Fidesz.[159] Átlátszó was accused of being a criminal organisation and of working for foreign interests, making them a national security risk. The attacks came after Átlátszó launched an investigation into the Orbán government's distribution of millions of Euro spent at Hungarian minority organisations in neighbouring countries to maintain influence and power abroad.

Attacks, threats and hate speech online

NGOs in Hungary often face threats and hate speech online, particularly on social media.[160] These organisations also receive death threats on the phone and through email. Many of these online attacks are government-led, carried out by state officials.

#Shepersisted, an initiative combating disinformation against women in politics, journalism and activism, found that big tech companies have failed to fight gender based disinformation against women in politics on social media platforms. Women political activists calling for democracy and human rights in Hungary have been increasingly attacked online by the government, which has attempted to portray them as untrustworthy, destroyers of conservative values, and maintaining ties with George Soros.[161] Attacks have taken the form of doxxing, disinformation campaigns and online harassment.[162]

157 Human Rights Watch, Hungary: Smear Campaign Targets Critical Voices, March 4, 2022

158 Civicus Monitor, Hungary: Overview of recent restrictions to civic freedoms, 2022

159 International Press Institute, Hungary: Investigative media Átlátszó targeted in latest smear campaign, January 24, 2023

160 Amnesty International, Hungary: Living under the sword of Damocles – The impact of the LEXNGO on civil society in Hungary, April 9, 2021

161 Di Meco, L. and Hesterman S., A perfect propaganda machine: A #ShePersisted Analysis of Gendered Disinformation and Online Abuse Against Women in Politics in Hungary March 2023

162 Martirosyan, L., Hungary's 'perfect propaganda machine' attacks women, report finds, March 22, 2023

Digital surveillance

State administered digital surveillance has been increasing in Hungary. In 2021, the Orbán regime used the Pegasus spyware to monitor more than 300 Hungarian phone numbers, including those of journalists and activists.[163] The spyware allows complete access to personal items such as emails, communications and photos, in addition to phone call audio. Additionally, the Hungarian government had a list of fifty thousand phone numbers in a database in over fifty countries linked to foreign civil society members. It is unclear if all of these were wiretapped, or simply on a stand-by list to possibly syphon information later.

Domestic laws in Hungary do not require that individuals are notified if they are under digital surveillance. This gives the government full power to monitor anyone they deem necessary.[164] For example, government representative Szilárd Németh attempted to justify surveillance of local NGOs, claiming that the institutions are "foreign agents" with the goals of undermining the government.[165] With no safeguards in place, individuals are unable to determine if they are being monitored and are therefore unable to challenge said monitoring. This undermines the digital privacy protections the European Union has in place.

Data protection and privacy issues

In the 2022 elections, the ruling party Fidesz misused personal data (email address), taken from documentation including Covid vaccine registration and tax and public services administration, for the party's political campaigning.[166] Fidesz largely used Facebook in particular to profile its users and advertise during the campaign to target potential Fidesz supporters. This targeting further influences public discourse and creates unfair elections, as only Fidesz has extensive access to personal data to use, whereas opposition parties do not. Additionally, using sensitive data for political advertising purposes can dissuade the public from voting in elections for fear that their data is not being properly managed. Such heavy government use of Facebook data may also prevent civil society from using social media platforms for personal or political expression.

New security measures that may affect civil society actors

During the Covid pandemic, prime minister Viktor Orbán declared a state of emergency and issued a bill that allowed ruling by decree. The government also established a criminal law presenting jail time of five to ten years

163 Birnbaum, M., In Orban's Hungary, spyware was used to monitor journalists and others who might challenge the government, July 19, 2021

164 Digital Freedom Fund, Secret, targeted surveillance in Hungary

165 Szabó, D., Mire használja németh szilárd a titkosszolgálatokat?, March 14, 2017

166 Human Rights Watch, Trapped in a Web The Exploitation of Personal Data in Hungary's 2022 Elections, December 1, 2022

for spreading what the government deemed 'false information' or 'distorted truth' on the pandemic.[167] However, these vague terms were never further detailed. As a result, any journalists releasing related information could be deemed as spreading disinformation by the government. Additionally, official institutes such as hospitals and ministries had to first give their information to the government for review before announcing pandemic related news to the press. Journalists were also banned from entering hospitals or speaking to physicians, unable to inform the public of any developments.[168] After the court found that the Ministry of Human Resources is not eligible to ban journalists from the hospitals,[169] the government issued a decree giving authority to the Operational Staff on the rules of entering hospitals as a journalist.[170] When Orbán eventually lifted the state of emergency for the pandemic, another was issued for reason of the war in Ukraine, allowing him to maintain his emergency powers.[171]

Online censorship

Hungary does not maintain any laws in regards to online censorship. Instead, the government at times distributes court orders and applies state pressure to encourage all online content publishers and hosts to delete content.[172] Despite this, in 2021, lawmakers approved a bill banning LGBT content from minors in school sex education programs, advertisements and films, including anything related to homosexuality or gender reassignment.[173] NGOs whose mission is to support the LGBT community and educate the public on LGBT matters, such as the Labrisz Lesbian Association, have experienced online attacks and hate speech. Pro-government newspaper *Magyar Nemzet* published an article accusing the Labrisz Lesbian Association of being a "paedophile organisation".[174] However, as a result of a judicial review, the appeals court later deduced that *Magyar Nemzet* did not ruin the organisation's reputation by making these claims and the newspaper went unpunished.

