VISEGRAD / INSIGHT

Disinformation | Visegrad Group | Polish Case Study

Problem

Disinformation in Poland has become a profitable industry, fuelled by digital models and weak oversight. Media and NGOs exploit public fears, creating an ecosystem where disinformation thrives and generates revenue, complicating regulation.

Key facts

TV Republika, Fundacja Nautilus, and Telegram channels profit from ads, pseudo-science and crypto donations.

UOKiK targets misleading ads; GDPR violations persist, especially in data collection.

Fundacja Nautilus misuses nonprofit status for financial gain while spreading disinformation.

Foresight

The growth of disinformation networks in Poland threatens public trust and the digital economy's regulation. Using AI and cryptocurrencies, these actors evade oversight, exploit new revenue streams and target niche audiences. Stronger content labelling, penalties and data audits are needed, along with financial transparency for NGOs and crowdfunding, to close loopholes enabling harmful activities.

Disinformation in Poland: Profiting from Loopholes and Regulatory Gaps

EXECUTIVE SUMMARY

Disinformation in Poland has transformed ideology into a profitable industry. Exploiting regulatory gaps and digital platforms, actors thrive on sensationalism around health, immigration and EU policies, raising concerns about Poland's digital future.

The following policy brief will show why it is necessary to:

- **Strengthen Regulatory Oversight**: The Polish government should tighten regulations by imposing stricter penalties for misleading ads, increasing media transparency and enforcing General Data Protection Regulation (GDPR) compliance on digital platforms.
- **Increase Financial Transparency**: Non-governmental organisations (NGOs) and decentralised platforms that profit from disinformation should face more rigorous financial audits. This will prevent the misuse of crowdfunding platforms and cryptocurrency transactions to fund disinformation.
- **Label Disinformation Sources**: A national strategy to label disinformation sources is crucial to help citizens spot unreliable content and curb false narratives.
- **Leverage AI and Data Analytics**: Utilise AI-driven content moderation tools and data analytics to track the spread of disinformation across platforms, enabling a faster response to false narratives and identifying threats.
- **Engage in cross-sector partnerships** among government, tech and civil society to understand economic drivers

About

Project

Visegrad Insight is the main Central European analysis and media platform. It generates future policy directions for Europe and transatlantic partners. Established in 2012 by the Res Publica Foundation.

The project was implemented in partnership with the Prague Security Studies Institute and supported by the Czech-Polish Forum program of the Ministry of Foreign Affairs of the Czech Republic.

Authors

Miles R. Maftean

INTRODUCTION

Disinformation is no longer just a tool for political manipulation – it has evolved into a highly profitable industry deeply embedded in the digital economy. In 2023, the global digital advertising market reached a staggering €625 billion, driven by a business model that rewards engagement above all else. This model turns incendiary and misleading content into lucrative assets, as each click, share, and comment translates into advertising revenue. Social media platforms, designed to maximise user engagement, exploit this system by promoting content that stokes fear, anger, and division – laying fertile ground for disinformation to thrive.

In Central and Eastern Europe (CEE), and particularly in Poland, disinformation networks have capitalised on this model, turning false narratives into revenue streams that feed off of public anxieties. In Poland, disinformation is not merely an ideological battleground; it's a commercial enterprise where actors exploit societal divisions for financial gain. From anti-immigrant rhetoric to COVID-19 conspiracies, disinformation is designed to capture attention and drive engagement, regardless of the truth.

This report, the second in our series, examines the evolving landscape of disinformation in Poland, focusing on how these networks profit from regulatory loopholes and weak enforcement. It analyses the financial underpinnings of disinformation, reveals connections between media, NGOs and political entities, and outlines the legal and ethical breaches that enable these operations to flourish. By examining the profit motives behind disinformation, this report aims to shift the conversation from ideological debates to the economic drivers that sustain these harmful networks.

