

DOCUMENTING THE SETBACKS:

The new environment for counter-disinformation in Europe and Germany



TABLE OF CONTENTS

1. EXECUTIVE SUMMARY	1
2. INTRODUCTION	2
3. POLITICAL SETBACKS IN THE INTERNATIONAL SCENE.....	4
4. PLATFORM POLICY CHANGES IN TACKLING DISINFORMATION	7
5. LEGAL AND STRATEGIC DEFENSES IN EUROPE AND GERMANY	11
6. CONCLUSION AND RECOMMENDATIONS	14

Deliverable written by Raquel Miguel and Maria Giovanna Sessa (EU DisinfoLab)
for the Friedrich Naumann Foundation



FRIEDRICH NAUMANN
FOUNDATION For Freedom.

1. EXECUTIVE SUMMARY

- As threat actors are growing in number and sophistication and technological advances make malicious activities easier and more effective, the counter-disinformation community faces mounting challenges. The picture is further complicated by rising geopolitical tensions and hybrid warfare, combining disinformation, FIMI, and related manipulative practices.
- Challenges also come from within. Domestic political shifts in several countries are eroding democratic safeguards, contributing to an environment that leaves rollbacks in platform policies largely uncontested, and weakening counter-disinformation efforts. Political developments in the U.S. echo across the Atlantic, affecting Europe at the very moment when some platforms are loosening controls against the threats policy-makers seek to contain. Practitioners now face a dual hurdle: hostile external actors on one side, and an increasingly adverse political and corporate environment on the other.
- The EU has built strong resilience through regulations such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). This framework distinguishes Europe from regions with weaker protections. Yet enforcing these safeguards is proving increasingly difficult under rising external and internal pressures.
- Germany illustrates both promise and vulnerability. Determined in its efforts to enforce the DSA, it nonetheless faces setbacks in platform moderation and political fragility at home. Given the country's central role in the European Union, its resilience will be decisive. Public debate reflects this dynamic: while some initiatives emphasise privacy protections, data access, and checks on platform abuses, others call for greater digital sovereignty.
- In this environment, Europe must strengthen its defences not only against adversarial actors but also against hostile political and corporate dynamics. Sustained resilience depends on recognising and addressing this multifaceted landscape to safeguard the integrity of the European information space.

2. INTRODUCTION

The fight against information manipulation and related distortions stands at a contradictory juncture. On the one hand, awareness has never been higher as [people](#), [political actors](#), and decision-makers increasingly [recognise the threat](#), frequently refer to it in [public interventions](#), and express the [intention to act](#).

On the other hand, the threats are multiplying. Several drivers fuel the **escalation of disinformation, Foreign Information Manipulation and Interference (FIMI), and other deceptive practices**: intensifying geopolitical tensions and armed conflicts, the rapid digitalisation of critical infrastructures, and accelerating technological development – all of which sustain the rise of hybrid warfare.

Within this context, information manipulation takes the form of orchestrated disinformation campaigns, broader FIMI strategies, propaganda, and even financially motivated scams. These practices often overlap, blurring the boundaries between political, economic, and criminal motivations. At the same time, growing access to advanced technologies – particularly artificial intelligence – has widened the pool of actors capable of exploiting such tools for malicious purposes.

Crucially, the challenge is no longer external to the EU. The counter-disinformation community increasingly operates in a hostile political and institutional environment. A recent example came during Commission President Ursula von der Leyen's [2025 State of the Union](#) address, when she was interrupted by dissenting shouts as she announced the creation of the European Centre for Democratic Resilience. Parliament President Roberta Metsola warned [MEP Christine Anderson \(AfD\)](#) that she would be removed from the chamber if she continued interrupting proceedings.

The rise of nationalist and conservative forces has brought elites into office that are sometimes resistant, or even openly opposed, to counter-FIMI initiatives, thereby undermining the work of practitioners and the overall resilience and trust in democratic processes. Meanwhile, major digital platforms have rolled back key policies designed to curb mis- and disinformation. These political and corporate retreats add a new layer of difficulty, forcing defenders to contend with both exogenous state and non-state actors and endogenous obstacles.