According to the Hungarian government, all online media service providers maintain "editorial responsibility" if they intend to

167 Keller-Alant, A., Hungary Censoring Information on COVID-19, Report Says, April 27, 2020
168 Dunai, M., Hungarian journalists say state conceals impact of world's deadliest COVID-19 outbreak, March 31, 2021
169 Szalay, D., Jogerős: jogtalanul tiltotta ki a minisztérium a sajtót a kórházakból a járvány idejére, February 2, 2022
170 Portfolio, Villámgyorsan reagált a kormány az elbukott bírósági ítéletre, February 4, 2022
171 Deutsche Welle, Hungary's Orban extends emergency powers, points to Ukraine, May 25, 2022
172 Freedom House, Hungary: Freedom on the net 2021, 2021
173 France 24, Hungary's controversial anti-LGBT law goes into effect despite EU warnings, July 7, 2021
174 Zalan, E., Budapest ruling seen as normalising anti-LGBT sentiment, February 3, 2015

publish information for purposes including entertainment, training or spreading information. However, Hungarian law does not define "editorial responsibility".[175] It further does not express if publications made on online platforms consequently maintain legal liability. Online media outlets are pressured to post content only regarded as 'politically safe', including information on potential government corruption, and many comply out of fear of legal repercussions.[176]

In 2020, due to Covid-19, the government's new policy was to release non-Covid patients to make more room for those suffering from the virus. As a result, some citizens were arrested and detained after they criticised the policy and local hospitals on social media. Police investigated these cases under new state-of-emergency legislation for "false information" and therefore endangering the public, but the citizens in detention were released within a short time and they did not have to face legal consequences.[177] This is an extension of a previous law that allows authorities to silence "alarmist comments".[178]

Doxing

Hungarian journalist András Pethő of the NGO Direkt36 fell victim of doxxing by hand of Hungarian government sponsored entities.[179] Direkt36's missions is to conduct detailed corruption investigations in order to hold high ranking officials accountable for their actions. A government-controlled magazine published a list online, labelled 'George Soros Mercenaries'- Pethő's name was on this list among with other NGO-coworkers, academic professionals and activists without any further context.[180] This label affiliates those on the list as enemies of the state, as Hungarian-American businessman George Soros himself has been deemed as an enemy of Hungary by the Hungarian government.[181]

Online political advertising

In Hungary's current legislation, there is no limit to online political advertising spending on social media platforms.[182] Therefore there is no limit to how much the government can spend on advertising for election campaigns. Megafon, a pro-government company fund,

175 Hungarian Media Law, Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules of Media Content

176 Selva, M., Fighting Words: Journalism Under Assault in Central and Eastern Europe, January 2020

177 Bod, T., Rémhírterjesztésért bevitték a gyulai ellenzéki kör helyi vezetőjét, a Momentum tagját, May 13, 2020

178 Sandford, A., Hungary: 'Critics silenced' in social media arrests as EU debates Orban's powers, May 15, 2020

179 Crowley, J., Doxxed journalist reveals perils of working in Hungary's hostile media environment, October 15, 2019

180 Crowley, J., Doxxed journalist reveals perils of working in Hungary's hostile media environment, October 15, 2019

181 Michalopoulos, S., Hungarian MEP: Orbán targets Soros because he is 'the perfect enemy', February 21, 2018

182 Hanula, Z., Orban's influencers shower cash, become largest social media spenders, January 4, 2022

has accrued over €1.3 million spent during last year's elections. The Hungarian government comes in second at €1.2 million spent and the Fidesz party third, spending €0.9 million. The three together make up about a third of Facebook's Hungarian ad revenue. Megafon initiated several press rectification processes against the news site Telex.hu which claimed that public sources are channelled to Megafon. Megafon lost these trials.[183]

Strategic Litigation Against Public Participation (SLAPPs)

In recent years, the GDPR has been misused to discourage news coverage in Hungary.[184] GDPR related litigation has been used as a tool to silence critical voices. Plaintiffs have claimed that their personal data is used unlawfully by journalists and that their data has been processed without their consent.[185] Recently, the Constitutional Court found that creating lists of dominant business persons without their consent infringes the law.[186]

In 2017, journalist Júlia Halász from the independent news website 444 was forcibly removed from a Fidesz community meeting and was subsequently stripped of her phone.[187] One of the meeting's organisers then deleted all photos she took of the event. Upon filing a complaint with the court, the investigation was dropped for a lack of evidence. After Halász wrote an article detailing her experience, a Fidesz politician sued her for defamation. Halász was found guilty of criminal defamation after a five years of investigation and court proceedings.[188]

Cyber attacks to IT infrastructure

In April 2023 several media websites were targeted with distributed denial-of-service (DDoS) attacks, temporarily crashing their websites. Seven media outlets were affected, namely 444.hu, hvg.hu, Nyugati Fény, Ellenszél, Ellenlábas, Balramagyar, Hírhugó.[189] Most of these media are independent and critical of the government.

183 Bozzay, B., A Megafon beperelt minket, de a Telexnek adott igazat a bíróság, January 28, 2022

184 Bodrogi, B., Case Study: SLAPP in Hungary, January 2023

185 Hungarian Civil Liberties Union, GDPR weaponized – summary of cases and strategies where data protection is used to undermine freedom of press in hungary, November 23, 2020

186 Farkas, G., Gazdaglistás tiltásról döntött az Alkotmánybíróság, April 28, 2023

187 Committee to Protect Journalists, Hungarian court convicts reporter Júlia Halász on criminal defamation charge, May 28, 2021

188 Bodrogi, B., Case Study: SLAPP in Hungary, January 2023

189 Media 1, Egy másik, a magyar kormányt kritizáló lap felfedte, hogy működését megbénították a hackerek, April 17, 2023

Law enforcement capacity to investigate online threats and attacks

In 2019, a police hate crime protocol was established to improve hate crime investigations. This includes a selected individual in a mentorship position at each local police unit in the nation to oversee police trainings.[190] Initiatives to investigate bias-motivated crimes have also been established.[191] Additionally, the Victim Support Service, which includes services for victims of hate crimes, offers a help-line providing victims assistance tailored to their specific needs. Despite these developments, very few cases of hate speech have been charged, let alone cases of hate speech online.[192]

Unofficial data related to online hate speech is collected by CSOs. In 2022, the EU Commission's sixth evaluation of the Code of Conduct on Countering Illegal Hate Speech Online reported 108 cases of online hate speech- only about 36% of which were actually removed by the overseeing social media platform. Despite the police hate crime protocol's implementation, xenophobic laws have minimised the efforts combating hate speech such as those targeting the LGBT community, refugees, Muslims and asylum seekers.