EVOLVING LANDSCAPE OF DISINFORMATION ACTORS

Classification of Previous Actors

Our initial report identified several key disinformation actors in Poland, which can be categorised based on their business models, motivations and primary methods of operation:

Contributors

Editors: Galan Dall, Jessica Moss and Kristína Šefčíková.

Team: Katarzyna Górska, Magda Jakubowska, Staś Kaleta, Jacek Karaczun, Tomasz Kasprowicz, Anna Kuczyńska, Natalia Kurpiewska, Albin Sybera, Magda Przemojska, Wojciech Przybylski and Luca Soltesz.

- **Media-Driven Actors**: Platforms like **TV Republika** operate as commercial enterprises, blending traditional broadcasting with digital disinformation, and are driven primarily by financial motivations. They monetise their content through diversified income streams, including advertising, e-commerce and paid content, allowing them to sustain their operations and expand their influence.
- **NGO-Linked Entities**: Disinformation actors like **Fundacja Nautilus** use their status as educational or cultural NGOs to promote pseudo-scientific and conspiratorial content. These organisations often rely on voluntary contributions and public donations, exploiting their nonprofit status to shield their financial activities from scrutiny. Their primary motivation is ideological, often cloaked under the guise of public service.
- **Decentralised Platforms**: Telegram channels such as 'Wiadomosci Czasow Ostatecznych,' loosely translated to 'End Times News,' are categorised as 'Preachers' or 'Healers,' focusing on socio-political or health-related disinformation. These platforms exploit the anonymity and lack of regulation on Telegram to spread unverified claims, particularly around sensitive issues like EU policies and COVID-19. Independent internet portals, such as **Racjonalista**, blend rationalist messaging with monetised esoteric content, driven by financial benefits and resulting in niche ideological communities.

Shifts in Tactics and Strategies

Previously identified actors, such as TV Republika, Fundacja Nautilus and various Telegram channels, have refined their tactics to maximise impact and evade regulatory scrutiny. These actors initially disseminated their content via traditional and digital media. However, with growing regulatory pressures and public awareness, they have shifted towards more covert and decentralised methods:

- **Enhanced Digital Integration:** Platforms like TV Republika have expanded their digital presence, increasingly leveraging social media algorithms to amplify their reach. By integrating content across multiple platforms – broadcast, web publishing and social media –

they create a feedback loop that maximises audience engagement and monetises disinformation through diverse channels.

- **AI and Deep Fake Technology:** Disinformation actors are now incorporating AI-generated content and deepfake technology to create more persuasive and emotionally charged narratives. These technologies allow them to fabricate events, impersonate credible figures and manipulate public perception on a larger scale than before, making it more challenging for fact-checkers and regulators to keep up.
- **Exploitation of Niche Communities:** Racjonalista and similar platforms have honed their strategies to appeal to niche audiences with specific interests, such as alternative medicine or conspiracy theories. By targeting these groups with tailored content, they build highly engaged communities that are more likely to donate, purchase products or further disseminate disinformation.

Shifts in Revenue Sources

Disinformation actors in Poland have diversified their revenue streams, moving beyond traditional advertising and donations to exploit newer, less transparent financial channels:

- **Cryptocurrency and Anonymous Funding:** Telegram channels, particularly 'Wiadomosci Czasow Ostatecznych,' have increasingly turned to cryptocurrencies for funding, allowing them to receive donations that are difficult to trace. This shift secures a steady income and shields these actors from financial oversight and accountability.
- **Commercial Partnerships and Affiliate Marketing:** Actors like TV Republika and Alphanet have cultivated partnerships with commercial entities, including advertising networks and affiliate marketing schemes. These partnerships often operate in a grey zone, where brands may unknowingly fund disinformation by purchasing ad space or engaging in affiliate relationships with these platforms.
- **Monetised Pseudo-Science and Esoteric Content:** Platforms such as Fundacja Nautilus position themselves as educational or cultural entities to attract donations. They also sell products related to their niche

topics, such as books, webinars, and exclusive content, creating a self-sustaining financial model.

