FIMI-ISAC

FDEI PROJECT

Report

Regulatory Challenges & Gaps in Addressing Systemic Platform Abuse

Authors:
Maria Giovanna Sessa, Raquel Miguel Serrano, Joe McNamee – EU DisinfoLab

EU DISINFOLAB

Table of Contents

Introduction

This report marks the culmination of a year-long effort to monitor elections across four countries by the "FIMI Defenders for Election Integrity" project, drawing on the collective work of partners engaged in exposing Foreign Information Manipulation and Interference (FIMI). Its purpose is to take a step further from incident documentation to reflect on what these findings reveal about **systemic violations and potential breaches of the EU Digital Services Act (DSA)**. The exercise is not a legal assessment, but rather a bridge between research and policy: an attempt to show how civil society monitoring can inform real accountability and guide future enforcement.

Because the analysis builds on secondary materials provided by partner organisations, it remains necessarily interpretative. Each case offers a window into how platform governance operates in practice, how certain forms of manipulation persist despite clearly defined but poorly enforced rules, and how the boundaries between illegal and permissible behaviour continue to blur. By revisiting twelve descriptive Incident Alerts (IAs) through a DSA lens, the report aims to identify **what evidence is still missing to transform qualitative observations into actionable evidence for current and future DSA infringement proceedings**.

The report is organised in three parts. It first outlines the methodology guiding the project. It then turns to the analysis, beginning with an overview of the selected cases before exploring their relevance under the DSA and platform Terms of Service (ToS). The final section reflects on emerging lessons and best practices – how researchers and policymakers can work together to close evidence gaps, strengthen systemic risk monitoring, and ensure that future election cycles are met with a more resilient digital environment.

Methodological note

The structure of this report follows a template developed by EU DisinfoLab for the "FIMI Defenders for Election Integrity" project. The template was intended to be applied to one-page descriptions of FIMI incidents produced by partners, referred to as Incident Alerts (IAs). It is designed to analyse repeated infringements of the DSA that may constitute systemic risks due to insufficient mitigation. While this analytical framework was originally intended to be integrated directly into each IA, practical constraints – such as time limitations, heterogeneous expertise, and limited resources among the contributing authors – prevented its full application. Therefore, this report seeks to bridge that gap, offering a consolidated analysis that extracts actionable insights on systemic infringements of the DSA from the descriptive IAs.

The analysis is conducted in three main steps. Firstly, we identify the infringement type. Each incident is examined to determine whether it involves a suspected content-related or behavioural violation. Actions taken by researchers are also documented, especially when they report potential violations to platforms, as this can eventually reinforce accountability claims.[1] The results are summarised in the overview of cases (section 3.I). Secondly, we assess the problematic or illegal nature of the alleged violation. At this stage, we evaluate whether the identified behaviour or content may breach national or international law, triggering the application of certain DSA provisions (section 3.II). These findings enable us to assess platform actions (or the lack thereof) in addressing and mitigating systemic risks to electoral integrity. When assessing systemic infringements, particular attention is given to **the recurrence of incidents and the persistence of platform inaction or inconsistent enforcement**, even when the risks or operations are well documented. Thirdly, we examine potential violations of platform ToS or internal policies (section 3.III), viewed as an additional layer of accountability in addressing "illegal or otherwise harmful content", as worded by the DSA.

[1] The assessment applies if certain criteria are met. Specifically, it must be shown that the notices were "sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content" (Article 16 DSA), or against content alleged to breach the platform's ToS (Article 14 DSA). Where these conditions are met, platforms may be held accountable for failing to act expeditiously on illegal content and, more broadly, for breaching Article 14 obligations to enforce their own ToS (since illegal content typically constitutes a ToS violation). This analysis assumes that the operators submitted properly formulated notices, as the underlying data are not directly accessible.

When looking into potential DSA violations, our primary objective is to identify what types of evidence are currently missing to substantiate allegations of potential infringements of specific DSA provisions. This step is essential to bridge the gap between descriptive or anecdotal observations of misleading content or deceptive behaviour and data that would enable regulators to take meaningful action when illegality is found. **By highlighting the evidentiary elements that need to be collected, we aim to inform future data collection strategies**. The ultimate goal is to ensure that researchers, while conducting their monitoring activities, also build stronger cases that not only enhance understanding of the full scope of FIMI operations but also enable concrete, policy-oriented interventions to stop them.

Regarding the case selection, three IAs were chosen for each of the four countries covered by the project. This selection aims to reflect the diversity of campaigns, platforms, and tactics, techniques, and procedures (TTPs) employed in FIMI activities. The objective was to ensure a balanced representation across different contexts and operational typologies. The analytical process relies primarily on the content of the IAs, cross-referenced against the DSA and the updated platform policies available at the time of writing.

In this regard, we acknowledge that Moldova, as a non-EU country, currently falls outside the scope of the DSA. However, as an EU accession candidate, considering how the legislation might be applied in this context offers valuable insights. This exercise not only helps assess the state of Moldova's digital environment but also provides a useful test case for the DSA's potential effectiveness in curbing influence campaigns – particularly given the country's status as a frequent target of Russian interference. Moreover, it allows for a comparison with EU member states where the DSA is already in force, helping to identify both similarities and key differences in enforcement contexts.

Finally, a methodological disclaimer is warranted: the data used in this report are secondary, relying on the work of partner organisations, as we did not have access to disaggregated datasets or primary investigative material. We therefore assume the accuracy of the information provided in the IAs; for example, when an IA attributes an operation to a sanctioned entity, this attribution is accepted as valid for the purposes of this analysis.

Analysis

I) Case selection: overview of the Incident Alerts

Each FIMI incident targeting elections in the four countries reflects distinct tactics but converging trends. The commonly promoted pro-Russian narratives – whether supporting aligned candidates or discrediting national government and supranational institutions such as the EU and NATO – appear borderline,[2] yet do not necessarily constitute violations under national and/or EU law, or platform ToS. More revealing, however, are the behavioural indicators: coordinated inauthentic activity, impersonation, and cross-platform amplification are consistent with the FIMI playbook. Together, these cases demonstrate a broad and adaptive ecosystem of foreign information interference, where malign actors exploit platform loopholes and regulatory gaps, sustaining their activities even after exposure or finding ways to circumvent sanctions.

The inconsistent removal of Doppelgänger-related X posts (IA 0058), TikTok accounts impersonating Polish candidates (IA 0070), and investment scam ads (IA 0096) provide further evidence of the **selective and opaque nature of platform moderation**. Platforms' inconsistent oversight and weak regulatory implementation emerge as a common shortcoming across cases. This challenge is even more concerning in Moldova, which lacks the protections of EU membership – creating conditions that risk normalising foreign interference and eroding civic discourse. The findings underscore the urgent need for systematic follow-up on enforcement outcomes and greater resourcing for researchers and defenders, who continue to face significant constraints in tracking the full lifecycle of such operations across multiple digital ecosystems.

Before delving into the incidents described in Tables 1 to 4, this section highlights the main takeaways.

Sanctioned entities

Several incidents involve **sanctioned entities whose content should not be hosted on major platforms** due to "the prohibition to make funds and economic resources available to them". For instance, the Social Design Agency is behind the Doppelgänger operation (IA 0058), while the Foundation to Battle Injustice is linked to the Storm-1516 operation (IA 0044). The latter not only spread fabricated news targeting German politicians but

[2] Social media platforms use the term "borderline content" to describe material that does not explicitly violate their community standards or the law but comes close to doing so, occupying a gray area of acceptability.

also appears to cross into defamation, a criminal offence under German law. Similarly, a YouTube channel operated by sanctioned outlet Radio Belarus (IA 0069) broadcast disinformation against Polish opposition candidate Rafał Trzaskowski, violating Poland's electoral silence law. Nevertheless, both the channel and the video remain accessible months later.