Online platforms connected issues

In 2021, Hungary's chief of data protection, Attila Péterfalvi, suggested a new law, the 'Facebook Act', that would allow Hungarian authorities to review banning decisions made by Facebook.[193] Péterfalvi expressed that the requirement to show personal documents to reactivate a suspended Facebook profile constitutes a breach of data protection. Although Facebook follows European regulations, Péterfalvi suggested a new regulation for Hungary's use of the platform. However, there have been no details clarified regarding account management and who may and may not access Facebook. This further strikes concern of potential threats to freedom of expression, as state interference of social media content may sway social media platform managers to remove all content that could possibly be considered as sanctioned.[194]

190 Council of Europe, Hungary: police hate crime investigations are enhanced, but growing LGBTI stigmatisation and xenophobic political discourse raise concern, March 9, 2023

191 European Commission against Racism and Intolerance, ECRI report on Hungary, March 9, 2023

192 European Commission against Racism and Intolerance, ECRI report on Hungary, March 9, 2023

193 Péterfalvi, A.,Hungary's Data Protection Chief Proposes 'Facebook Law', April 8, 2020

194 Hungarian Civil Liberties Union, Facebook act: the regulation should not be about censorship, but about transparency, June 28, 2021

ITALY

Key findings:

- Disinformation around Covid-19, immigration and social inequalities are frequent and are used as a political communication tool, particularly by the far right.
- With the rise of the far-right and the election of Giorgia Meloni as Prime Minister, threats and attacks against journalists and NGOs, particularly those working on immigration, have increased.
- SLAPPs are a serious issue in Italy and raise fears about shrinking press and media freedom.

Online smear and disinformation campaigns

The EU Disinfo Lab has drawn its conclusions on the state of disinformation in Italy in March 2023:[195] narratives frequently discussed in the public discourse, fuelled by political polarisation, include Covid-19, immigration and social inequalities. The report laments the lack of disinformation legislation in Italy, which gives social media platforms too much power.

The Italian NGO Emergency was the target of disinformation campaigns during the pandemic as it provided life-saving services. Mandatory vaccines and lockdowns during the pandemic led to distrust in the government and have turned NGOs such as Emergency into "collateral victims."[196]

Attacks, threats and hate speech online

The election of Italian Prime Minister Giorgia Meloni and far-right party Brothers of Italy inspired a surge of far-rights threats and attacks against journalists and critics.[197] NGOs are also targeted by Girorgia Meloni's government on subjects such as immigration.

The new government and its allies have targeted NGOs rescuing migrants at sea. Tightening sea regulations and imposing financial sanctions, the government is criticizing these NGOs for allowing illegal immigration. The Prime Minister went as far as suing anti-mafia

195 Giovanna Sessa M., EU Disinfolab, Disinformation Landscape in Italy, March 2023

196 International Observatory Human Rights, Covid-10 and our Human Rights, April 9th, 2020

197 Speri A., The Intercept, "We're coming for you": Italy's neofacists target journalists as they assume power", December 7th, 2022

journalist Roberto Saviano for his criticism of her immigration policies.[198]

Being close to France, Italy's immigration issue can be linked to far-right leader Marine Le Pen in France, who used the same discourse as the Prime Minister Giorgia Meloni.

Online political advertising

If regulation concerns of online political communication first arose during the 1990s when Berlusconi entered politics, the digital age has prompted an update of the existing framework.[199] The weight of digital and political communications on social media such as Facebook has prompted the Italian Data Protection Authority to cooperate in order to regulate the actions of political parties.[200]

SLAPPs

If SLAPPs have been a recurrent issue in Italy, they have become more important since the start of the leadership of Prime Minister Giorgia Meloni. Concerns about dwindling media freedom were raised in the legal case against journalist Robert Saviano. Saviano was accused of defamation in a lawsuit filed in 2020 by Meloni.[201] Despite the 2002 law fighting SLAPPs, Italy still struggles with the disproportion of power between the government, and the accused journalist or association.

In 2020, The president of the Federazione Nazionale della Stampa Italia (FNSI), Giuseppe Giulietti, helped the Repubblica journalist Federica Angeli in the 111th SLAPPs case of her career, with most being on the grounds of defamation. With 126 lawsuits in total (15 still ongoing), the Federica Angeli case has shown Italy's struggle to address SLAPPs.

198 Walfisz J., Euronews with AFP, "A chilling message to all journalists" as Italy's PM Meloni sues Roberto Saviano for defamation", November 17th, 2022

199 Balcani Caucaso, The regulation of political communication during electoral campaigns in Italy, February 22nd, 2019

200 Holroyd M., Italy elections: who has spent the most money on Facebook ads?, September 23rd, 2022

201 Elia C., IPI, Italy: lawsuits against Saviano and Domani highlight wider SLAPP problem, December 12th, 2022

POLAND

Key findings

The Polish government, under the Law and Justice (PiS) party, is reputed for carrying out smear campaigns against dissenters of their autocratic rule. CSOs, ethnic and religious minorities, and the LGBTQ+ community are attacked and harassed online by politicians, and religious leaders and their supporters.

The spyware Pegasus has been used as part of a system to monitor opposition and government critics, violating democratic standards and citizens' rights. Despite criticism, the government has continued surveillance practices, prompting legal challenges.

Strict defamation laws have led to charges against individuals expressing critical views on social media, with potential prison sentences for such offences.

