edam
Centre for Economics
and Foreign Policy Studies

CYBER GOVERNANCE & DIGITAL DEMOCRACY PROGRAMME

SEPTEMBER 2023

COMBATING DISINFORMATION: THE POLICY FRAMEWORK

Ekin Balkan, Analyst, EDAM
Akın Ünver, Associate Professor, Ozyegin University

INTRODUCTION

Disinformation is not a new challenge for societies. Today, however, combating disinformation has become crucial as a result of structural changes in the information ecosystem. In particular, with the rise of digital news media and the proliferation of social media, the speed at which information spreads and its impact on the masses are important dynamics that increase the impact of disinformation, however it should be noted that the changes brought about by digital news media and social media platforms are not limited to these. Due to fewer constraints on content than traditional media, the removal of the requirement for content producers to be professionals, the anonymity of these content creators, social media and the digital landscape already dramatically facilitate the production and dissemination of disinformation. Moreover, the fact that consumers also play an important role in disseminating information on social platforms and in determining what other consumers see further increases both the social and political impact of disinformation. As a direct consequence, the abundance of online content, as many studies have shown, has a negative impact on consumers' attention span and cognitive abilities and thus risks making people more vulnerable to disinformation.

Another critical dynamic that makes disinformation a chronic and serious threat is the attention economy (which monetizes disinformation by making it a useful tool to attract consumers' attention) and the place of social platforms in this economy. Disinformation content characteristically contains emotional language, often appeals to negative emotions and is scandalous in nature, thus increasing the likelihood that the content will attract more attention and will spread faster. The fact that false news spreads 6 times faster than true news on social media, and especially false political news spreads much faster and to more people than other types of false news, further emphasizes the potential impact of disinformation on social platforms and highlights the necessity of combating disinformation. In addition, the fact that these platforms aim to increase user interaction and attract their attention for the purpose of profit carries the risk that content that aims to agitate people and contains disinformation is boosted through the algorithms of the platforms and becomes more prominent. Therefore, the regulation of social platforms and the transparency of the algorithms they use, and the content moderation rules and methods they adopt become particularly important and critical issues that need to be addressed.

[1] Androniki Christopoulou, "Bilgi Bozukluğu Ekosistemi: Sosyal Medyanın Rolü, Dezenformasyonla Mücadele Girişimleri ve Yanlış Bilgi Taksonomilerinin Sistematik Literatür Taraması Üzerine Bir Çalışma," 18 Nisan 2019, https://repository.ihu.edu.gr//xmlui/handle/11544/29381. 18.

[2] Stephan Lewandowsky ve diğerleri, "Teknoloji ve Demokrasi: Understanding the Influence of Online Technologies on Political Behaviour and Decision-Making," JRC Publications Repository, 26 Ekim 2020, https://doi.org/10.2760/709177. 27.

[3] Camille D. Ryan ve diğerleri, "Monetizing Disinformation in the Attention Economy: The Case of Genetically Modified Organisms (GMOs)," European Management Journal 38, no. 1 (1 Şubat 2020): 7-18, https://doi.org/10.1016/j.emj.2019.11.002. 9.

[4] Stephan Lewandowsky ve diğerleri, "Teknoloji ve Demokrasi: Understanding the Influence of Online Technologies on Political Behaviour and Decision-Making," JRC Publications Repository, 26 Ekim 2020, https://doi.org/10.2760/709177. 62-63.

[5] Soroush Vosoughi, Deb Roy ve Sinan Aral, "The Spread of True and False News Online," Science 359, no. 6380 (9 Mart 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

The Case for Public Intervention

Regarding these challenges and problems mentioned above, there is a growing belief and expectation that public intervention, (in addition to self-regulation of social platforms), is necessary to address the challenges and problems mentioned above. Public intervention is seen as an effective and necessary answer to large, structural problems and especially to the interference of foreign actors in democratic processes. It is also seen as a necessary measure to ensure transparency and to prevent arbitrary self-regulation of social media platforms. Therefore, if properly designed, public intervention can be an appropriate tool for empowering and enabling civil society to play an active role in this field while paving the way for transparent and effective regulation, and thus for adopting a multi-stakeholder approach to combating disinformation that involves different actors from society.