State-linked media

Other cases reveal how state-linked media continue to circumvent sanctions and bans. The persistence of the RT Deutsch network (IA 0047) demonstrates how sanctioned outlets still remained accessible to German-speaking audiences via mirror sites and alternative platforms despite official restrictions. In the Czech Republic, the re-emergence of Russian state-affiliated outlet NeČT24 (IA 0097) – a rebranded successor to the sanctioned Sputnik – enabled the promotion of election fraud narratives and deep state conspiracies targeting national institutions, including the Constitutional Court. In Moldova, a Belarusian state-linked YouTube campaign (IA 0084) published over 50 videos promoting pro-Russian figures such as former president Igor Dodon and discrediting pro-European actors. Although not a state media outlet, the Rybar network (IA 0091) benefitted from amplification by Infodefense and Pravda. This demonstrates how nominally independent channels are integrated into state-aligned influence networks, **blurring the boundaries between direct state control and orchestrated proxy activity**.

Known campaigns

Several well-known campaigns reappeared across multiple countries, showing that exposure of the incident through the compilation of the IA or even notices to platforms rarely results in sustained takedowns or platform accountability. In Poland, the Doppelgänger operation (IA 0058) persisted online despite clear indicators of CIB such as bots and fabricated personas. X concluded that the reported content did not violate its policies, reflecting a decision not to enforce its own ToS, even under the DSA framework. In Germany, Storm-1516 (IA 0044) or Overload (IA 0046) remained available to wide audiences, posing tangible risks to civic discourse and election integrity. In particular, Overload used AI-driven amplification to circulate false claims about terrorist threats on X, displaying how manipulation tactics can translate into real-world risks.

Ads and scams

FIMI campaigns can also be financially motivated, blurring the line between fraud and disinformation. A large-scale deceptive advertising campaign on Meta platforms in the

Czech Republic, operated by the fake page "Šokující Česká 24" (IA 0096), ran hundreds of fraudulent ads using spoofed news headlines to reach millions of users and lure them to fake investment sites. The use of ads for malign purposes is not new, yet its persistence reveals how platform advertising systems can be weaponised. While some fraudulent Meta ads were removed following Rapid Response System (RRS) reporting, others remained operational. Similar patterns emerged in Moldova, where Meta accounts managed from Russia and South East Asia (IA 0085) used sponsored content to meddle in the elections. Collectively, these cases demonstrate how **financial deception and political interference converge with algorithmic manipulation to exploit attention economies and platform loopholes**.

Table 1. Overview of the German Incident Alerts

Germany	IA 0044: Storm-1516 and R-FBI: Russian attempts to interfere in the German election	IA 0046: Overload-coordinated disinformation network uses AI, media impersonation to target German election	IA 0047: Uncovering RT Deutsch's content-laundering ecosystem
Description	Russian state-linked operations Storm-1516 and the Foundation to Battle Injustice ran a cross-platform coordinated operation campaign (>25 million views), discrediting CDU and Green politicians, with AfD-linked amplification.	Operation Overload used AI-generated audio and media impersonation through 48 X accounts and over 6,000 bots to spread disinformation about alleged terrorist threats and allegedly corrupt politicians ahead of the German elections.	RT Deutsch has been evading bans through a network of automated aggregators and mirror websites that repost its content for German-speaking audiences despite restrictions.
Platforms	Facebook, Instagram, Telegram, TikTok, X, YouTube	X	Odysee, Rumble, Telegram, VK, X
Suspicious content	→ Disinformation; → Fabricated news articles; → AI-generated content (deepfakes); → False allegations and potential defamation (illegality).	→ Disinformation about alleged terrorist threats; → AI-generated content.	→ Pro-Russian propaganda.
Suspicious behaviour	→ Fabricated news websites; → Baiting influencers to spread the content; → The Foundation to Battle Injustice is a sanctioned entity (illegality).	→ Impersonation of media, government agencies, and academic institutions, among others (illegality). → Bot-driven amplification.	→ RT is a sanctioned entity (illegality).
Actions taken	→ Cases flagged to EU and German authorities and social media platforms.[3]	→ Exposure via the IA but no reporting to platforms.	→ None indicated.

[3] Based on the IA, it is unclear whether all the content was reported to all the platforms and whether it was reported as illegal content.

Table 2. Overview of the Polish Incident Alerts

Poland	IA 0058: Illegal influence operation Doppelgänger continues: targeting the Polish elections	IA 0069: Sanctioned Belarusian media channel violating electoral silence law: discrediting presidential candidate Rafał Trzaskowski	IA 0070: Murky accounts on TikTok impersonating Polish presidential candidates and political parties
Description	279 X posts linked to the Doppelgänger network (gaining >1.2 million views).	YouTube video attacking Polish politician Rafał Trzaskowski (minimal views and likes) broadcasted by Radio Belarus.	107 TikTok accounts impersonating Polish candidates and parties (one video gained >8.1 million likes).
Platforms	X	YouTube	TikTok
Suspicious content	→ Pro-Russian propaganda.	→ Disinformation on Presidential candidate Rafał Trzaskowski.	/
Suspicious behaviour	→ Bots; → Inauthentic social media comments; → Fabricated personas; → Social Design Agency is a sanctioned entity (illegality).	→ Radio Belarus is a sanctioned entity (illegality); → Violation of the Polish electoral silence law (illegality).	→ Impersonation of parties and politicians (illegality); → Concealed network identity.[4]
Actions taken	→ Posts reported to X via its DSA-mandated reporting interface, but X replied that they did not constitute a violation; → IA shared with Polish government entities and media.	→ Channel reported to YouTube but no update on platform response (both the channel and the video are still available as of 6/10/2025).	→ Accounts reported but while some were removed others remained active as the platform did not consider them in violation of its policy against impersonation.

[4] As the origin is unknown, the incident's classification as FIMI remains uncertain.

Table 3. Overview of the Moldovan Incident Alerts

Moldova	IA 0084: Moldova elections targeted by Belarusian YouTube disinformation campaign	IA 0085: Vietnamese bots boost pro-Kremlin channels meddling in Moldovan elections	IA 0091: REST Media-Rybar Link: Coordinated Pro-Kremlin Network Targeting Moldova
Description	At least 54 videos (gaining >3.8 million views) published by five Belarusian channels (CTVBYvideo, ont_by, sbbytoday, beltavideo, and news.by_btrc).	Facebook and Instagram accounts branded as "Moldavian Calendar", administered from Russia and Thailand, engaging in CIB (gaining 31.5k followers).	REST Media's website and social media (gaining 3.1 million views on TikTok), linked to the Rybar network.
Platforms	YouTube	Facebook, Instagram	TikTok, X, Telegram
Suspicious content	→ Disinformation through claims of rigged elections; → Pro-Russian propaganda.	→ Disinformation against Sandu's government; → Pro-Russian propaganda.	→ Pro-Russian propaganda.
Suspicious behaviour	→ Coordination among channels; → Belarusian state-controlled channels.	→ Inauthentic social media accounts and ads; → Artificial amplification; → False news sites.	→ Fabricated website (inauthentic news and covert identity); → Concealed network identity (Cloudflare masking); → Coordinated amplification across platforms and by Infodefense, Pravda, and pro-Russian influencers.
Actions taken	→ None indicated.	→ None indicated.	→ None indicated.