Online smear and disinformation campaigns

The Polish government, led by the ruling national-conservative Law and Justice (PiS) party, is known for conducting smear campaigns against those who oppose their autocratic regime. Since the start of the Russian invasion of Ukraine, PiS politicians have attempted to label critical voices, including politicians, civil society organisations (CSOs) and journalists, as "Russian agents".[202]

Attacks, threats and hate speech online

The political discourse in Poland is highly polarised. Polish politicians, particularly from the ruling national-conservative Law and Justice (PiS) party,[203] and religious leaders have attacked CSOs, ethnic and religious minorities and the LGBTQ+ community.[204] Islamophobic and homophobic narratives, spread by nationalists and right wing extremists, have become socially acceptable within Poland.

LGBTQ+ activists interviewed by the NGO Amnesty International have reported being victims of intimidation and harassment,

202 P. Buras How the fight against Russian agents in Poland could destroy democracy, June 6, 2023
203 D. Tilles, LGBT "deviants don't have same rights as normal people", says Polish education minister, June 23, 2021
204 S. Walker, Polish president issues campaign pledge to fight 'LGBT ideology', June 12, 2020

including death threats on the internet, and online surveillance.[205] For many activists, these attacks led to changes in career plans and significant financial burdens.

Meanwhile, hate speech rules are often arbitrarily applied. For example, in April 2023, Poland's Supreme Court overturned the conviction of a man who had been sentenced for inciting hatred and calling for a "white Poland". This decision came following a request by the Minister of Justice, who himself is known for his strong nationalist views.[206]

Digital surveillance

In Poland, the spyware Pegasus has been part of a system for monitoring the opposition or critics of the controversial judicial reform introduced by the right-wing conservative PiS party. Control mechanisms were non-existent.

The Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) of the European Union found that the use of Pegasus has been part of "a system for the surveillance of the opposition and critics of the government - designed to keep the ruling majority and the government in power".[207] Government officials, including the Interior Minister, refused to meet the PEGA delegation during their fact-finding mission in Poland. The PEGA delegation in their final report noted how illegal spyware has been used to target political opponents and that democratic standards and citizens' rights have been "grossly violated".[208]

The Polish government has been late to introduce the European Electronic Communications Code from December 11, 2018 - which member states were supposed to implement by December 2022. In 2022, the first reading of the Electronic Communications Law, or "lex pilot", finally took place in the Polish Parliament. The government initially proposed a law that would give authorities broad surveillance powers and allow it to store data on potentially all citizens for as long as 12 months, even if they have not committed any crime.[209] All this, knowing that Polish authorities have surveilled 1.8 million citizens in 2021, and have used the

205 Amnesty International, Poland: "They Treated Us Like Criminals": From Shrinking Space to Harassment of LGBTI Activists, July 20, 2022

206 D. Tilles, Polish Supreme Court overturns "Poland for Poles" hate speech ruling at request of justice minister, April 20, 2023

207 European Parliament, PEGA Spyware: MEPs sound alarm on threat to democracy and demand reforms, May 8, 2023

208 European Parliament, PEGA, Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, May 22, 2023

209 K, Izdebski and M. Musidłowska, New Polish Digital Law is Government Overreach, January 18, 2023

spyware software Pegasus to surveil political opponents and journalists.[210]

The proposal was criticised by civil liberties groups, who argued that it would violate the privacy of Polish citizens and could be misused to target political opponents and other groups the government deems to be a threat. The law would have also been in violation of the European Court of Justice's (CJEU) judgments on data retention, which state that it is not possible to treat all citizens as suspects and store their data just in case.

However, after much criticism, the government declared on February 6th, 2023 that the data retention obligation would not be expanded.[211]

Meanwhile, the surveillance overreach continues. The Polish secret services continue to monitor citizens, beyond the Pegasus scandal, which is now being challenged by the digital rights organisation Panoptykon Foundation, which has started a strategic litigation process.[212]

Online censorship

Twitter's decision to ban Donald Trump's Twitter account due to "incitement of violence"[213] in January 2021, was heavily criticised by Polish government officials. The government announced their plan to introduce a law that would make it illegal for tech companies to remove posts that do not break Polish law.[214] The law would allow users to file a court petition to force social media companies to restore removed content if they believed it did not violate Polish law. The NGO Reporters Without Borders warned that the law would put freedom of expression at risk, as it would give the government the power to "control news and information on social media".[215]

While people are generally free to express their personal views, Poland has strict defamation and public insult laws, including against offending the President or offending religious feelings. In March 2021, Jakub Żulczyk, a well-known Polish author, faced charges for calling the president a "moron" on social media, potentially leading to a three-year prison sentence.[216] In another case, the journalist Piotr

210 B. Sieniawski, Polish government working on controversial surveillance bill, January 20, 2023

211 Panoptykon Foundation, Successful advocacy: the government declares no further extension of data retention obligation, February 24, 2023

212 Panoptykon Foundation, Activists v. Poland. European Court of Human Rights hearing on uncontrolled surveillance, November 4, 2022

213 Twitter, Permanent suspension of @realDonaldTrump, January 8, 2021

214 S. Walker, Poland plans to make censoring of social media accounts illegal, January 14, 2021

215 Reporters Without Borders, Poland's new social media law puts freedom of expression at risk, RSF warn, January 28, 2021

216 N. Camut, Writer who called Polish president 'a moron' should not be punished, court rules, May 23, 2023

Maślak was charged in March 2022 by the military prosecutor's office with defamation. The charges refer to a message posted by the journalist on Twitter, in which he criticised the actions of the Polish Border Guard against a group of refugees at the Polish-Belarusian border. The charges pressed against the journalist are punishable by up to one year in prison.[217]

Freedom of information

During April and May 2022, a request under the Freedom of Information Act made by Polish daily newspaper *Gazeta Wyborcza* was rejected[218] by the Regional Prosecutor's Office in Krakow without legitimate reasons. The newspaper requested information about proceedings related to a decision on whether to outlaw the National-Radical Camp (ONR), a group of fascist, far-right, and ultranationalist Polish organisations.