Against this backdrop, the European Union in general, and Germany in particular, demonstrates notable resilience, thanks to a regulatory framework unparalleled in other regions. Yet its effective enforcement is increasingly at risk.

This report examines how the current context affects the EU's capacity to counter information manipulation, with a focus on Germany's defensive measures. It concludes by arguing for the maintenance and expansion of protective mechanisms to address both **external threat actors and the increasingly adverse political and platform environments shaping the fight against disinformation**. While Germany is used as a focal case study, it is important to note that the drivers, threats, and responses are overwhelmingly European in scope, making it difficult to fully disentangle country-specific dynamics from the broader continental landscape.

3. POLITICAL SETBACKS IN THE INTERNATIONAL SCENE

DISTORTING THE FIGHT AGAINST DISINFORMATION AS CENSORSHIP

The [measures adopted](#) by [Trump](#)'s administration in the U.S. reverberated dangerously in Europe, emboldening certain political forces. By [casting doubts](#) on the legitimacy of counter-disinformation efforts and framing them as partisan or biased, political shifts in the United States offered a convenient narrative for European actors eager to delegitimise similar initiatives at home. This **transatlantic ripple effect eroded institutional trust in information integrity safeguards and gave weight to calls for weaker oversight of online platforms**. Almost as a self-fulfilling prophecy, these dynamics spilled into technology policy debates, where regulation became entangled with [accusations of censorship](#).

This erosion both draws on and reinforces the narrative that any form of regulation equals censorship or an assault on free speech. As a result, defenders are discredited, antagonised, and exposed to political as well as personal attacks. Beyond reputational harm, their financial survival is also at stake: **weakened institutional support deters funders and shrinks the space for sustained collaboration**. What begins as a rhetorical framing thus evolves into a structural threat to the community's resilience and long-term viability.

SETBACKS IN THE UNITED STATES

One of the Trump administration's first moves was an [executive order](#) against so-called "federal censorship", presented as a defence of free speech. In practice, it prohibited [federal agencies](#) from engaging in counter-disinformation and FIMI activities, dismantling much of the infrastructure built by previous administrations. Among the casualties were the [FBI's specialised unit](#) on [foreign election interference](#) and the State Department's [Counter-Foreign Information Manipulation and Interference Hub](#) (previously the Global Engagement Center, GEC). More recently, the [Foreign Malign Influence Center \(FMIC\)](#) was dissolved, with its functions dispersed across the U.S. intelligence community.

In parallel, the [National Science Foundation](#) cancelled hundreds of research grants it deemed "not aligned" with its new priorities. [Projects](#) on [diversity, equity, and inclusion \(DEI\)](#), as well as misinformation and disinformation, were among those cut. This dealt a double blow: [cutting ongoing work](#) while narrowing the scope of future research. Since malign actors exploit societal grievances, prejudices, and divisions – often targeting minority

groups through identity-based disinformation – restricting research in these areas critically undermines the ability to assess vulnerabilities that are systematically exploited for FIMI purposes.

Compounding the problem, key political appointments went to [figures](#) long associated with conspiracy theories and the disinformation-prone [MAGA movement](#). In a reversed dynamic, disinformers moved from being subjects of scrutiny to holders of power. From that position, they could discredit the journalists, academics, and researchers who had challenged them. These experts found themselves under [heightened surveillance](#) and [public scrutiny](#), targeted by occasional [attacks](#), while deprived of [funding](#) – a set of conditions that made rigorous research, precarious to say the least.

REVERBERATIONS IN EUROPE, AND GERMANY

The [closure of the GEC](#) also terminated memoranda of understanding with European partners. These frameworks had been designed to coordinate efforts against foreign disinformation, particularly from Russia, China, and Iran. Their dissolution, as reported by the [Financial Times](#), now hinders collective transatlantic responses. This shift has also echoed in Europe’s political discourse. Pro-Trump – and sometimes pro-Russian – segments of the political scene have adopted a rhetoric that converges with that of openly hostile actors and formerly reliable allies, who now both work to discredit the counter-disinformation community.