Table 4. Overview of the Czech Incident Alerts

Czech Republic	IA 0096: Deceptive Meta ads via "Šokující Česká 24" drive users to fake investment platform	IA 0097: Russian state affiliated outlet NeČT24 promoting election fraud narratives	IA 0101: Coordinated TikTok bot network targeting Czech elections
Description	316 Meta ads, run by deceptive Facebook Page "Šokující Česká 24", using fake Czech news headlines and spoofed domains to redirect users to fraudulent investment sites promoting the fake "CisporaSeek" platform (reaching nearly 3.4 million EU users).[5]	Social media presence of Russian state-linked outlet NeČT24, a rebranded successor to sanctioned Czech Sputnik.	146 TikTok accounts (mostly bots, totalling 10.5 million likes) amplified pro-Russian narratives though automated posting, repetitive hashtags, and meme-based propaganda.
Platforms	Facebook and Instagram	Facebook, X, Telegram	TikTok
Suspicious content	→ Disinformation about Czech public figures; → Clickbait political content.	→ Disinformation about election fraud and deep state conspiracies.	→ Pro-Russian propaganda.
Suspicious behaviour	→ Scam ads; → Redirection to inauthentic websites promoting a fake investment platform (illegality); → Impersonation of media and trusted institutions (illegality).	→ Ties to Sputnik, which is a sanctioned entity (potential illegality).	→ Bot accounts; → Automated posting.
Actions taken	→ Page reported to Meta through the Rapid Response System (RRS) (221 out of 316 ads were removed)[6]	None indicated.[7]	→ Accounts reported to TikTok accounts flagged using the RRS, but no update on the outcome.

[5] The incident's classification as FIMI is uncertain, as the only indicator reported in the IA is the presence of "Russian-language HTML comments".
[6] The IA does not specify whether an explanation was provided for the ads that were not removed.
[7] We flag that IA 0098, titled "Sputnik continuation NeČT24 created a new Facebook page ahead of the Czech elections" mentions that all NeČT24 social media were reported to the respective platforms, but no additional information is provided on the outcome.

II) Potential DSA violations: building cases for systemic risk infringement

This section outlines an analytical exercise for evaluating the applicability of the EU Digital Services Act (DSA) to the twelve FIMI Incident Alerts (IAs) spanning Germany, Poland, Moldova, and the Czech Republic. The objective is to assess how existing DSA provisions could apply to the observed behaviours of Very Large Online Platforms (VLOPs), particularly regarding systemic risk assessment and mitigation, and other hosting providers.

While the DSA provides a harmonised EU framework, it is important to clarify that this analysis is illustrative and does not represent a legal determination of infringement. Furthermore, the DSA does not apply to non-EU jurisdictions such as Moldova, except when the service provider has a substantial connection to the Union. Nonetheless, simulating the DSA's application to these cases is crucial, given the country's EU candidate status, its diaspora communities, and the persistence of Russian interference.

Likewise, certain platforms do not meet the 45 million monthly active users' threshold – such as Odysee, Rumble, VK (IA 0047), and Telegram (IA 0044, 0047, 0091, 0097) – and are therefore not subject to the DSA's additional obligations for VLOPs. Nevertheless, the fact that these smaller platforms appear repeatedly across several incidents in Germany, Moldova, and the Czech Republic highlights how malign actors exploit less regulated environments.

Together, the IAs show recurring FIMI patterns – including impersonation, the use of synthetic media, ad monetisation, coordinated amplification, and the concealment of network infrastructures – all facilitated by inconsistent platform enforcement, which in some cases even enables evasion of sanctions. As a result, several DSA provisions may apply or be considered potentially violated.

Hosting liability

If it was reported in a way that generates "actual knowledge", then platforms become accountable

For starters, Article 6 (hosting liability) states that platforms are shielded from liability only if they act expeditiously after obtaining specific knowledge of the illegality of specific content. Various incidents are part of well-known campaigns such as Doppelgänger, Overload, or Storm-1516, and in many cases researchers submitted formal reports through DSA-mandated tools, notifying platforms about content linked to

sanctioned entities such as the Social Design Agency (0058), the Foundation to Battle Injustice (IA 0044), or RT (IA 0047). Failure to act after such notifications could constitute a breach of this duty. Evidence would need to comprise: **copies of Article 16-compliant notices (or authority orders) establishing actual knowledge** – including content IDs or URLs, timestamps, notifier details, and the applicable legal ground – plus **platforms' receipt IDs and internal logs** showing when the notice (or order) was received and when action was taken (or not), **decision records, and timestamped captures**[8] proving the content remained available beyond a reasonable ("undue delay") window. In the cases regarding sanctioned entities, proof of attribution should also be included.

Terms of Service

If platforms have (self-defined) rules, they must follow them

Article 14 (ToS) requires consistent and proportionate enforcement of the platform's own rules. In practice, platforms often fail to apply their ad standards, community guidelines on coordinated inauthentic behaviour, or impersonation policies consistently. Evidence-wise, a comprehensive pack should contain **timestamped captures of the exact ToS** in force at the time of reporting, in all relevant EU languages, together with a concise, machine-readable summary outlining available remedies and redress. These should be compared against the platform's Statements of Reasons, using before-and-after archives to show how the cited rule was (not) applied. The provision demands that the required information is easily accessible and not scattered across multiple links. Moreover, the ToS must explicitly disclose the use of algorithmic decision-making, the extent of human review, and the procedural rules governing the internal complaint procedures.

Notice-and-action and statement of reasons

If platforms act on it, they must explain it

Article 16 (notice-and-action) and Article 17 (statement of reasons) oblige platforms to process reports diligently and to issue transparent, reasoned responses. Several cases – such as Doppelgänger-related X posts (IA 0058) or murky TikTok accounts (IA 0070) during the German elections – show platforms rejecting or delaying removal without clear or procedural justification.

[8] Archived webpages are always preferable to screenshots, as they are more secure and admissible as evidence in legal proceedings.

To prove a violation of Article 16, evidence should include **copies of the notice form submitted** (showing the URLs or content IDs, legal basis, and timestamps), the **successful submission receipt**, and **any follow-up messages including decision times, stated reasons, final decision on action or inaction, and available redress mechanisms** (e.g., internal complaint-handling, out-of-court). Moreover, screenshots or archived versions of the notice interface demonstrating it is easily accessible, electronic, and supports precise item reporting (e.g, of multiple items if applicable) are also valuable evidence.

For every restriction or removal of content (or lack thereof) under Article 17, it is important to obtain the issued statement of reasons and check it comprises all mandated elements: what measure was taken (e.g., remove, restrict visibility, suspend payments, etc.), plus territorial scope and duration; the facts and circumstances for the decision, including whether it followed an Article 16 notice or the platform's own-initiative; whether automated means were used; the legal ground and why the content is illegal (for illegal content) or the contractual ground and/or why the content breaches it (for ToS violations); and clear, user-friendly information on redress options (internal complaints, out-of-court, judicial).

This is an opportunity to reiterate the **importance of reporting each piece of content or account through the official channels of every relevant platform, as only documented notifications can trigger platforms' DSA obligations**. In half of the cases (IA 0046, 0047, 0084, 0085, 0091, 0097), researchers authoring the IAs missed the opportunity of submitting formal reports, and such omissions ultimately perpetuate platform inaccountability by leaving potential violations undocumented.