Strategic Litigation Against Public Participation (SLAPPs)

The use of bogus lawsuits against media freedom actors is a common practice in Poland. According to the International Press Institute (IPI), the independent newspaper Gazeta Wyborcza faces approximately 90 Strategic Litigation Against Public Participation (SLAPPs) cases.[219] On 9th May 2022, Gazeta Wyborcza and its journalist Agnieszka Kublik received a pre-litigation warning regarding alleged defamation from Piotr Woyciechowski, the former head of the Polish Security Printing Works and a member of the Polish National Foundation. He demanded that a report be immediately removed from the newspaper website. The report quoted a testimony during the Senate Investigative Committee on Pegasus spyware, in which an individual alleged that Woyciechowski was involved in a blackmailing scheme. The newspaper defended the article, stating that it had simply quoted from the parliamentary inquiry, and called the warning an "attack on the freedom of speech".

Online platforms connected issues

In December 2018, the Polish government signed a Memorandum of Understanding with Facebook that allowed users to challenge any takedown decisions.[220] Facebook, however, would continue to reserve the final decision to remove any content or accounts. While some saw this as a positive development from the point of view of user protection, others raised concerns about the power of social media platforms over freedom of expression.

217 Civil Liberties Union for Europe, Liberties Rule of Law Report 2023, February 2023

218 MAPMF, FOI requests by Gazeta Wyborcza repeatedly denied by Krakow Prosecutor's Office, May 10, 2022

219 A. Kublik, M. Wiatrowski, J. Kibitlewski, Increased attempts to silence Poland's free media through lawsuits (Gazeta Wyborcza), June 9, 2022

220 https://edri.org/our-work/poland-privatised-law-enforcement-or-protecting-users-rights/

In 2018, Facebook removed fan pages and groups belonging to the NGO Civil Society Drug Policy Initiative (SIN), allegedly because the NGO violated Facebook's community standards. In 2019, the Facebook-owned Instagram account of SIN was also removed. This happened without any warning or clear explanation. SIN's online communications aim to provide drug education and warnings against substance abuse, targeting young people who are active on social media.

In May 2019 SIN filed, with the support of the Polish NGO Panoptykon, a lawsuit against Facebook, arguing that their freedom of speech was violated.[221] The plaintiffs argue that final decisions on content moderation should be subject to independent judicial scrutiny, and they hope the case will set standards for other platforms as well. In a first ruling, the District Court in Warsaw temporarily prohibited Facebook from removing fan pages, groups and profiles run by SIN.[222]

Facebook appealed the decision by the Warsaw court. On February 7, 2023 the first SIN vs Facebook hearing took place.[223] The court wanted to gather information about the circumstances of the blocking, SIN's appeals, and the outcome. During the hearing, Facebook representatives argued that educating about substance abuse is equivalent to promoting it.

Facebook has been using unfair legal tactics, such as insisting that the lawsuit is not in Polish but in English, despite the platform having over 16 million accounts in Poland, forcing SIN to pay close to 9,000 PLN for translation. It also has tried to convince the judges to not accept an *amicus curiae* opinion[224] of the German civil rights association Gesellschaft für Freiheitsrechte (GFF), arguing that this case does not fall into the category of cases where civil society organisations can express their views.[225]

221 https://www.euractiv.com/section/media/news/facebook-hit-by-landmark-censorship-lawsuit-in-poland/

222 https://edri.org/our-work/sin-vs-facebook-first-victory-against-privatised-censorship/

223 https://edri.org/our-work/case-challenging-metas-arbitrary-removal-of-polish-ngos-accounts-finally-in-court/

224 GFF's opinion includes a summary of a similar case issued in Germany, in which the courts upheld a ban against an NGO and criticized the non-transparent and arbitrary moderation on the platform.

225 https://panoptykon.org/facebook-podwaza-opinie-sprawa-o-cenzure

SLOVAKIA

Key Findings:

- Verbal attacks and smear campaigns targeting journalists remain a challenge. Authority and political figures continue to attempt to discredit and threaten civil society actors online.
- Slovakia sees an increase of Russian support during the war in Ukraine and struggles to combat Russian disinformation online. Efforts to block disinformation websites have been made, but Russian propaganda inclines Slovak society to believe Russia is not responsible for the attack.
- SLAPP cases continue to plague online civic space. Online sources experience forced removal of content following lawsuits, and journalists continue to be targets of defamation suits following publications.

Disinformation

Russian disinformation has been a growing issue in Slovakia, since the Russian invasion of Ukraine. In response to Russian propaganda in 2022, the National Security Office (NBÚ) blocked websites deemed to contain disinformation, including any platforms which threaten or damage national security, economic interests or foreign policy.[226] Some local news and current affairs sites were therefore banned for fitting this description.[227] Hlavné Správy, a pro-Kremlin propaganda website, was among the list of banned sources.[228] The list was put together by the Konšpirátori.sk project, an NGO that gathers intel on sites that have conspiracies and deceptive information, with the intention of making sure businesses do not advertise on these pages.[229] However, despite efforts to combat disinformation by both government and civil society, the battle against Russian propaganda seems to be losing. According to GLOBSEC, only 40% of Slovaks believe Russia is responsible for the war in Ukraine.[230]

226 The Slovak Spectator, Slovakia plans to ban disinformation websites from spring again, November 2, 2022
227 Školkay, A. Regulating fake news and hoaxes within visegrad countries, December 30, 2022
228 The Slovak Spectator Popular pro-Kremlin propaganda-peddling website back on the list of disinformers, December 22, 2022
229 Zorád, L. Grass Roots Initiatives Combating Extremism in Online Space in Slovakia, March 23, 2018
230 Bayer, L. Slovakia risks succumbing to Russian disinformation, president warns, June 3, 2023

Online smear campaigns

Online smear campaigns in Slovakia are often at the hands of authority or political figures. In 2019, Aktuality.sk was victim of a smear campaign by the former chief of national police, Tibor Gašpar.[231] Gašpar accused Aktuality.sk of disinformation and spreading lies to expand liberal ideologies. This followed after Aktuality.sk published content accusing him of misleading followers of his Facebook page about the government administration. He also claimed that Aktuality.sk journalists were funded by George Soros in an effort to discredit them. Gašpar was the chief of national police at the time of journalist Jan Kuciak's murder, who was a journalist at Aktuality.sk. He was among those who were asked to step down following protests on the murder investigation.