Germany illustrates these dynamics well. As the EU’s largest country, it has long championed platform regulation, media governance, and the protection of information integrity. Yet, its polarised politics make **a testing ground for reframing protective measures as threats to free expression**. After the February 2025 elections, opponents accused the new CDU/CSU-SPD government coalition of planning a “[ban on lying](#)”, misrepresenting the cabinet’s stated intention to curb deliberate disinformation. The controversy shows how legitimate initiatives can be distorted as censorship claims and weaponised to prevent any democratic regulation.

In addition to [fringe German outlets](#), the German far-right party Alternative für Deutschland (AfD) has also amplified this reframing. It tabled [two parliamentary motions](#) to abolish the Digital Services Act (DSA) under the slogan “no restrictions on freedom of expression on social media”. It also sought to normalise hate speech through [attempts](#) to repeal Article 188 of the Criminal Code (covering insults and defamation against political figures) and paragraph 130 of the Criminal Code (criminalising incitement to hatred). [Correctiv](#) reports that party leader Björn Höcke unsuccessfully pushed for the latter in the electoral programme. The AfD also opposed [government plans](#) to bar individuals repeatedly convicted of incitement to hatred from standing for election,

dismissing such offences as mere opinions. Party members even defended a YouTuber convicted of hate speech for anti-Semitic, racist, and Islamophobic posts, with some proposing to raise the case to the [European Commission](#) via a European Parliamentary question. Judges and prosecutors handling such cases have meanwhile faced targeted harassment by far-right activists.

In an [interview](#) in August 2025, former Trump administration official Mike Benz claimed that the Obama-era U.S. State Department – along with CIA, NATO, and the EU – pressured Germany to adopt the NetzDG (Network Enforcement Act), a move he said served to suppress far-right parties. However, concerns over institutional overreach are not confined to the past. After the recent motion of censure against Commission President von der Leyen, Romanian MEP [Gheorghe Piperea](#) accused two EU-based organisations on the frontlines of tackling interference, Check First and Debunk, of bias and political servitude, echoing U.S. narratives that portray independent civil society organisations as unaccountable agents. Similarly, **debates around the DSA have been reframed, from requesting transparency on how private companies moderate and delete content, to attempts to restrict legitimate expression.** This narrative appears to have slowed national implementation: the [European Commission](#) has launched infringement proceedings against Czechia, Cyprus, Poland, Portugal, and Spain for failing to establish enforcement structures. In several member states, critics warn that the DSA constitutes “[preventive censorship](#)”, further deepening mistrust.

At the same time, some [civil society groups](#) have raised more nuanced concerns. They caution that the DSA’s broad scope might incentivise platforms to [over-remove content](#), silencing lawful speech, and consolidating tech companies’ control over online debate. These are not rejections of the law but calls for oversight and clarification – for example, ensuring platforms are also held accountable against unjustified takedowns. Still, even **well-founded concerns risk being distorted by actors seeking to undermine regulation altogether**, with very strong case law of the Court of Justice of the EU defending freedom of expression simply ignored or contradicted. Much of the “censorship” that is alleged is already prohibited and confirmed via rulings such as the Scarlet case ([C-70/10](#)) and the eBay case (C-324/09), but these are conveniently never mentioned.

4. PLATFORM POLICY CHANGES IN TACKLING DISINFORMATION

While most companies rolled back measures against disinformation over the past years, major U.S. tech companies quickly did a U-turn to align with the Trump administration. They **scaled back content moderation and platform safety efforts, often adopting anti-censorship rhetoric to justify the shift**. The presence of Elon Musk, Jeff Bezos, Mark Zuckerberg, Sundar Pichai, and Tim Cook at Trump's 2025 inauguration underscored this new alignment.