Systemic risk assessment and mitigation

If there are risks for democracy, designated VLOPs must anticipate and alleviate them

Under Article 34 (systemic risk assessment) and Article 35 (systemic risk mitigation), VLOPs must identify and assess systemic risks related to civic discourse, electoral integrity, and information manipulation, among other things. The continuation of years-long FIMI campaigns, the repetitive use of coordinated amplification tactics, and the ability of recurrent perpetrators (including sanctioned entities) to circumvent restrictions in the run-up to elections highlight failures in risk anticipation and alleviation. To demonstrate how the collected incidents may indicate a systemic risk that the platform should have assessed under Article 34, researchers should document **links between individual items to broader platform-level patterns**. This includes recording **timestamps, geographic, or linguistic availability within the EU; reach and propagation metrics** (views, shares, and reposts), and **identifying where the content appeared** (e.g.,

in recommendation feeds, search results, notifications, or paid ads). The evidence should spell out **which parts of the platform helped the content spread** or stay up – for example the recommender system, how moderation was (or was not) applied and how fast, any paid promotion or targeting, and the data signals the platform used to deliver it. It should also show **signs of coordinated boosting** – for example, amplification of the same content across platforms or by automated accounts – and note any **earlier warnings** the platform received (e.g., trusted-flagger reports, prior removals, or "statement of reasons"). The ultimate goal is to clearly show that the issue is a recurring pattern and not just a one-off situation.

Under Article 35, the focus shifts to identifying and documenting failures to implement mitigation measures to which platforms have publicly committed. Researchers should verify whether the announced safeguards were actually activated in practice. These may include the labelling of state-affiliated or AI-generated content, the demotion or demonetisation of repeat offenders, and the takedown or restriction of problematic material. When such interventions are absent and the related content remains accessible, this indicates possible enforcement gaps. Platforms that have pledged to apply specific mitigations should be able to provide verifiable records showing when and how these were executed. To substantiate such assessments, researchers should seek **supporting evidence that demonstrates whether enforcement took place in measurable terms** – for instance, logs or datasets showing moderation actions over time, records of content labelling or removal, or documentation of ad-level interventions (such as the blocking of redirects to external fake or scam websites, or the suspension of monetisation for sanctioned entities). Comparing these records with the platforms' stated commitments would allow for a clearer evaluation of **whether promised safeguards translated into tangible outcomes**, or whether problematic content continued to reach users despite the announced controls. On an additional note, access to data requests based on Article 40 are fundamental to identifying, measuring, and independently verifying systemic risks.

Ad transparency

If platforms sell ads, they must show who paid for them

Ad-related provisions apply to some of the IAs. Article 26 (advertising on online platforms) and Article 39 (additional ad transparency for VLOPs) potentially apply to the Vietnamese bot network (IA 0085) and the fraudulent investment scheme (IA 0096) targeting the Moldovan and Czech elections respectively. To document potential non-compliance under Article 26, researchers should capture **timestamped archived versions or screenshots of the ads as they appeared in the user interface, noting any**

missing or unclear sponsorship labels or "why am I seeing this?" label. Each record should also include the ad creative, landing URL, and indication of the natural or legal person on whose behalf the ad is presented.

Under Article 39, which requires VLOPs to maintain **publicly accessible ad repositories**, researchers should query the relevant repository for the captured ad and archive the results (or lack thereof). They should verify whether **mandatory fields** – advertiser identity, ad content and creative, display period, targeting parameters, and audience reach by Member State – are present and consistent with the live ad.

Recommender systems

If platforms boost it, they must show how

Additional considerations should be made regarding Article 27, which mandates transparency around recommender systems. The selected IAs illustrate a broader structural opacity: it remains impossible for external researchers to determine whether the content documented was algorithmically recommended to users or whether it would have appeared organically in non-profiled accounts. One exception might be the coordinated TikTok bot network targeting Czech elections (IA 0101), where amplification through the "For You" page was reported – illustrating how recommender-driven visibility can serve as a central vector for coordinated manipulation. Overall, this uncertainty prevents the independent assessment of how recommender systems may have amplified or accelerated the spread of FIMI. While platforms disclose limited information about ranking and personalisation parameters, current reporting practices fall short of enabling meaningful scrutiny of algorithmic amplification effects.

Access to data

If researchers are entitled to the data, platforms must give it to them

This brings us to a final point regarding access to data as defined by Article 40. At present, it remains difficult to go beyond qualitative, observational reporting of what researchers see on platforms. This can lead to missing accounts within the same network, an inability to follow-up actions on reported content, or a lack of visibility of whether additional measures – such as demonetisation or downranking – were applied. To address this, platforms must provide standardised, timely, and meaningful access to data to researchers, in full respect of relevant legal obligations, such as the GDPR, to bridge the current evidence gap and enable a more substantiated assessment of DSA compliance. This would allow independent scrutiny of risk assessment (Article 34), support the

evaluation of mitigation efficacy (Article 35), and strengthen the empirical foundation for regulatory oversight under the DSA.

The rest of this section presents a hypothetical scope of application of the DSA across the twelve IAs, underscoring the DSA's potential to serve as a comprehensive accountability framework for assessing platform diligence, transparency, and systemic risk mitigation in the face of coordinated influence operations.

Tables 5 to 8 assess the potential DSA violations based on the information provided in the IAs and detail what evidence is needed to prove them.

Table 5. Potential DSA violations in German Incident Alerts

Germany	IA 0044: Storm-1516 and R-FBI: Russian attempts to interfere in the German Election	IA 0046: Overload-coordinated disinformation network uses AI, media impersonation to target German election	IA 0047 Uncovering RT Deutsch's Content-Laundering Ecosystem
Art. 6 Hosting liability	→ The platforms were notified of the incident and were aware of the Storm-1516 operation but failed to act; → Evidence gap: Proof of reporting the posts[9] and that they are operated by a sanctioned entity (Foundation to Battle Injustice).	/	/
Art. 14 Terms of Service	→ If the posts are linked to a sanctioned entity (Foundation to Battle Injustice), posting their content may be illegal.[10] Platforms may have not diligently and proportionately applied their policies on CIB, influence operations, and election integrity; → Evidence gap: Proof[11] that the posts involved in the incident are linked to a sanctioned entity.	→ X may have not properly enforced its authenticity policy and its trademark policy; → Evidence gap: Proof that the accounts and bots or engage in impersonation of news media, government agencies, and academic institutions.	→ If the social media posts are linked to a sanctioned entity (RT), posting their content may be illegal; → Evidence gap: Proof that the accounts involved in the incident are operated by a sanctioned entity.

[9] This should consist of submitted notices and receipts to establish actual knowledge.

[10] A distinction must be drawn between illegality and a ToS violation. Illegality is a matter of law, not contract, and should not be collapsed into a platform's ToS. Any reference to a ToS breach here serves only to establish a potential Article 14 issue, not to reclassify unlawful content as a mere contractual matter. In this case, the conduct appears to breach the platform's ToS clause prohibiting uses that violate applicable law – independently of and beyond ToS.

[11] This evidence should come in the form of a timestamped capture of the ToS in force at the time of reporting, compared against the platform's Statements of Reasons, using before-and-after archives to show misapplication of the cited rule.

Art. 16 Notice and action	→ The platforms may have failed to act on notices in a timely, diligent, non-arbitrary manner and give clear reasons for rejecting notices demanding removal of the posts; → Evidence gap: Submitted notices with all the required elements.[12]	/	/
Art. 17 Statement of reasons	→ Platforms may have failed to issue compliant statements of reasons explaining the legal basis for and the effects of their decisions, as well as redress mechanisms; → Evidence gap: The platforms' statement of reasons for each reported post showing all the required elements.[13]	→ If X was to remove the content on grounds of illegality, it should issue a statement of reasons explaining its decision; otherwise, this would constitute a violation; → Evidence gap: The platform's statement of reasons for each reported post showing all the required elements.	→ If X was to remove the content on grounds of illegality, it should issue a statement of reasons explaining its decision; otherwise, this would constitute a violation; → Evidence gap: The platform's statement of reasons for each post(s) on which action was taken, showing the required elements.
Art. 34 Risk assessment	→ VLOPs may have failed to adequately assess risks to electoral processes in Germany between Nov. 2024-Feb. 2025; → Evidence gap: Timestamped risk assessment records before the German elections and prior analysis of the Storm-1516 campaign.[14]	→ X may have failed to properly assess risks related to civic integrity and the well-known Overload operation ahead of the German elections; → Evidence gap: Timestamped risk assessment records before the German elections and prior analysis of the Overload campaign.	→ X may have failed to properly assess risks stemming from state-controlled media circumventing EU sanctions and content restrictions; → Evidence gap: Timestamped risk assessment records before the German elections and prior analysis of RT-affiliated content.