Attacks, threats and hate speech online

Online harassment of journalists continues to be a consistent problem,[232] and these attacks are often instigated by politicians. According to a survey conducted by the Investigative Centre of Ján Kuciak, about two thirds of media workers have experienced some kind of attack within 2022, with online harassment being the most common.

Former Prime Minister Igor Matovič has been the source of numerous online attacks targeting journalists.[233] For example, in 2022, Matovič attacked the editor-in-chief of the news website Denník N's, Matúš Kostolný, in a Facebook post after the journalist had published a critical opinion piece. Matovič further claimed that an unnamed media group was corrupt and spreading lies, comparing their work with Nazi propaganda.

Strategic Litigation Against Public Participation (SLAPPs)

Slovakia struggles with a number of SLAPP cases. In 2020, Hlavné správy, a new source that is known for spreading disinformation, sued disinformation-fighting NGO Konšpirátori.sk to have their name removed from Konšpirátori.sk's list of problematic sources.[234] The Bratislava District Court ruled that until a decision is made, Konšpirátori.sk must comply with this request and remove them from the list.

With precedent now established, new source Hlavný Denník, known to spread conspiracy theories and disinformation online, additionally

231 Wiseman, J. Slovak news website targeted in smear campaign, September 19, 2019

232 Wiseman, J. Analysis: How much has media freedom in Slovakia changed five years after Ján Kuciak murder?, February 24, 2023

233 International Press Institute, Slovakia: Deputy PM's attacks undermined government's broader effects to strengthen press freedom, October 6, 2022

234 Sawiris, M. Strategic lawsuits erode the fight against disinformation, October 4, 2021

sued the NGO. As a result, Hlavný Denník was able to successfully remove their name from Konšpirátori.sk's database.

Slovakia's notoriously loose defamation laws have been misused to punish journalists for their publications. For example, journalist Michal Havran was victim to a criminal defamation suit for publishing an article criticising a Slovak Catholic priest's public statements in regards to homosexuals, his links to a far-right party and his support of banning abortions. Police investigators accused Havran of both infringing on the priest's freedom of expression and defaming one's faith.[235] The charges were eventually dropped.

New security measures that may affect civil society actors

In 2022, the Slovak parliament passed a new Act on Media and the Act on Publication, aimed at strengthening journalist protection.[236] These new laws also strengthened transparency of media funding, making journalists' credibility stronger when diffusing disinformation. The act further establishes the right of confidentiality of sources, including online media journalists. However, members of parliament also incorporated a "right of reply" for public officials, granting them more room in the media - and potential room for further online smear campaigns and harassment - than citizens.

Online platforms connected issues

In Spring of 2022, the National Security Office (NBÚ) was granted permission to block online content under reasons to minimise radicalisation, political destabilisation and threats to democratic institutions. Additionally, Slovak online content is regularly monitored by Slovak intelligence services. The decision to permit blocking brought controversy, as it previously lost its legitimacy due to flawed legislation and the power was ultimately lost.[237] The Slovak government then approved an amendment for this authority in November 2022, allowing nine months of blocking decisions to be made. If passed by parliament, the NBÚ must report and publish these decisions on their website.

235 Committee to Protect Journalists, Slovak authorities file criminal defamation charges against columnist Michal Havran, February 10, 2020

236 International Press Institute, Slovakia: Government pushes ahead with ambitious media reform program, October 24, 2022

237 The Slovak Spectator, Slovakia plans to ban disinformation websites from spring again, November 2, 2022

SPAIN

Key findings

- Catalonia has been the region with the most attacks on civil society. Those attacks try to prevent the Catalonian independence movement from growing further while keeping an eye on Catalonian personalities pushing for autonomy. Therefore, Catalonian associations are more exposed in the online civic space than others in the rest of Spain.

Online smear and disinformation campaigns

Reporters Without Borders (RSF) explained in their 2022 Spain Report that "*the level of violence against journalists has fallen considerably thanks to a decline in the tension over Catalan independence demands,*" linking the threats to journalists with the political context.

The Federation of Journalists Association in a seminar organised in October 2022, concluded that smear campaigns against journalists are mainly directed against women journalists. These attacks aim to silence the voices that cover certain topics.[238]

The Madrid Press Association criticised the Russian Embassy in Spain for its discrediting campaign against the newspaper ABC. The diplomatic mission accused the outlet of censoring an alleged interview initially planned with the Speaker of the Russian Foreign Ministry. The interview was never granted. Instead, the Russian authorities submitted a written statement by the Speaker of the Russian Foreign Ministry. The Spanish newspaper refused to publish the written statement made by the Speaker of the Russian Foreign Ministry.[239]

Attacks, threats and hate speech online

Similar to online smear and disinformation campaigns, journalists are targeted by attacks, threats, and hate speech online, usually when their coverage is likely to embarrass a public official or institution.

In 2017, the International Press Institute condemned the threats emitted by the Spanish

238 Federacion de Asociaciones de Periodistas de Espana (FAPE), El ciberacoso a periodistas tiene sexo femenino, October 27, 2022

239 Asociación de la Prensa de Madrid, La APM rechaza la campaña de desprestigio de la Embajada rusa contra 'ABC', May 5, 2022

police against the news site Público when the news site covered a case of alleged corruption implicating law enforcement officials.[240] The news site was able to shine light on these corruption incidents thanks to its recorded conversations with its sources: the investigation even allowed to discover the existence of a "political brigade," an alleged police unit acting in the margins of the law but with the acquiescence of the political elite. While the current police director-general, German Lopez, denied these allegations by refuting the existence (at least since his arrival four months ago) of a political brigade. Nevertheless, the police officials threatened to Publico to disclose personal information on the investigative journalist (doxxing) - and invent false information if necessary.