In January, [Mark Zuckerberg](#) announced that Meta would end its cooperation with independent fact-checkers on Facebook and Instagram, replacing them with community notes. While limited to the United States, this announcement sent a troubling signal for Europe, raising the risk of similar measures being extended across the Atlantic. Soon after, [Google](#) informed the EU it would no longer use fact-checks in search results or YouTube videos for ranking or removal, despite commitments under the [Code of Practice](#).

The U.S. government has also warned digital companies [against complying](#) with EU and UK content regulations, giving platforms both political cover and a pretext to resist compliance. This intervention opens new fault lines in the regulatory sphere. Hence, this section reviews recent changes by several platforms, their potential impact on Europe, and possible responses.

PRIVILEGING USER-DRIVEN VERIFICATION

X pioneered community-driven moderation with Birdwatch and later [Community Notes](#), and [Meta](#) quickly followed after Trump's inauguration. This shift replaced collaboration with independent fact-checkers in the U.S., which Zuckerberg dismissed as [biased](#) and ineffective in restoring trust. While the company insists there are "no immediate plans" to end fact-checking in the [EU](#), signals suggest such a move could be on the horizon.

[TikTok](#) has also introduced user-driven moderation through its "[footnotes](#)" feature, though it continues to rely on professional fact-checkers and automated review. Crowd-sourced systems offer additional context, but their effectiveness remains [mixed](#): while they can reduce the [spread](#) of falsehoods, they are often [too slow](#) to contain viral misinformation in its early, most damaging stages.

In an understated developers' [blog post](#), Google announced the end of its ClaimReview programme, which had displayed fact-checking snippets directly in search results. The initiative, developed in cooperation with fact-checkers over nearly a decade, exposed millions of users to verified content at the point of search. [Experts](#) warned that its termination marks a serious setback for the visibility of fact-checked information.

A recent [report](#) by the European Fact-Checking Standards Network (EFCSN) flags that many major platforms are abandoning their commitments to fact-checking under the Code of Conduct on Disinformation. EFCSN notes that Google, YouTube, Microsoft (Bing Search and LinkedIn), TikTok, and Meta (Facebook and Instagram) have either scaled back their fact-checking efforts, withdrawn from key responsibilities, or have plans to do so. In January, Google, YouTube, and LinkedIn [unsubscribed](#) from their fact-checking commitments, shortly before the voluntary Code of Practice became a Code of Conduct under the DSA.

DISMANTLING TRUST AND SAFETY TEAMS

The steady dismantling of trust and safety teams has weakened platforms' capacity to address disinformation and harmful content. Human moderation has often been replaced by automation or outsourced labour. In [2023](#), Elon Musk [confirmed](#) the [closure](#) of Twitter's Election Integrity team.

TikTok is reportedly preparing to cut about 40% of its trust and safety team in [Germany](#), with similar reductions expected in the [UK](#), as it pivots toward AI-driven moderation. [Bloomberg](#) has reported concerns that such reliance on automation will allow coded hate speech, propaganda, child grooming, and other harms to persist and proliferate.

LOOSENING CONTENT MODERATION POLICIES (HEALTH, ELECTIONS, AND CLIMATE)

Some of the most consequential changes concern platforms' Terms of Service and content policies that are central to ensure a level of predictability for measures to prevent harmful or illegal content, as required under the DSA.

Relaxing or removing them has deeper implications than simply loosening moderation. **When a platform eliminates, for example, its misinformation policy, it erases the very category by which harmful content can be identified, measured, and sanctioned, even if terms of service are generally vague enough to permit the platform to remove misinformation, if they wish to.** What is no longer named, risks ceasing to exist as a problem: if COVID-19 misinformation is not defined as such, its circulation becomes increasingly normalised.

In this sense, the erosion of policy language does more than reduce enforcement capacity: it voids concepts like misinformation, hate speech, or discrimination of meaning within the platform environment. The result is both a loss of visibility and a dangerous mainstreaming of behaviour that may be harmful or even unlawful.

Since Musk's takeover, X has scrapped [crisis-](#) and [COVID-19](#)-related misinformation policies as well as some of its [civic integrity](#) safeguards. The concept of "[informational harm](#)" has also disappeared from its policies, as documented by the [Institut für Internet und Gesellschaft](#).