[12] This includes: URLs and exact timestamps, platform receipt IDs, communication logs showing decision times and stated reasons, final outcomes, notice of available redress, and proof that the notice interface is easily accessible, electronic, and supports precise item reporting.

[13] These are: the type of decision, its territorial scope and duration, the facts and circumstances leading to it, whether automation tools were used, the legal or contractual ground, and options for redress.

[14] One should remember that the goal is to show that the issue is systemic and not episodic. Archived evidence should display the EU availability, outreach, and platform presence of the content. It should identify how the platform design helped proliferate the content, document coordinated behaviour, and prior warnings received by the platforms.

Art. 35 Risk mitigation	→ VLOPs may have failed to deploy effective, proportional mitigations (e.g., synthetic-media labels, demotion, removal) to curb influence operation from sanctioned entities; → Evidence gap: Documented election integrity measures active during the election period and enforcement logs[15] against Storm1516-related activities.	→ X may have inadequately mitigated foreseeable systemic risks (e.g., labels, downranks, takedowns) allowing the operation to target German audiences; → Evidence gap: Documented election integrity measures active during the election period and enforcement logs against Overload-related activities.	→ X may have not implemented effective mitigation measures (e.g., labels, demotions, deplaforming of mirror or aggregator domains pointing to RT-related material; → Evidence gap: Documented election integrity measures active during the election period and enforcement logs against RT-related activities.

[15] The goal is to verify whether announced safeguards were actually enforced (e.g., stopping electoral interference).

Table 6. Potential DSA violations in Polish Incident Alerts

Poland	IA 0058: Illegal influence operation Doppelgänger continues: targeting the Polish elections	IA 0069: Sanctioned Belarusian media channel violating electoral silence law: discrediting presidential candidate Rafał Trzaskowski	IA 0070: Murky accounts on TikTok impersonating Polish presidential candidates and political parties
Art. 6 Hosting liability	→ X was notified of the incident and is aware of the Doppelgänger operation but failed to act; → Evidence gap: Proof of reporting the posts and that they are operated by a sanctioned entity (Social Design Agency).	→ YouTube was notified of the channel's visibility in Poland and the EU but failed to act; → Evidence gap: Proof of reporting the channel and that it is operated by a sanctioned entity (Radio Belarus).	→ TikTok was notified about the murky accounts but failed to act consistently; → Evidence gap: Proof of reporting the accounts.
Art. 14 Terms of Service	→ If the posts are linked to a sanctioned entity (Social Design Agency), posting their content may be illegal; → Evidence gap: Proof that the accounts involved in the incident are operated by a sanctioned entity.	→ If the Belarusian media is a sanctioned entity, posting its content may be illegal; → Evidence gap: Proof that the channel is operated by a sanctioned entity.	→ The unmoderated accounts may violate TikTok's policy against impersonation; → Evidence gap: Proof that the accounts engage in impersonation of politicians or parties.
Art. 16 Notice and action	→ X may have failed to act on notices in a timely, diligent, non-arbitrary manner and give clear reasons for rejecting notices demanding to remove the posts; → Evidence gap: Submitted notices for each post with all the required elements.	→ YouTube may have failed to act timely and diligently on the 15 May notice, as the channel remained EU accessible and uploaded the 17 May video; → Evidence gap: Submitted notices for the video (and channel) and with all the required elements.	→ TikTok may have rejected notices or delayed action without clear, non-arbitrary reason and without a sufficiently accessible, precise reporting path and redress; → Evidence gap: Submitted notices for each account with all the required elements.

Art. 17 Statement of reasons	→ X's rejection email may have not met the DSA's statement of reasons requirements; → Evidence gap: X's statement of reasons for the flagged posts showing all required elements.	→ If YouTube declined removal or geoblocking, it may have failed to issue an adequate statement; → Evidence gap: YouTube's statement of reasons for the flagged video showing all the required elements.	→ For the unmoderated accounts, TikTok may have failed to issue compliant statements of reasons; → Evidence gap: TikTok's statement of reasons for each retained account showing all the required elements.
Art. 34 Risk assessment	→ X may have failed to properly assess risks associated with the Doppelgänger operation, CIB, and Polish-speaking content; → Evidence gap: Timestamped risk assessment records before the Polish elections and prior analysis of the Doppelgänger campaign.	→ YouTube's most recent assessment may have not sufficiently identified risks for foreign state media breaching Polish electoral silence rules; → Evidence gap: Timestamped risk assessment records before the Polish elections and prior analysis of Radio Belarus-related activities.	→ TikTok may have failed to adequately assess the systemic risks from impersonation and fabricated personas during the Polish elections; → Evidence gap: Timestamped risk assessment records before the Polish elections.
Art. 35 Risk mitigation	→ X may have inadequately mitigated systemic risks allowing the Doppelgänger operation to target Polish audiences during the elections; → Evidence gap: Documented election integrity measures active during the election period and enforcement logs against Doppelgänger-related activities.	→ YouTube may have lacked proportionate, targeted mitigations (e.g., EU geofencing, state media labelling, downranking) for the Polish elections; → Evidence gap: 2025 Documented election integrity measures active during the election period and enforcement logs against Radio Belarus-related activities.	→ TikTok's election- and impersonation-related mitigations may have been insufficient or ineffectively deployed, yielding inconsistent enforcement; → Evidence gap: 2025 Documented election integrity measures active during the election period and enforcement logs against political impersonation.

Table 7. Potential DSA violations in Moldovan Incident Alerts[16]

Moldova	IA 0084: Moldova elections targeted by Belarusian YouTube disinformation campaign	IA 0085: Vietnamese bots boost pro-Kremlin channels meddling in Moldovan elections	IA 0091: REST Media-Rybar Link: Coordinated Pro-Kremlin Network Targeting Moldova
Art. 6 Hosting liability	/[17]	/	/
Art. 14 Terms of Service	/	→ Meta may have not properly enforced its election policies (including prohibition of CIB) and its Ad Standards; → Evidence gap: Proof of unmoderated bot activity and fake accounts in posts and ads.	/
Art. 16 Notice and action	/	/	/
Art. 17 Statement of reasons	→ If YouTube was to remove the content and the recipient of the service was in the EU, it should issue a statement of reasons explaining its decision; otherwise, this would constitute a violation; → Evidence gap: YouTube's statement of reasons for the channels on which action was taken, showing all required elements.	→ If Facebook was to remove the content, and the recipient of the service was in the EU, it should issue a statement of reasons explaining its decision; otherwise, this would constitute a violation. The only exception would be if it considered the ads as "deceptive high-volume commercial content"; → Evidence gap: Facebook's statement of reasons for the Page and ads on which action was taken, showing all required elements.	→ If TikTok and X were to remove the content and the recipient of the service was in the EU they should issue a statement of reasons explaining their decision; otherwise, this would constitute a violation; → Evidence gap: TikTok and X's statement of reasons for the accounts or posts and videos on which action was taken, showing all required elements.

[16] As mentioned before, the DSA does not apply to non-EU countries, but given Moldova's EU accession status, Moldovan diaspora presence in the EU, and high level of Russian interference, it provides a relevant case study to anticipate how DSA provisions might function in similar contexts.

[17] None of the incident reports mentions if the content was reported to the platforms, triggering their liability under Article 6 and demanding them to act under Article 16.