Digital surveillance

The federal government has been surveilling specific personalities and regions of Spain. According to an investigation from the University of Toronto Citizen Lab,[241] the Spanish government extensively used the Pegasus and Candiru programs to spy on journalists, lawyers, human rights defenders and political representatives from Catalonia and the Basque country. The investigation, published in April 2022 and confirmed by Amnesty International, showed how 65 individuals sharing the trait of being critical voices and political dissidents were surveilled from 2015 to 2021.

The Citizen Lab's report[242] explained how the Spanish government targeted members of the Catalan Civil Society (Assemblea Nacional Catalana, Omnium Cultural, Catalan's Open-Source and Digital Voting Community, etc.). The "Catalangate" illustrated how this abusive surveillance is a flagrant violation of the right of privacy and secrecy of communications.

Months later, the news outlet Directa[243] published a report showing that 38 left-wing activists were spied on by the Spanish police under the justification of "anti-terrorist fight."

Doxing

Articles 197 to 201 in the Spanish Criminal Code regulates the disclosure and revelations of secrets, and the 2015 reform[244] covered the offence of doxing as "*disseminating, disclosing or transferring to third parties images or audiovisual*

240 International Press Institute, IPI condemns Spain police threats against news site, March 24, 2017

241 Civic Space Watch, Spain: CSOs statement against state surveillance on journalists, politicians, and lawyers, May 3, 2022

242 Citizenlab, CatalanGate: extensive mercenary spyware operation against catalans using Pegasus and Candiru, April 18, 2022

243 Rodriguez J. and Garcia G., El Ministeri de l'Interior espanyol ha punxat massivament les communicacions de l'Esquerra Independentista i dels CDR, October 10, 2022

244 Ministerio de Justicia, Criminal Code, 2016

recordings of the one obtained with their consent in a home or in any other place out of sight of third parties, when the disclosure seriously undermines the personal privacy of that person."

Like online smear campaigns, the victims of doxxing (leading to attacks and threats online) in Spain are journalists. In 2021, Reporters without Borders (RSF) has criticised the far-right Spanish party Vox for threatening on Twitter the editor of a satirical magazine, El Jueves.[245] The party published the person's name and photograph on the social media platform in an act of revenge (due to the magazine frequently lampooning the party in its columns). Additionally, Vox's Twitter account disclosed the city and the street location of the magazine office[246] in order to have the editor "takes responsibility when he leaves his office."

Strategic Litigation Against Public Participation (SLAPPs)

Spanish journalists frequently face SLAPPs procedures, which limits the right to freedom of information and expression. Following are some examples:

Iberdrola, a big Spanish hydroelectric corporation, presented a defamation lawsuit against the Spanish digital newspaper "El Confidencial" for offences against its honour. The Federación de Asociaciones de Periodistas de España (FAPE) and the Madrid Press Association supported El Confidential and the right to freedom of information by stating that the information relayed by El Confidencial was true.[247]

Ignacio Cembrero, a journalist specialised in the Maghreb and working for the digital newspaper El Confidencial, has been sued by the Moroccan Government after he published his suspicion that his telephone had been subject to the spyware Pegasus by the Moroccan government.[248] The Madrid Press Association issued a statement in support of Cembrero, arguing that this new legal complaint has no other intention than to intimidate the journalist and prevent him from carrying out his profession as a journalist.[249]

Whistleblower protection

On February 23rd, 2023, the Spanish government adopted a new whistleblowing law by transposing the EU Directive on

245 Jones S., Spain's far-right Vox party under fire for veiled Twitter threat against editor, July 6, 2021

246 Liberties, Protests over gender-based violence; office of LGBTI organisations vandalised, July 29, 2021

247 Asociación de la Prensa de Madrid, La FAPE y la APIE defienden la libertad de información de 'El Confidencial', February 9, 2022

248 Morel S., Spanish journalist accused by Morocco of "boasting" goes on trial, January 13, 2023

249 Asociación de la Prensa de Madrid, La APM respalda a Ignacio Cembrero ante la demanda de Marruecos, July 4, 2022

Whistleblowing.[250] The Spanish Senate approved the legislation, making it the eighteenth EU country to implement said directive.

Since 2018, several attempts to implement some whistleblower protection have failed, according to the EU Whistleblowing Monitor.[251] In 2018, civil society expert Simona Levi addressed the Transparency Committee of the Parliament of Catalonia to promote amendments proposed by the NGO Xnet. The NGO carefully followed every step of the EU transposing phase to be sure that whistleblower protection rights were not reduced during the process.

From time to time, the EU Directive has been used as an example in current affairs regarding whistleblower protection. In the Roberto Macías case,[252] the whistleblower was sentenced to 2 years of imprisonment in Spain for reporting information on corruption in the trade union organisation where he worked. Xnet deplored the judge's ruling which mentioned the EU Directive seeking to protect whistleblowers, specifically mentioning that this required "the person to have first made a complaint through internal or external channels, without appropriate measures having been taken." Xnet found that the judgement was a serious misunderstanding of the spirit of the Directive.

Online platforms connected issues

In 2017, the Spanish government fined Facebook for illegal tracing of users, a violation of data protection rules according to the Spanish Data Protection Agency, the AEPD (Agencia Española de Protección de Datos).[253] The platform received a €1.2 million fine from the Spanish government, following an investigation conducted conjointly with France, Netherlands, Belgium and Germany.

In April 2023, the AEPD opened an investigation under its purview against ChatGPT for a suspected breach of data protection rules.[254] Again, this investigation started following an action by a European neighbour (Italy), which decided to conduct a review on this platform's impact on data protection.