[Meta](#) has followed a similar trajectory. In 2023, it removed COVID-19 content labels and [rolled back](#) related misinformation rules. In 2025, it revised its [misinformation policy](#) to remove explicit references to "hoaxes" and "viral misinformation". Similarly, its Climate Science Center and Climate Info Finder disappeared from public-facing resources, suggesting a [deprioritisation](#) of climate information. These reversals are especially concerning because health and election misinformation have been areas of rare consensus for enforcement across platforms.

ERODING PROTECTIONS AGAINST IDENTITY-BASED DISINFORMATION

Hate speech rules are also under threat. X deleted passages prohibiting the "[misgendering or deadnaming of transgender individuals](#)" from its [policy on hateful conduct](#), and removed explicit recognition of "women, people of color, and LGBTQ+ individuals" as disproportionate targets of online abuse. Meta, meanwhile, has signalled it will follow broader U.S. trends of removing [DEI provisions](#).

These setbacks are particularly concerning because hate speech, which is unlawful, and [identity-based disinformation \(IBD\)](#) – targeting groups defined by gender, sexual orientation, race, or ethnicity – which is harmful though not illegal, should be seen as part of the same continuum. IBD fosters a culture in which stereotypes and falsehoods are normalised, creating the conditions that enable and reinforce hate speech. Unfortunately, the prospect of recognising IBD in platform policies is receding under these shifts.

SOFTENING INTERVENTIONS AGAINST VIOLATIONS

For policy violations, X has shifted from relying primarily on takedowns and bans to emphasising softer interventions, such as reducing the reach of contentious posts and accounts under its [civic integrity policy](#). This reflects its "[freedom of speech, not freedom of reach](#)" approach, where suspensions or permanent bans are now

reserved for only the most severe violations—illegal conduct, violent threats, targeted harassment, privacy breaches, or platform manipulation and spam, as noted by researchers in [Berlin](#).

Regarding AI-generated content, Meta’s 2024 [policy update](#) for Facebook, Instagram, and Threads follows a similar logic: prioritising transparency over removal to deflect accusations of restricting freedom of expression. Rather than deleting synthetic or misleading content, Meta now labels it with tags to indicate when it has been created or altered synthetically.

REDUCING PRIVACY PROTECTION

Evidence also points to the erosion of user privacy protections, particularly through the use of personal data to train AI systems.

One of the most controversial cases arose in April 2024, when Meta revealed plans to train its [AI models](#) on user interactions with AI tools as well as on public content shared by adults on its platforms. Although European users were offered an opt-out option, the plan sparked strong resistance. Germany took a leading role in opposing the move: a national consumer organisation sought an urgent injunction to halt Meta’s EU-wide AI training. While the attempt failed, Hamburg’s data protection commissioner [Thomas Fuchs](#), who led the challenge, has stated that the case is likely to reach the European Court of Justice (ECJ).

Even when not outright violations, such measures conflict with the spirit of Europe’s digital legal framework. **Tech companies’ push toward AI-driven development raises tensions with data protection rules, while simultaneous cutbacks in content moderation may leave them at odds with the DSA and related obligations.**

5. LEGAL AND STRATEGIC DEFENSES IN EUROPE AND GERMANY

A new battle is looming and escalating. Just as tariff negotiations between the United States and the European Union seemed to be wrapping up, Washington has threatened additional “[substantial](#)” tariffs, citing what it calls “discriminatory” legislation, particularly the DSA and the Digital Markets Act (DMA). At the same time, the US administration is considering [sanctions](#) on DSA implementers, potentially in the form of visa restrictions. According to [Reuters](#), U.S. diplomats in Europe have also been instructed to lobby against the DSA in an effort to have it amended or repealed.

While [European leaders](#) have so far demonstrated [determination and resilience](#), this hostile environment will test the strength of Europe’s regulatory framework, complemented by a series of emerging initiatives designed to reinforce it. What follows is a non-exhaustive overview of both, especially focusing on Germany.