The Risks and Challenges of Public Intervention

Whilst public intervention has the potential to be an answer to the challenges mentioned above, all these advantages bring their own risks. One of the most fundamental problems is the censorship that may arise from the way disinformation is defined in regulations and the impact on freedom of expression. Disinformation already carries the risk of being subjective and arbitrary due to the need to define "intent to harm". For this reason, while the conceptual definition of disinformation in regulations is a challenge on its own, the rather vague definition and securitization of disinformation, which is especially seen in authoritarian states, and can also be observed in liberal democracies, carries the risk of paving the way for censorship policies and especially social and political repression.

The challenges posed by disinformation and the regulation of disinformation take on new dimensions with the development and evolution of advanced technologies. Advanced technologies not only affect the ways and methods of producing and disseminating disinformation and information manipulation, but also require new measures in the fight against disinformation in order to adapt to the innovations brought about by these technologies.

[6] Brittany Doyle, "Self-Regulation Is No Regulation--The Case for Government Oversight of Social Media Platforms," Indiana International & Comparative Law Review 32, no. 1 (11 Nisan 2022): 97-130.

[7] Ben Epstein, "Çevrimiçi Dezenformasyonu Düzenlemek Neden Bu Kadar Zor," The Disinformation Age ed. W. Lance Bennett ve Steven Livingston, 1. baskı (Cambridge University Press, 2020), 190-210, https://doi.org/10.1017/9781108914628.008.

[8] justitia, "The Digital Berlin Wall - How Germany (Accidentally) Created a Prototype for Global Online Censorship - Act Two," The Future of Free Speech, 1 Ekim 2020, https://futurefreespeech.com/the-digital-berlin-wall-how-germany-accidentally-created-a-prototype-for-global-online-censorship-act-two/.

The Technology Dimension

The current trajectory of global digital evolution is predominantly influenced by the merger of intricate computational frameworks with vast information networks. This confluence not only paves the way for enhanced information dissemination but also presents multifarious challenges associated with data integrity, veracity, and geopolitical implications.

a. The Advent and Proliferation of Deepfakes

The fusion of deep learning and Generative Adversarial Networks (GANs) has brought forth the era of 'deepfakes'. These sophisticated visual and audio simulations, distinguishable only through advanced forensic tools, threaten the underpinnings of digital trust. The political terrain of Malaysia in 2021 experienced the disruptive power of deepfakes firsthand. An opposition figure, previously insulated from major controversies, was suddenly embroiled in a scandal rooted in a seemingly authentic video. Subsequent forensic analysis revealed its deepfake origin, but the damage was palpable, causing ripples in the national trust framework. This incident is not isolated. Similar instances have emerged globally, signifying the critical need for developing advanced countermeasures.

b. Algorithm-Driven Bots and Information Dynamics

Advanced algorithms, particularly those rooted in machine learning, are increasingly being harnessed to shape public sentiment. These entities, designed for high-frequency content generation and dissemination, are becoming instrumental in various sectors, including electoral processes. During Brazil's recent local elections, sophisticated AI-driven bots played a critical role. Through large-scale data analysis, these bots generated content tailored to specific demographic profiles, significantly influencing voter sentiment. The blurred lines between organic discourse and algorithmic narratives underscore the challenges that digital democracies face today.

c. Open Source Intelligence (OSINT) and Blockchain Integration

OSINT methodologies, while democratizing information access, grapple with challenges related to data authenticity. Blockchain's Distributed Ledger Technology (DLT) can offer transformative solutions in this domain. Platforms such as Africa Uncensored, which focuses on investigative journalism across the continent, can significantly benefit from DLT integration. By anchoring data sources and evidentiary trails on blockchain, these platforms can ensure the immutability and authenticity of their findings, thereby enhancing credibility.

d. Neural Networks, Natural Language Processing, and Fact Verification

With the digital realm flooded with vast amounts of information, real-time fact verification emerges as a paramount necessity. Tools harnessing the power of neural networks and natural language processing are establishing new paradigms in this space. Both Factmata, operating within the European digital ecosystem, and Logically, rooted in the Indian subcontinent, exemplify the advanced strides in combating misinformation. By parsing through extensive digital datasets and contrasting narratives against trusted repositories, these platforms provide essential bulwarks against misinformation.