Art. 26 Ad transparency	/	→ The ads ran by the Facebook Page may have lacked clear and unambiguous information about the advertiser; → Evidence gap: Proof that the ads contained all required information.[18]	/
Art. 34 Risk assessment	→ YouTube may have insufficiently assessed systemic risks to democratic processes from foreign state media potentially targeting EU recipients (e.g., the Moldovan diaspora); → Evidence gap: Proof of any risk assessment prior to the Moldovan election and regarding EU audience targeting	→ Meta may have failed to adequately assess foreseeable risks from coordinated manipulation and ad abuse targeting the Moldovan election with EU targeting; → Evidence gap: Proof of any risk assessment prior to the Moldovan election and regarding EU audience targeting.	→ TikTok and X may have failed to adequately assess systemic risks to civic discourse and democratic integrity by allowing influence operations to reach EU audiences; → Evidence gap: Proof of any risk assessment prior to the Moldovan election, regarding EU audience targeting, and the Rybar network.
Art. 35 Risk mitigation	→ YouTube may have lacked context- and language-specific election safeguards for Moldova-related content accessible to EU users → Evidence gap: Documented election integrity measures active during the election period and enforcement logs against Belarusian state media	→ Meta may have failed to implement appropriate mitigations; → Evidence gap: Documented election integrity measures active during the election period and enforcement logs against bot networks and political ads.	→ TikTok and X may have failed to implement proportionate mitigation measures against known risks, allowing REST Media content to persist unchecked; → Evidence gaps: Documented election integrity measures active during the election period and enforcement logs against the Rybar network.
Art. 39 Additional ad transparency for VLOPs	/	→ Meta may have failed to archive political ads reaching EU users; → Evidence gap: Repository records in the Ad Library for each flagged ad detailing all required information.[19]	/

[18] This includes archived versions or screenshots of each ad as shown to users, evidencing a clear advertisement label, the natural or legal person on whose behalf the ad is presented, and a "why am I seeing this?" disclosure with meaningful description of the main parameters used to determine delivery to that user (and how to adjust them), tied to the specific ad ID and timestamp.

[19] This consists of the ad content and creative, the identity of the advertiser (and, if different, on whose behalf), the period displayed (start and end time), the main parameters used for targeting and for delivery (including audience criteria), and the total number of recipients reached, broken down by EU Member State.

Table 8. Potential DSA violations in Czech Incident Alerts

Czech Republic	IA 0096: Deceptive Meta ads via "Šokující Česká 24" drive users to fake investment platform	IA 0097: Russian state affiliated outlet NeČT24 promoting election fraud narratives	IA 0101: Coordinated TikTok bot network targeting Czech elections
Art. 6 Hosting liability	→ Meta was notified of the deceptive ads and took down some but left others; → Evidence gap: Proof of reporting the ads.	/[20]	→ TikTok is aware of the bot accounts as they were reported through the RRS → Evidence gap: Proof of reporting the accounts
Art. 14 Terms of Service	→ Meta did not consistently implement its Ad Standards and policy against impersonation; → Evidence gap: Proof that some scam ads were not removed and engaged in impersonation.	→ If the NeČT24 is a cover for Sputnik CZ, a sanctioned media, posting its content would be illegal if the hosting provider has actual knowledge of this illegality; → Evidence gap: Proof that the social media accounts are operated by a sanctioned entity.	→ The accounts violate TikTok's Community Guidelines on "deceptive behavior and fake engagement"; → Evidence gap: Proof that the accounts are bots and engage in automated behaviour.
Art. 16 Notice and action	→ Failure to act on notices in a timely, diligent, non-arbitrary manner and failure to give clear reasons for rejecting notices; → Evidence gap: Submitted notices for each ad with all the required elements.	/	→ If TikTok did not process notices in a timely manner or prioritise the RRS notices received, it might be in breach of its notice-and-action duty; → Evidence gap: RRS submissions with all the required elements.
Art. 17 Statement of reasons	→ Meta did not remove some of the scam ads; → Evidence gap: Meta's statement of reasons for not removing the ads, showing all required elements.	→ If Facebook and X were to remove the content on grounds of illegality, they should issue a statement of reasons explaining their decision; otherwise, this would constitute a violation.	→ If TikTok failed to issue a statement of reasons for each decision and compile it in the DSA Transparency Database, there might be a violation; → Evidence gap: Copies of TikTok's statements of reasons and

[20] Articles. 6 and 16 do not apply as the incident was not reported to the platforms.

		The only exception would be if they considered the ads as "deceptive high-volume commercial content"; → Evidence gap: Facebook and X's statement of reasons, showing all the required elements.	corresponding Transparency Database entries.
Art. 26 Advertising on online platforms	→ The ads ran by the Facebook Page should provide clear, concise and unambiguous information about the advertiser; → Evidence gap: Proof that the ads contained all required information.	/	/
Art. 34 Risk assessment	→ Meta's latest systemic risk assessment likely failed to explicitly identify and quantify the recurring risk for Czech or EU audiences of cloaked, domain-spoofed scam ads using public-figure bait, underestimating exposure and vulnerable cohorts; → Evidence gap: Timestamped risk assessment records before the Czech elections and prior analysis on ads and investment scams.	→ Facebook and X failed to adequately assess systemic risks to Czech electoral integrity from FIMI actors and regarding electoral fraud narratives; → Evidence gap: Timestamped risk assessment records before the Czech elections and prior analysis of Sputnik-related activities.	→ TikTok inadequately assessed risks related to the Czech elections, coordinated inauthentic behaviour, meme distortion, and hashtag swarming; → Evidence gap: Timestamped risk assessment records before the Czech elections and prior analysis on bot networks.
Art. 35 Risk mitigation	→ Risk mitigation appears insufficient as it failed to prevent or promptly suppress the cloaked, spoofed-domain, scam ad cluster across Facebook and Instagram; → Evidence gaps: Documented election integrity measures active during the election period	→ Facebook and X failed to implement proportionate mitigation measures against identified electoral integrity risks; → Evidence gap: Documented election integrity measures active during the	→ Although these risks were known, TikTok did not effectively implement mitigations, enabling the network's continued reach; → Evidence gap: Documented election integrity measures active during the election period

	and enforcement logs against investment ads.	election period and enforcement logs against Sputnik-related activities.	and enforcement logs against bot networks.
Art. 39 Additional ad transparency for VLOPs	→ The ads should be included in the Meta Ad Library; → Evidence gap: Repository records in the Ad Library for each flagged ad detailing all required information.	/	/

III) Potential Terms of Service violations: insights on platform policies

This section examines how the identified FIMI incidents (IAs) may breach platforms' Terms of Service (ToS) and related integrity policies. A relevant premise is that these policies are updated often, and some changes may narrow their practical application, even as the formal framework remains unchanged. A recent example is Meta's revision of its "hateful conduct" (i.e., hate speech) policy to allow allegations of "mental illness or abnormality" directed at LGBTIQ+ people. The result is an excessive focus on defining what content is allowed or prohibited, which fuels unproductive, polarising, and ultimately misleading debates about censorship and free speech rather than addressing the root issue: the persistence of illegal and demonstrably inauthentic behaviour online. Instead, the priority should not be the policing of content categories but the action against illegal content and the prevention of systemic risks that undermine democratic processes.