EU REGULATION ON DISINFORMATION

This section recaps the core binding instruments of EU digital regulation, which form the backbone of its response to online challenges and are essential to keep in mind when addressing disinformation.

- **DSA** – The [Digital Services Act](#) regulates online intermediaries and platforms such as marketplaces, social networks, app stores, and content-sharing platforms. Its primary goals are to prevent harmful or illegal online activities (including the spread of disinformation), safeguard user safety and fundamental rights, and foster a fair and open online environment.
- **GDPR** – In force since 2018, the [General Data Protection Regulation](#) remains the EU’s flagship privacy and security law. It applies to all organisations targeting services to EU residents or processing personal data in the EU. With strict standards and fines reaching tens of millions of euros, GDPR is widely seen as a global benchmark.
- **DMA** – The [Digital Markets Act](#) establishes criteria to designate “gatekeepers” (i.e., large platforms with significant market power) and imposes obligations to prevent abuse of dominance, ensure fair practices, and leave space for competition. The DMA is a central pillar of the EU’s digital strategy.
- **EMFA** – The [European Media Freedom Act](#) aims to strengthen media pluralism and independence across the EU, reduce undue political or economic pressure, and facilitate collaboration across member states. It explicitly addresses the challenges of the digital era.

- **AI Act** –The EU’s [Artificial Intelligence Act](#) is the world’s first comprehensive AI law. It applies a risk-based approach, tailoring requirements to the potential risks posed by different AI systems, from minimal to unacceptable.

GERMANY IN THE LEAD OF RESEARCHER DATA ACCESS REQUESTS

Beyond this regulatory framework, German society is actively debating how best to respond to recent developments and how to position itself at this critical juncture. Some initiatives campaign for extensive researcher access to platform data, as mandated by the DSA, while others (discussed in the next section) focus on defending privacy protections they believe are threatened by certain platform practices.

In a landmark case, Democracy Reporting International (DRI) and the Society for Civil Rights (Gesellschaft für Freiheitsrechte, GFF) sued [X](#) at the Berlin Regional Court after the platform refused to grant researchers access to data under Article 40(12) of the DSA. The organisations sought to study X’s impact on the 2025 German federal election. The Court ruled that DRI was entitled to enforce its claim in Germany rather than in Ireland, where X’s European headquarters are located. This decision set an [important precedent](#), establishing that **national courts across the EU can hold platforms accountable when they fail to meet their data access obligations towards researchers.**

GERMANY AT THE FRONTLINE OF DIGITAL PRIVACY

Germany’s determination to protect personal privacy – shaped in part by its history of state surveillance – is widely recognised. Some observers often call it “[Europe’s most private country](#)”, while others describe its relationship with privacy as “[complicated](#)”. Legally, this priority is reinforced through the [Federal Data Protection Act](#) (Bundesdatenschutzgesetz, BDSG), which supplements the EU’s GDPR with national rules on how public authorities and private companies handle personal data, as well as the GDPR itself.

Perhaps the most illustrative episode is Germany’s long-running dispute with Google over [Street View](#). For years, the service was effectively unavailable because large numbers of residents objected to camera cars photographing their homes, leading to mass requests for façades to be blurred. This undermined the utility of the product until Google relaunched Street View in Germany in 2024.

Another emblematic case involves Green Party politician [Renate Künast](#). Since 2015, a false quote attributed to her has circulated on Facebook. Although Facebook removed individual posts when reported, Künast went to court in 2021 to demand that the platform proactively delete identical and near-identical (“kerngleiche”)

versions so she would not have to flag each one manually. [HateAid](#), a non-profit dedicated to fighting digital violence, played a key role in supporting her case. In January 2024, the Higher Regional Court of Frankfurt upheld a lower court ruling and rejected Meta's appeal. The court decided that once notified of one infringing post, Meta must also identify and remove "near-identical" copies – variants differing only slightly in font, typos, or added comments. Media coverage described the decision as requiring platforms to go beyond user reports and independently track down duplicates once a first notice has been given.