e. Geopolitical Implications of Digital Tools

Digital advancements are not merely tools; they have become potent weapons in the arsenal of statecraft and geopolitics. In the Baltic region, nations have reported alleged digital disinformation campaigns. Backed by sophisticated AI algorithms, these campaigns transcend traditional propaganda, hinting at the evolving fabric of geopolitical confrontations. Moreover, the proliferation of quantum computing adds another layer of complexity. As states like China and the United States make strides in quantum research, the potential decryption capabilities of these quantum machines present challenges to established cryptographic protocols.

f. Digital Surveillance and the Quantum Paradigm

Digital surveillance, augmented by AI-based facial recognition and extensive biometric databases, is reshaping state-citizen dynamics, often tilting the balance towards state oversight. The Belarusian protests in 2020 showcased state-backed digital surveillance's efficacy. Authorities employed advanced surveillance tools, leveraging AI algorithms for facial recognition, to track and, in many cases, preemptively detain protesters. However, on the flip side, the rise of quantum-resistant cryptographic algorithms provides a glimpse into future avenues where individual communications could remain secure, even in an age of advanced digital oversight.

e. Implications for Global Norms and Protocols

The intertwining of advanced technological frameworks with global information dynamics necessitates the formulation of new norms and oversight protocols. International consortiums, such as the United Nations, are now confronted with the imperative to devise standardized measures to ensure the stability of the digital realm. These measures encompass everything from countering digital misinformation to establishing protocols for state-backed digital operations. Recent moves by the United Nations, in collaboration with multiple state and non-state actors, to establish a framework for digital norms signify the recognition of this emerging domain's criticality. Such initiatives aim to provide a blueprint for responsible state behavior in the digital space, encompassing areas like cyber warfare, digital disinformation, and state-backed digital espionage.

As the landscape of global digital interactions undergoes rapid transformations, the technical and geopolitical implications of these shifts become increasingly intertwined. The complex interplay of advanced algorithms, AI-driven tools, and geopolitical objectives necessitates rigorous analytical frameworks and proactive measures. Addressing these challenges is not merely a technical imperative but a requisite for preserving the stability and integrity of global digital and geopolitical systems.

Criteria and Principles for Anti-Disinformation Policies

In developing policies to combat disinformation, it is essential that these policies are both effective and protect democratic values and rights. Authoritarian states, in particular, tend to prosecute individuals, criminalize disinformation, and establish state institutions that define what is and is not disinformation based on their own interests and worldviews. As a direct consequence, harsh sanctions against individuals lead to self-censorship by both users and journalists. Furthermore, the possibility of harsh government sanctions against social media platforms carries the risk that social media platforms will restrict freedom of expression on their platforms in order to avoid sanctions. All these risks and the negative effects of anti-disinformation policies become even more critical given the polarised nature of the digital media landscape in Turkey and the fragmentation of the media. Moreover, the heavy reliance on judicial procedures and the criminalization of disinformation risks politicizing disinformation regulation and turning it into a repressive mechanism, particularly in Turkey, where the independence of the judiciary is under serious threat and ranks very poorly globally. Therefore, both as a general principle and specifically for Turkey, policies to combat disinformation should adopt an inclusive approach that prioritizes the participation and balance of different stakeholders in order to ensure, the protection of democratic values and the protection of freedom of expression.

In addition, the disinformation landscape is undergoing major changes with the development of technologies in this field and has a very dynamic structure. Therefore, in order to ensure effective governance in this area, innovation, information sharing, and access to data by researchers and fact-checkers should be supported and encouraged, and a flexible governance method should be adopted.

Taking all these objectives into account, policies to combat disinformation should prioritise transparency and accountability as well as effectiveness. These regulations and initiatives should also focus on the preservation and strengthening of a vibrant information ecosystem, including stakeholders such as fact-checkers, researchers and the private sector, in order to uphold democratic rights and principles.

Policy Recommendations

- Regulations and especially laws designed to combat disinformation should be clear and unambiguous. The ambiguity of the wording used to define disinformation in legislation restricts freedom of expression by allowing the judiciary to arbitrarily use these laws as a weapon, taking advantage of the ambiguity of the wording and definitions and prosecuting those who share content that does not fall within the scope of disinformation. For this reason, very broad, vague and open to interpretation terms such as "information that misleads people", "disrupts the country's internal and external security, public order, public health or domestic peace" should be avoided or the meaning of these terms should be clearly stated in order to prevent arbitrary and selective judicial decisions.