- **Compliance with Taxation Regulations for Digital Platforms:** Disinformation actors monetising content on platforms like YouTube may be required to adhere to specific taxation regimes, particularly for income earned from abroad. However, the opaque nature of online revenue and lack of stringent enforcement allows them to potentially evade tax obligations. Enhanced regulatory scrutiny in this area could serve as a deterrent, ensuring these actors comply with tax laws and reducing their ability to profit from disinformation.

BREACHES OF NATIONAL LAW

Advertising Violations

Although the available reports for the aforementioned disinformation actors do not cite documented cases of failure to label sponsored content, the Polish Office of Competition and Consumer Protection (UOKiK) is stepping up its efforts to combat misleading advertising practices across various media platforms. Recently, UOKiK has targeted influencers for failing to adequately disclose sponsored content, a widespread issue that highlights broader advertising irregularities within Poland's media landscape. The agency has imposed fines on several influencers and has been investigating influencers and their advertisers to develop stricter guidelines on labelling commercial relationships. In total, the fines come out to 139,000 Polish zloty (€32,000).

However, while UOKiK has intensified its focus on misleading advertising practices, there have been no reports of measures against disinformation outlets, such as those identified in this report. If these media outlets have failed to label ads or disclose paid partnerships properly, as suspected, they should face similar, targeted regulatory actions. UOKiK's intensified approach should be extended to include disinformation sources, ensuring that these actors are held to the same standards as other media.

Data Protection Violations

There are growing concerns that disinformation websites in Poland may violate the General Data Protection Regulation (GDPR), though cases of non-compliance are not always publicised. These sites often lack clear mechanisms for obtaining explicit consent from users, providing adequate privacy notices or offering users the right to opt-out – core requirements

under GDPR. This raises the possibility that personal data is being improperly collected and used to target and amplify disinformation. Authorities should closely monitor the compliance of such websites with GDPR standards.

The Polish Data Protection Authority (UODO) has primarily focused on broader GDPR compliance issues across digital platforms, but more targeted scrutiny is needed for disinformation websites specifically. By flouting GDPR requirements, disinformation websites not only breach EU data protection laws but also reinforce their ability to manipulate public opinion through targeted misinformation campaigns.

Exploitation of NGO Status by Disinformation Actors

Polish NGOs are legally required to adhere to financial transparency laws, which include submitting financial reports to the Polish National Court Register (KRS). NGOs, particularly those with Public Benefit Organisation (PBO) status, must prepare annual financial statements, which typically include a balance sheet, a profit and loss statement, and notes detailing their financial activities. These requirements are part of the broader effort to maintain transparency and accountability in the nonprofit sector. However, these reports are not always easily accessible to the public.

Making these financial reports publicly accessible would increase the scrutiny of NGOs, making it more difficult to obscure their funding sources or misuse public donations for purposes that may include disinformation campaigns or personal interests.

The rising popularity of crowdfunding further complicates the financial landscape for NGOs, particularly in Poland, where regulatory enforcement remains inconsistent. Although the European Crowdfunding Service Providers Regulation (ECSP), which came into force in 2021, introduced stricter guidelines regarding transparency and investor protection, enforcement has struggled to keep pace. Several crowdfunding campaigns related to social and political causes have lacked clear financial reporting or traceability of funds. These gaps in oversight create opportunities for misuse, as funds raised through crowdfunding platforms can be difficult to trace, making it challenging to verify their intended purpose or track their origins. Without consistent enforcement, NGOs and other entities can exploit this regulatory grey area to redirect or misuse funds.

These financial reporting challenges and the unregulated nature of crowdfunding provide fertile ground for disinformation actors. Without rigorous checks, funds raised under the guise of charitable purposes can be diverted into disinformation activities. As Poland works to implement more stringent financing regulations, making financial reports publicly accessible and improving oversight mechanisms could prevent the misuse of funds and strengthen accountability in the nonprofit sector.