Germany also appears ready to confront privacy challenges in the age of artificial intelligence. As noted earlier, the country was at the forefront of trying to suspend Meta's EU-wide [AI training plans](#). Beyond these high-profile disputes, ordinary citizens are also taking action. In one recent case, a German woman sued Google after [intimate images](#) of her were leaked and circulated online without her consent. The content, tied to her identity, surfaced in Google search results under her name – raising further questions about platforms' responsibility for privacy protection.

DIGITAL SOVEREIGNTY AS A RESPONSE

Some voices in Germany are calling for greater [digital sovereignty](#) to reduce dependence on big tech. Suggested measures include expanding the use of open-source licences in public administration and fostering cooperation between the public sector and non-commercial actors. German experts highlight these steps as pathways to **reducing dependency on foreign digital infrastructure and platforms**.

Beyond national initiatives, European-level instruments are also available to counter external pressure. In force since 2023 but not yet applied, the [Anti-Coercion Instrument](#) (ACI) equips EU countries – individually and collectively – with a range of countermeasures when confronted with coercion from a foreign power. These include tariffs, restrictions on trade in services and intellectual property, and limits on access to foreign direct investment or public procurement. While originally designed to address China's economic retaliation against Lithuania, the German outlet [Netzpolitik.org](#) has recently suggested the ACI could also be directed at the United States in response to its pressure in the digital sphere.

Moreover, since Trump's first term, hundreds of volunteers have joined the Data Rescue Project to safeguard public datasets at risk of deletion or manipulation. The initiative tracks compromised and recovered datasets and develops tools for data recovery. Among its contributors is Cologne-based historian [Sebastian Majstorovic](#), whose expertise supports the preservation of data that might otherwise be lost.

6. CONCLUSION AND RECOMMENDATIONS

The fight against disinformation in Europe is entering a decisive phase. Awareness of the threat has never been greater, yet resilience is being eroded by hostile foreign and domestic actors, shifting U.S. politics, the retreat of online platforms from fact-checking and transparency commitments, and growing domestic political polarisation that deepens divides and weakens trust in institutions.

Germany captures this dual reality. Its strong privacy tradition, active civil society, and readiness to test the protections provided by the DSA before national courts give it the potential to be a frontrunner in defending information integrity. At the same time, political fragility and spurious but frequently unchallenged far-right efforts to reframe protective measures as censorship expose how vulnerable these gains can be. Division of powers in media regulation between the regional, national and EU levels also limits predictability and creates problems of coordination.

At the European level, the regulatory framework remains unmatched globally, but enforcement is challenging. As platforms roll back key policies, harmful content spreads unchecked, and behaviour once deemed unacceptable risks being normalised. Without consistent implementation, even the most advanced laws lose their force.

Resilience depends on three pillars. First, **strong enforcement of EU regulations** is essential to counter both platform resistance and external political pressure. Germany, with its courts already testing the limits of the DSA and its regulators pushing back against AI-related privacy risks, will be fundamental in showing that these safeguards can be made to work in practice.

Second, **active engagement of civil society and legal action** strengthens this effort. German organisations have already demonstrated how litigation and advocacy can expand data access, defend privacy rights, and challenge platforms' abuses. Their cases are setting precedents that shape enforcement not just nationally, but across the EU.

Third, **strategic autonomy and digital sovereignty** are also at stake. German debates on reducing dependence on big tech illustrate how national choices can reinforce Europe's resilience while still safeguarding fundamental rights.

Ultimately, defending Europe's information space requires more than legal instruments. It also requires long-term political will and financial resources. Support for defenders and their independence must be guaranteed, including through **dedicated EU budget lines such as the Multiannual Financial Framework (MFF)**. **Without secure funding and institutional backing, the work of civil society remains precarious, leaving Europe exposed to manipulation.**

Strengthening Europe's democratic resilience requires affirming the legitimacy of counter-disinformation work, challenging efforts to brand it as censorship, and upholding accountability mechanisms that protect democracy, free expression, and fundamental rights – grounded in Germany's example but extending across the EU.