Misinformation

The presence of mis- and disinformation[21] is not a necessary condition for FIMI. Across the examined incidents, **few cases explicitly involve fabricated information**; rather, most revolve around the dissemination of propaganda and pro-Russian or anti-EU narratives. While such narratives are manipulative, they generally fall outside the scope of existing platform rules, which **narrowly define misinformation in election contexts**. For instance, X's civic integrity policy clarifies that "not all false or untrue information about politics or civic processes constitutes manipulation or interference", explicitly excluding "inaccurate statements about an elected or appointed official, candidate, or political party." Similarly, YouTube's election misinformation policy limits violations to voter suppression, false claims about a candidate's eligibility, or obstruction of voting procedures. As a result, even targeted attacks – such as those against Polish presidential candidate Rafał Trzaskowski (IA 0069) – may not qualify as violations.

Meta's policies and safeguards for elections are broader, encompassing the prohibition of conducting deceptive influence operations, as they engage in Coordinated Authentic Behaviour. Yet even these are inconsistently enforced. For example, content from sanctioned entities such as the Foundation to Battle Injustice (IA 0044), RT Deutsch (IA 0047), or Social Design agency (IA 0058) circulated on Meta platforms, TikTok, X and YouTube – despite each platform's ToS requiring compliance with applicable law. Hosting

[21] In cases where it was present though, it would be more accurate to refer to disinformation, since foreign actors deliberately produce and disseminate false, inaccurate, or misleading content. However, as most platforms use the term misinformation in their policies, this terminology is adopted here for consistency.

(or monetising) such content thus constitutes **a dual breach: a violation of the platforms' own ToS and a failure to act against known illegal content** originated from sanctioned entities. Despite these clear breaches, no systematic enforcement followed.

Deceptive and inauthentic behaviour

The main category of policy violations observed concerns authenticity rather than the veracity of content. Most operations rely on the manipulation of platform dynamics through deceptive identities, synthetic media, and artificial engagement. The impersonation of outlets and individuals, the coordination across channels or bot networks, or the inauthentic amplification of content directly contravene X's authenticity policy and trademark policy, Meta's inauthentic behaviour rules, or TikTok's rules on deceptive behaviour and intellectual property policy. Despite platform knowledge of campaigns such as Overload (IA 0046) or Doppelgänger (IA 0058), which rely on this consistent inauthenticity playbook, or the exposure of networks of bots and fake or automated accounts across various IAs (e.g., IA 0085, 0101), **enforcement remains slow and inconsistent**.

Ad standards

In several cases, the violations extended to advertising standards. Meta's Ad Standards explicitly prohibit fraud, scams, and deceptive practices – rules breached in the Czech operation "Šokující Česká 24" (IA 0096). Ads on social issues, elections, and politics – used by the Vietnamese bot networks interfering in the Moldovan election (IA 0085) – explicitly prohibit foreign interference. In any case, they should be stored in the Ad Library.

Law compliance

While most platforms' rules, terms, or guidelines state that the use of the service is bound to **compliance with all applicable laws** (e.g. Meta, TikTok, X, YouTube,), it is important to keep legal obligations distinct from contractual (i.e., ToS-related) ones. Consequently, knowingly hosting or facilitating content from sanctioned entities can amount to a legal breach and a ToS violation; likewise for conduct engaging national provisions, such as the German defamation law (IA 0044) or the Polish electoral silence law, which applies to online platforms too (IA 0069). In practice, platforms tend to moderate content primarily on the basis of ToS violations rather than legal breaches, which also allows them to avoid assessing or disclosing the actual volume of illegal content on their services. Yet quantifying how much illegal content circulates online is essential to understand the true scope of systemic risks and ensure meaningful compliance with the law.

Election-related policies

This comparative analysis reveals a high threshold for triggering **election misinformation policies, which remain too restrictive in scope and too lax** in enforcement. Content must explicitly entail voter suppression or obstructing voting procedures, excluding the majority of FIMI incidents that rely on misinformation and coordinated inauthentic practices. As a result, **many operations deliberately exploit this grey zone, crafting content that is manipulative yet technically policy-compliant so it can thrive largely undisturbed**. Surprisingly, within the context of an electoral monitoring project, only one of the twelve analysed incidents – the case involving false claims of terrorist threats (IA 0046) – would constitute **a clear violation of the hosting platform's civic integrity policy, as it could be interpreted as a form of voter suppression**. Meanwhile, non-VLOPs like Telegram, Odyssey, Rumble, and VK exclude any civic integrity or misinformation-specific provisions, offering a lax moderation environment that appears to explain their growing appeal among users seeking fewer restrictions.

Tables 9 to 12 below assess in detail potential violations of platform Terms of Service in the various incidents.

Table 9. Assessment of platform policy violations in German Incident Alerts

Germany	IA 0044: Storm-1516 and R-FBI: Russian attempts to interfere in the German election	IA 0046: Overload-coordinated disinformation network uses AI, media impersonation to target German election	IA 0047 Uncovering RT Deutsch's content-laundering ecosystem
Platform	Facebook,Instagram, Telegram, TikTok, X, YouTube	X	Odysee, Rumble, Telegram, VK, X
Presumed violation	→ Meta's policies and safeguards for elections prohibit Coordinated Inauthentic Behaviour (under "stopping influence operations") and fake accounts (under "fighting abuse"); → Meta prohibits defamation; → Meta's ToS demand compliance with applicable law, so posting content from a sanctioned entity would constitute a violation. → TikTok's integrity and authenticity policy prohibits deceptive behaviours and unlabeled AI content; → TikTok's ToS prohibit illegal content and violations of applicable law, which would include content from sanctioned entities. →X's Authenticity policy prohibits synthetic and manipulated media; → X's ToS require compliance with applicable law, which would be violated by posting content from sanctioned entities.	→ X's authenticity policy prohibits coordinated, inauthentic amplification and artificial boosting; → X's trademark policy prohibits intellectual property rights violations; → X's civic integrity policy prohibits voter suppression (e.g., spreading fabricated terrorist threats) and bans "false or misleading affiliation" (e.g., impersonation).	→ Odysee's ToS ban content violating national and international law. → X's ToS require compliance with applicable law, which would be violated by posting content from sanctioned entities.

	→ YouTube's ToS require compliance with applicable law, which would be violated by posting content from sanctioned entities; → YouTube also prohibits defamation.		
Other comments	→ The incident does not describe explicit violations of X's civic integrity policy or YouTube's election misinformation policies. → Meta and YouTube encourage labelling synthetic content. → Telegram's ToS bans "activities that are recognised as illegal in the majority of countries".	→ This is potentially the only case in which civic integrity policies are violated, as the dissemination of fabricated terrorist threats could constitute voter suppression. → A peculiar detail is that the content circulated in multiple languages but not in German, which could be a strategy to circumvent content moderation.	→ Telegram's ToS bans "activities that are recognised as illegal in the majority of countries". → Rumble's Terms & Conditions require user compliance with applicable laws. → VK's ToS mentions law compliance exclusively in terms of user liability.

Table 10. Assessment of platform policy violations in Polish Incident Alerts

Poland	IA 0058:Illegal influence operation Doppelgänger continues: targeting the Polish elections	IA 0069: Sanctioned Belarusian media channel violating electoral silence law: discrediting presidential candidate Rafał Trzaskowski	IA 0070: Murky accounts on TikTok impersonating Polish presidential candidates and political parties
Platform	X	YouTube	TikTok
Presumed violation	→ X's authenticity policy prohibits "inauthentic accounts, behaviours or content", including unauthorised automation, fake personas, and impersonation; → X's ToS require compliance with applicable law, which would be violated by posting content from sanctioned entities.	→ YouTube's ToS require compliance with applicable law, which would be violated by posting content from sanctioned entities; → YouTube also prohibits defamation.	→ TikTok's content violations and bans page prohibit impersonation; → TikTok's intellectual property policy prohibits trademark and copyright infringements.
Other comments	→ The IA does not describe explicit violations of X's civic integrity policy.	→ The IA does not report actions that explicitly violate YouTube's elections misinformation policies.	→ The IA is not described with enough detail to confirm a violation of TikTok's civic and election integrity policy.