CASE STUDIES: CONNECTIONS TO BUSINESS, NGOS AND POLITICS

Business Sector Involvement

Poland's disinformation landscape demonstrates how business models prioritising profit and engagement intersect with the propagation of false information. Companies such as Alphanet, the parent company of TV Republika, illustrate the entanglement of business interests and disinformation. Alphanet operates an extensive network of websites that covers diverse topics ranging from politics to health, creating a hybrid ecosystem that integrates legitimate and disinformation content. This broad media presence allows Alphanet to monetise disinformation effectively through advertising revenue, affiliate marketing and commercial partnerships, often without transparent disclosure of these relationships.

A closer examination of the individuals operating these platforms reveals a broader web of interconnected business ventures. For instance, Erich Syrovatka, linked to Alphanet, has established businesses like 'INTERNET SK, s.r.o.' in Slovakia and 'INTERNET CZ, a.s.' in Czechia. His involvement spans multiple defunct and active companies across Central Europe, suggesting a pattern of leveraging diverse media channels for various financial purposes. Another individual, Roman Rajmund Lissok, is also associated with Alphanet, further highlighting the networked nature of these operations. While there is no direct evidence tying these individuals to disinformation, their extensive media and digital footprint suggest a capacity for broad content dissemination that could include disinformation.

The business models behind these platforms vary but often focus on high-engagement content that attracts advertisers. TV

Republika, for example, uses automated advertisements, generating substantial monthly revenue while integrating sensationalist and controversial content to maximise audience engagement. This strategy ensures a steady flow of advertising income, potentially without advertisers realising their ads are funding disinformation.

Platforms like Racjonalista operate under the ownership of LH.pl Sp. z o.o., managed by Marek Robert Panek, whose business interests range from solar energy to digital services, and who also owns companies registered in Cyprus. This demonstrates how platforms can leverage their network connections and business interests to sustain their operations and expand their reach.

NGOs and Financial Misconduct

Nonprofit entities with supposedly cultural or educational missions, like Fundacja Nautilus, benefit from reduced scrutiny compared to commercial enterprises. Investigations by Polish transparency watchdogs have highlighted financial irregularities, suggesting that funds meant for public benefit may support disinformation activities. This misuse of nonprofit status not only undermines public confidence but also allows these organisations to evade regulations.

Similarly, Fundacja Otwarty Dialog (Open Dialogue Foundation) has faced serious allegations of financial misconduct, including accepting funds from sources linked to Russia and Kazakhstan. Reports indicate involvement in dubious property dealings and lobbying efforts that contradict their stated mission, raising concerns about the transparency and integrity of their operations. Meanwhile, the Ordo Iuris Institute for Legal Culture, a Warsaw-based ultra-conservative foundation, has not been directly accused of financial misconduct, but its opaque funding sources and links to international conservative networks have sparked criticism. Despite the foundation's calls for transparency in NGO funding, its own practices remain unclear.

In other Central European countries, such as the Czech Republic, evidence suggests that disinformation actors engage in debt avoidance tactics while continuing to raise funds using accounts registered under different names, such as those of company leaders' family members or associates. This allows them to circumvent debt recovery processes while maintaining

financial flows to support their activities. It remains crucial to explore whether similar tactics are employed in Poland, and to what extent they enable disinformation networks to evade financial accountability.

These cases illustrate how some Polish NGOs exploit their nonprofit status to shield disinformation activities from legal accountability, complicating regulatory oversight and further blurring the line between legitimate and harmful operations.

Political Ties

The intersection of politics and disinformation is starkly evident in the activities of groups like Konfederacja Korony Polskiej, which leverage disinformation networks to manipulate public discourse and influence elections. Investigations have revealed that these political actors utilise disinformation as a strategic tool, funding it through opaque channels that bypass traditional campaign finance regulations.