- Adopting a multi-stakeholder approach rather than focusing on criminalization and the intervention of the state and the judiciary. Instead of criminalizing and targeting individuals, regulation should focus on cooperation between the private and public sectors, increased sharing of data and information with researchers and fact-checkers, ensuring that social media platforms take responsibility for combating disinformation on their platforms, and increasing transparency and accountability of the methods used to combat disinformation on these platforms. Criminalizing individuals often leads to self-censorship and does not solve the main problem. On the other hand, measures aimed at cooperation between stakeholders, prioritizing the transparent and appropriate implementation of self-regulation and co-regulation, and ensuring accountability, both strengthen a strong information ecosystem, which is essential to effectively combat disinformation, by creating a cooperative and flexible model that is necessary to take measures against advanced technologies and new developments in this dynamic field, and to prevent a blow to democratic rights and freedoms.

- Establishing and implementing redressive measures based on clear and effective procedures. Judicial decisions and related sanctions against both platforms and individuals should be appealable. The inability to challenge verdicts and sanctions seriously undermines accountability, and individuals' beliefs and fears that these verdicts cannot be challenged may push them toward self-censorship. Similarly, in cases where it is difficult or even impossible to challenge judicial decisions, social platforms may see the filing of these lawsuits and the imposition of these sanctions as a much greater risk, and these social platforms may harm freedom of expression by taking overly restrictive measures on their own platforms to avoid these sanctions and to avoid being targeted. This is particularly important in a country like Turkey, where the judiciary is under pressure and there are problems with judicial independence. The politicization of judicial decisions and the belief that state intervention is crucial in these decisions when remedies are ineffective increases self-censorship and undermines accountability. It should be noted, however, that the mere existence of these measures on paper does not solve this problem. These procedures, rights of appeal and processes must be easily accessible and clear, and the completion of these procedures and processes must be guaranteed within a specified timeframe. Otherwise, even if these measures are officially in place, the improbability of getting positive results (e.g. these appeal procedures take too long, it is difficult to appeal decisions) will still lead to the negative consequences mentioned above.

BIBLIOGRAPHY

1. Christopoulou, Androniki. "The Information Disorder Ecosystem: A Study on the Role of Social Media, the Initiatives to Tackle Disinformation and a Systematic Literature Review of False Information Taxonomies," April 18, 2019. https://repository.ihu.edu.gr//xmlui/handle/11544/29381.

2. Doyle, Brittany. "Self-Regulation Is No Regulation--The Case for Government Oversight of Social Media Platforms." Indiana International & Comparative Law Review 32, no. 1 (April 11, 2022): 97–130.

3. Epstein, Ben. "Why It Is So Difficult to Regulate Disinformation Online." In The Disinformation Age, edited by W. Lance Bennett and Steven Livingston, 1st ed., 190–210. Cambridge University Press, 2020. https://doi.org/10.1017/9781108914628.008.

4. justitia. "The Digital Berlin Wall – How Germany (Accidentally) Created a Prototype for Global Online Censorship – Act Two." The Future of Free Speech, October 1, 2020. https://futurefreespeech.com/the-digital-berlin-wall-how-germany-accidentally-created-a-prototype-for-global-online-censorship-act-two/.

5. Lewandowsky, Stephan, Laura Smillie, David Garcia, Ralph Hertwig, Jim Weatherall, Stefanie Egidy, Ronald E. Robertson, et al. "Technology and Democracy: Understanding the Influence of Online Technologies on Political Behaviour and Decision-Making." JRC Publications Repository, October 26, 2020. https://doi.org/10.2760/709177.

6. Ryan, Camille D., Andrew J. Schaul, Ryan Butner, and John T. Swarthout. "Monetizing Disinformation in the Attention Economy: The Case of Genetically Modified Organisms (GMOs)." European Management Journal 38, no. 1 (February 1, 2020): 7–18. https://doi.org/10.1016/j.emj.2019.11.002.

7. Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." Science 359, no. 6380 (March 9, 2018): 1146–51.
https://doi.org/10.1126/science.aap9559.

Centre for Economics
and Foreign Policy Studies

edam

Address : Hare Sokak NO:16 AKATLAR 34335 İstanbul/Türkiye
Phone : +90 212 352 18 54
Fax : +90 212 351 54 65
Email : info@edam.org.tr