Table 11. Assessment of platform policy violations in Moldovan Incident Alerts

Moldova	IA 0084: Moldova elections targeted by Belarusian YouTube disinformation campaign	IA 0085: Vietnamese bots boost pro-Kremlin channels meddling in Moldovan elections	IA 0091: REST Media-Rybar Link: Coordinated Pro-Kremlin Network Targeting Moldova
Platform	YouTube	Facebook and Instagram	TikTok, X, and Telegram
Presumed violation	→ YouTube's information panels policy providing publisher context for government-funded news channels may apply.	→ Meta's policies and safeguards for elections prohibit Coordinated Inauthentic Behaviour (under "stopping influence operations") and fake accounts (under "fighting abuse"); → Meta's Ad Standards on ads about social issues, elections and politics prohibit foreign interference.	→ TikTok's state-affiliated media policy (including labels) may apply. → X's policy on labelling state-affiliated media entities may apply.
Other comments	→ The incident may be borderline but not in explicit violation of YouTube's elections misinformation policies.	/	→ The incident is not described with enough detail to ascertain if this would be a violation of TikTok's Community Guidelines (i.e., civic and election integrity) or X's civic integrity policy. → There is no identifiable violation of Telegram policy.

Table 12. Assessment of platform policy violations in Czech Incident Alerts

Czech Republic	IA 0096: Deceptive Meta ads via "Šokující Česká 24" drive users to fake investment platform	IA 0097: Russian state affiliated outlet NeČT24 promoting election fraud narratives	IA 0101: Coordinated TikTok bot network targeting Czech elections
Platform	Facebook and Instagram	Facebook, X, Telegram	TikTok
Presumed violation	→ Meta's Ad Standards prohibit fraud, scams and deceptive practices; → Meta's Community Standards prohibit fake accounts (engaging in impersonation).	→ Meta's ToS demand compliance with applicable law, so posting content from a sanctioned entity would constitute a violation. →X's ToS require compliance with applicable law, which would be violated by hosting content from sanctioned entities.	→ TikTok's Community Guidelines prohibit deceptive behaviour and fake engagement.
Other comments	/	→ The actions described in the IA (i.e., implying that the Czech government and Constitutional Court wished to manipulate election results) are not explicitly prohibited by Meta's misinformation policy. Meta's policies and safeguards for elections do not apply either as the incident does not include CIB. → The incident does not describe explicit violations of X's civic integrity policy. → There are no identifiable violation of Telegram policy.	→ The IA does not report explicit violations of TikTok's civic and election integrity policy.

Best practices: lessons for future monitoring

The overarching aim of this analysis has been to reflect on systemic infringements arising from FIMI campaigns during four European elections. This section identifies best practices for future monitoring projects, drawing lessons from the challenges and gaps identified throughout this report. Ultimately, the goal is not only to map or describe FIMI incidents, but to deter and prevent them through better-informed, evidence-based responses.

From exposure to deterrence

FIMI monitoring should be seen as part of a broader accountability process: it begins with raising situational awareness through exposure and can lead to the deterrence of malign actors via accountability and policy enforcement. Civil society plays a key role in this process. Under the DSA, it can act as a bridge between detection and enforcement – pressing platforms and regulators to uphold their legal obligation. To do so effectively, researchers, analysts, and experts need a **clear understanding of the available accountability channels, including reporting mechanisms, transparency tools, and formal complaint procedures** established under this important regulation.

The central role of reporting and follow-up

Reporting remains the first and most essential step in activating legal accountability. It lifts hosting liability exemptions and triggers the corresponding platform responsibilities. Yet, many IAs revealed that no reporting action was taken, perhaps due to the overwhelming volume of content or discouragement following repeated inaction by platforms. While these challenges are understandable, consistent reporting is indispensable. Equally important is **systematic follow-up** – documenting if platforms act (or fail to act) upon reports and maintaining records of their responses. **Such data are vital to identify patterns of neglect and demonstrate systemic non-enforcement under the DSA**. While reporting mechanisms under the DSA are open to all users, researchers occupy a particularly important position in documenting non-compliant responses. Whether or not formally recognised as vetted researchers, they could play a crucial role in improving reporting outcomes. In retrospect, the research community may have missed an opportunity to engage more actively with these mechanisms and demonstrate their potential impact.

Shifting focus from content to behaviour

Future monitoring efforts must **prioritise behavioural analysis over content-based assessments**, as FIMI operations often rely on tactics that are not overtly illegal, exploiting the grey zone between "awful but lawful" and explicitly unlawful activity. The dismantling or weakening of platform integrity policies only deepens this vulnerability, allowing **manipulative networks to operate below the threshold of formal violations**. Analysts should therefore focus on **documenting core behavioural indicators** – including coordination patterns, automation, and amplification mechanisms – and invest in improving attribution to reveal the campaign's origin. This shift is crucial because platforms tend to act more decisively when presented with misuse of their services through inauthenticity rather than when confronted solely with propagandistic or misleading content. However, when disinformation constitutes the only ground for a reported violation, the claim should be substantiated with independent expertise – such as verified fact-checks from trusted organisations – to reinforce its evidentiary basis.

Defining scope and relevance

In some cases (IA 0070, 0096), **uncertainty persists as to whether an operation is foreign-led (FIMI) or domestically-driven (DIMI)**. While the overlap is natural, clear prioritisation criteria are essential to ensure analytical focus. The EU DisinfoLab triage template is particularly useful here, helping analysts distinguish between isolated incidents and components of a coordinated campaign, and to classify operations based on attribution confidence of foreign origin. Furthermore, selecting incidents that have reached a measurable level of virality or societal impact helps avoid inadvertently amplifying minor or fringe activities, which can serve malign actors' goals.

The importance of disaggregated and evidentiary data

This report was necessarily based on secondary data, relying on partner contributions within the project. However, these **Incident Alerts lacked verifiable source material** such as specific URLs, which limited the ability to substantiate specific claims or trace the original dissemination pathways. In many instances, disaggregated data by platform were unavailable: while the case and platforms were described in general terms, the specific role of each platform was not detailed, hindering the analysis of platform-specific violations. Future monitoring must go further by **systematically collecting disaggregated and verifiable proof** to substantiate claims. **Hard evidence is crucial to transform qualitative assessments into actionable cases.** In this context, Article 40 of the DSA

offers an important opportunity: vetted researchers can request access to platform data, a mechanism that should be strategically leveraged to secure supporting documentation – including network linkages, engagement metrics, or moderation decisions – to strengthen the evidentiary basis of future analyses. The collection of such evidence enables civil society to demand concrete enforcement actions that platforms are already obliged to implement, including labelling state-affiliated media, adjusting recommendation and search systemic to reduce the amplification of problematic content, or enforcing stricter transparency obligations for political and issue-based advertising.

Strengthening election integrity frameworks

Finally, the current platforms' election policies remain excessively narrow and lack meaningful enforcement. Their limited scope – often restricted issues such as voter suppression – fails to address the full range of manipulative tactics observed in FIMI operations. Moreover, **platforms still treat much of this activity as mere violations of Terms of Service rather than as potential breaches of law, for which a robust flagging system that prioritises the identification and removal of illegal content is needed**. Researchers and civil society must advocate for more robust, detailed, and enforceable election integrity policies, underpinned by transparent enforcement mechanisms and grounded in legal accountability. Without such measures, the online information ecosystem will remain structurally vulnerable to manipulation, enabling malign actors to exploit regulatory gaps and distort democratic discourse.

FIMI -ISAC

FDEI PROJECT

Report

REGULATORY CHALLENGES & GAPS IN ADDRESSING SYSTEMIC PLATFORM ABUSE