The funding practices of disinformation actors that transition into political roles or seek to influence political campaigns should be scrutinised. In Poland, political candidates and parties must set up transparent accounts for campaign funding and comply with regulations governing donations and expenditures. However, there are concerns that these networks may evade regulations by accepting unregulated donations or via indirect political advertising — advertising ideas which align with a candidate or platform, for instance, but which are not formally linked. By aligning with these disinformation networks, politicians or parties can benefit from narratives that resonate with their political agendas, such as anti-immigrant sentiment or Euroscepticism, while evading the scrutiny typically applied to political financing.

RECOMMENDATIONS

To effectively counter the growing influence of disinformation in Poland and the CEE region, the following actions are recommended:

- **Develop a Unified Labelling Standard for Sponsored Content Across All Media Platforms:** EU and national bodies should establish a standardised system for labelling sponsored content across online platforms, social media and traditional media. This would close regulatory gaps that disinformation actors exploit. Currently, Poland's media regulations, such as the

Broadcasting Act of 1992 and the Act on Competition and Consumer Protection of 2007, focus on traditional media and lack explicit regulation of online platforms. To ensure transparency and accountability, media legislation should be updated to include online media, holding all platforms equally accountable for content disclosure.

- **Increase Penalties for Advertising Non-Compliance and Expand Enforcement Capacity:** Given the recent fines imposed on influencers in Poland, penalties for advertising violations should be increased to serve as a stronger deterrent. Additionally, greater resources should be allocated toward enforcement, increasing the frequency of audits and investigations into advertising practices across digital and traditional media platforms.
- **Implement Targeted Audits of Data Practices on Decentralised Platforms Like Telegram:** The Polish Data Protection Authority (UODO) should coordinate with EU data protection bodies to develop a framework for auditing data practices on decentralised platforms like Telegram. This could involve deploying AI-driven tools to monitor data flows and detect non-compliance in real time. Collaboration with cybersecurity experts and civil society organisations could provide the necessary technological support and grassroots insights to ensure comprehensive audits.
- **Establish a Task Force for Cross-Platform Advertising and Data Compliance Monitoring:** Create a specialised task force involving UOKiK, UODO, other regulatory bodies and key NGOs to monitor compliance with advertising and data protection laws across platforms. Key NGOs can play a crucial role in this task force by monitoring, flagging potential violations and providing grassroots insights. The task force should leverage advanced analytics and AI-driven tools to identify violations in real time, enabling quicker responses and corrective actions. This collaborative approach would enhance oversight, combining regulatory authority with the agility and reach of civil society organisations.
- **Create a 'Disinformation Accountability Index' for Businesses and NGOs:** A joint venture between civil society actors and state authorities should be initiated to develop an index to publicly rate businesses and NGOs involved in disinformation based on their compliance with advertising and data protection standards. This index

would specifically target entities that have been identified as spreading, funding or hosting false information. It would serve both as a consumer guide, warning the public about these actors, and as a regulatory tool, encouraging organisations to maintain transparency and ethical practices to avoid reputational damage. By highlighting non-compliant organisations, the index would deter disinformation activities and promote accountability.

- **Expand UOKiK's Scope to Include Disinformation Sources:** To enhance the effectiveness of the current regulatory efforts, UOKiK should expand its scrutiny to explicitly include disinformation websites and media outlets that may not be properly labelling advertisements or paid partnerships. Examples of potential violations should be shared with UOKiK to encourage focused investigations and enforcement actions against these sources. By doing so, UOKiK can further strengthen its stance against deceptive practices and help reduce the spread of disinformation in Poland.
- **Enhanced Scrutiny for GDPR Compliance:** Regulatory authorities should prioritise investigating disinformation websites for potential GDPR violations. This should involve audits of data collection practices, ensuring transparency about data usage and imposing penalties for non-compliance. Enhancing oversight in this area will deter websites from exploiting personal data and reduce their capacity to manipulate public discourse through targeted disinformation.

Galczynskiego 5, 00-032 Warszawa, Poland
contact@visegradinsight.eu
www.visegradinsight.eu