250 Grainger M., Spain wraps up EU Whistleblowing Directive transposition, February 28, 2023
251 EU Whistleblowing Report, Spain, 2023
252 Minder R., A Spanish Whistle-Blower Appeals to the E.U. for Help, August 22nd, 2022
253 Les Échos, Facebook sanctionné en Espagne sur la protection des données, September 11, 2017
254 Euronews, Spain open an investigation into OpenAI's ChatGPT over a potential data breach, April 14, 2023

SWEDEN

Key Findings:

- In response to rising trends in disinformation, the Swedish government has established a new agency dedicated to combat these issues.
- The misuse of data collection and surveillance techniques have grown in Swedish police forces.
- Proper management of online hate speech and online threats are yet to be fully understood or investigated by police. These issues require better knowledge and training within law enforcement to best investigate.
- Due to the overwhelming spread of disinformation across social media platforms, some organisations have opted to delete their accounts altogether to avoid the need to combat it.

Disinformation

Disinformation has been on the rise in Sweden. Particularly, Sweden has fallen victim to pro-Russian disinformation narratives.[255] Swedish Security Services have expressed great concern over disinformation campaigns and cyber attacks from Russia.[256]

Sweden has additionally faced anti-Muslim disinformation online.[257] Particularly, there have been claims that Swedish social services have been removing - or kidnapping - Muslim children from their homes without legal reasons. As a result, Swedish social service workers have fallen victim to threats and their work has been negatively affected. In response to the attack on the public sector, the Swedish government is establishing several measures to counteract disinformation, such as forming harsher punishments for spreading disinformation and proposing new legislation to maintain more security officers within social services buildings.

Further, in 2022, the Swedish government established a new Psychological Defence agency with the purpose to combat dis- and misinformation while protecting democratic

255 Giandomenico, J. et al., The disinformation landscape in Sweden, May 5, 2023
256 Szumski, C., Threats from Russia, disinformation rises in Sweden, February 23, 2023
257 Government of Sweden, Government taking strong action against disinformation and rumour-spreading campaign, February 6, 202

society.[258] According to the agency's deputy director, the agency's purpose is "to identify and counter foreign malign information influence, disinformation and other dissemination of misleading information directed at Sweden."

Attacks, threats and hate speech online

Activists and journalists experience a plethora of attacks online. Many of these take place on Facebook, where users write hateful comments.[259] Journalists who focus on extremist groups, organised crime and religious groups especially are targets of intimidation.[260] In a government survey conducted in 2021, results showed that 67% of female journalists and 41% of male journalists were victims of online attacks, including abuse and hate speech. Additionally, in 2023 the president of the Swedish Union of Journalists reported that 30% of members indicated that they had received threats online.[261]

Digital surveillance

In the past few years, there have been many instances of misuse of data collection and surveillance techniques in Sweden. For example, Swedish police were found to be using Clearview AI, an app that uses facial recognition images to find matches on online platforms such as Facebook and Instagram, for investigations.[262] The images on the app are used to compile a biometrics database with these photos. The app then sells these images to police and private security companies. Eventually, an investigation was launched into the police's use of Clearview AI, later deeming its use in their investigations illegal.

Strategic Litigation Against Public Participation (SLAPPs)

In 2020, the website Realtid was sued for defamation by a Swedish businessman, Svante Kumlin. This was a result of Realtid's financial investigation into Kumlin's company, Eco Energy World. In 2022, a court in London found that there was insufficient evidence in eight of Realtid's articles to prove harm to Eco Energy World. However, three are still under investigation.[263]

258 Suliman, A., Sweden's new Psychological Defense Agency to fight fake news, foreign interference, January 6, 2022
259 Civil Liberties Union for Europe, Liberties Rule of Law Report 2022, February 2022
260 Freedom House, Sweden: Freedom in the world 2022 country report, 2022
261 European Federation of Journalists, Journalist unions shared best practices on online harassment in Sweden, February 17, 2023
262 University of Gothenburg, What does the increased surveillance mean for society?, May 3, 2023
263 Civil Liberties Union for Europe, Liberties Media Freedom Report 2023, April 2022

Law enforcement capacity to investigate online threats and attacks

There is a lack of proper understanding on what constitutes online hate speech, or hate speech generally, within the Swedish police and further training is needed to develop knowledge in key areas such as discrimination and threats.[264] There is still a greater need for the police to investigate such attacks on journalists and other civil society actors.

At the start of 2023, a "foreign espionage" law was incorporated into Sweden's penal code.[265] The law allows law enforcement to investigate publishers, journalists and whistleblowers if they disclose confidential information that may be detrimental to Sweden's relationships to other states or international institutions.[266] This would further put their sources in danger. Those found guilty can be sentenced to prison for up to four years.

Online platforms connected issues

In 2023, public broadcaster Sveriges Radio decided to remove their Twitter account over several concerns, including fake news. Sveriges Radio cited concerns over the company's ability to handle so many fake accounts, hate speech and threats, and misinformation and bots. Although Sveriges Radio has been reducing their activity on Twitter for several years, there was a boom in hate speech and fake news that the broadcaster team was unable to keep up with, pushing them to close the account altogether.[267]

264 Civil Liberties Union for Europe, Liberties Rule of Law Report 2022, February 2022

265 European Federation of Journalists, Tove Carlén: "The Swedish new law on public espionage provides little protection for journalists' sources", February 12, 2022

266 Gosztola, K., Sweden Expands Espionage Law, Endangering Freedom of Journalists and Whistleblowers, November 21, 2022

267 Mac Dougall, D., Concerned about fake news and hate speech, Sweden's public radio closes Twitter accounts, April 18, 2023

Contact info:

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of 19 national civil liberties NGOs from across the EU.

info@liberties.eu
Jascha Galaski j.galaski@liberties.eu

Website:

liberties.eu

Authors:

Malcolm Biiga, Autumn Mozeliak, Jascha Galaski

The Civil Liberties Union for Europe e. V.

Ebertstraße 2,
10117 Berlin, Germany

Subscribe to our newsletter

https://www.liberties.eu/en/subscribe

Reference link to study

Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/7t3dyb

Photocredit

Andrea Piacquadio/Pexels.com

Follow us