

Navigating the Intersection of Technology, Disinformation, and Human Rights: Balancing Freedom of Expression and Speech*

Hamza Iftikhar,^{1*} Umelaila Shah,² Uzair Hashmi,³

Inayatullah,⁴ Sanaullah Khan⁵

National University of Science and Technology, Islamabad, Pakistan



[10.15408/jch.v13i2.47165](https://doi.org/10.15408/jch.v13i2.47165)

Abstract

The spread of deceptive content online threatens human rights, particularly freedom of expression and access to accurate information. In Pakistan, the rise of digital platforms has fuelled misinformation, weakening democratic processes, polarizing society, and eroding public trust. The challenge lies in balancing disinformation regulation with protecting free speech. While false narratives undermine institutions, restrictive measures risk suppressing dissent and opposition voices. The Prevention of Electronic Crimes Act (PECA) exemplifies this tension. This study critically evaluates Pakistan's regulatory approach, assessing its effectiveness and alignment with international human rights standards. Through qualitative analysis of PECA's provisions and case studies, findings highlight key concerns: ambiguous legal definitions and politically motivated enforcement. Case studies illustrate how disinformation affects public trust and democratic engagement. Despite the challenges posed by disinformation, a practical framework must protect fundamental rights while addressing online harms. Recommendations include refining PECA's provisions, introducing robust procedural safeguards, and promoting digital literacy programs to empower citizens to counter misinformation. A multi-stakeholder approach involving government, civil society, and technology platforms is essential for fostering a more accountable digital environment in Pakistan. Striking a balance between regulation and free speech is crucial for preserving democracy and public trust.

Keywords: Disinformation; Human rights; Freedom of expression; Freedom of information; Prevention of Electronic Crimes Act (PECA)

* Received: January 15, 2025, revised: March 17, 2025, accepted: June 24, 2025, Published: June 30, 2025.

^{1.} **Hamza Iftikhar.** PhD, Assistant Professor, Department of Government of Public Policy, School of Social Sciences and Humanities, National University of Science and Technology, 44000, Islamabad, Pakistan. Email: hiftikhar@s3h.nust.edu.pk, ORCID: <https://orcid.org/0000-0001-8278-3747>

^{2.} **Umelaila Shah.** Associate Professor, Department of Government of Public Policy, School of Social Sciences and Humanities, National University of Science and Technology, 44000, Islamabad, Pakistan. Email: dr.umelaila@s3h.nust.edu.pk, ORCID: <https://orcid.org/0000-0001-5935-4637>

^{3.} **Uzair Hashmi.** Head of Department, Government of Public Policy, School of Social Sciences and Humanities, National University of Science and Technology, 44000, Islamabad, Pakistan. Email: uzair.s3h@s3h.nust.edu.pk ORCID: <https://orcid.org/0000-0002-5800-3189>

^{4.} **Inayatullah.** Assistant Professor, Department of Government of Public Policy, School of Social Sciences and Humanities, National University of Science and Technology, 44000, Islamabad, Pakistan. Email: inayat@s3h.nust.edu.pk, ORCID: <https://orcid.org/0000-0003-0520-0311>

^{5.} **Sanaullah Khan.** Assistant Professor, Department of Government of Public Policy, School of Social Sciences and Humanities, National University of Science and Technology, 44000, Islamabad, Pakistan. Email: sanaullah.s3h@s3h.nust.edu.pk ORCID: <https://orcid.org/0009-0001-3194-2442>

**Corresponding author: hiftikhar@s3h.nust.edu.pk

A. INTRODUCTION

With the rapid dissemination of online information in the contemporary digital era, the landscape of global communication has been completely transformed. On the other hand, such a change made it even easier to circulate false information, which poses new challenges to human rights, including free speech and access to reliable information ([Wardle & Derakhshan, 2017](#)). According to Freedom House ([2023](#)), the consequences of disinformation are compounded by the political polarization and institutional fragility of emerging democracies like Pakistan, and the situation remains aggravated. Democratic processes are under threat worldwide; disinformation amplifies social divisions and undermines public confidence in the media. Wild misinformation, McKay and Tenove ([2021](#)) have argued, is a form of political discourse that undermines governments and leads to more conflicts. Various governments around the world have enacted legal frameworks to control disinformation; however, such efforts often jeopardize free speech and expression. Such is the challenge in formulating strategies that serve as effective counter-disinformation while preserving authentic dissent and opposition. ([Human Rights Watch, 2022](#))

The widespread use of social media, coupled with the pervasiveness of the Internet in Pakistan's digital landscape, has given a fillip to misinformation (Chan et al., 2024). Misinformation on highly sensitive social and political issues, such as minority rights, health crises, and elections, has been addressed through campaigns aimed at deepening political divisiveness and eroding public faith in democratic institutions ([Azam, 2021](#)). This is because, though there is a proliferation of online platforms that afford more opportunities for citizen participation, this often makes fighting the damage that misinformation can cause more difficult. Against this backdrop, Pakistan's Prevention of Electronic Crimes Act of 2016 is a significant legislative tool in combating cybercrime, including disinformation ([Azam, 2021](#)). Though the PECA covers some aspects of digital scarring, critics have argued that its overly broad provisions could be used to justify political repression, targeting journalists, activists, and opposition with disproportionate frequency or severity. However, Pakistan's regulatory structure has failed to meet these standards, thereby earning the ire of domestic and foreign stakeholders alike.

The EU's analysis of the Digital Services Act, along with other effective regulatory models, could prove helpful to Pakistan's digital governance. Reform in policies, stakeholder engagement, and mass education are key components of the multi-pronged strategy against disinformation in Pakistan. Digital literacy programs are considered to be an integral part of equipping citizens to assess

information critically and avert the spread of false news narratives ([Jia et al., 2024](#)). Besides defending democratic freedoms, regulatory efforts can be more efficient through collaboration among government, civic society, and technology platforms. To align with the suggestions and limitations provided, the scope of the study is now focused on events and cases after the enactment of the Prevention of Electronic Crimes Act (PECA) in 2016, ensuring the analysis remains relevant to the framework's application in Pakistan—vaccine misinformation globally and in Pakistan, and issues surrounding polio vaccination campaigns.

In light of these, it is clear that there is an urgent need for a balanced regulatory framework capable of combating disinformation effectively without infringing on freedom of expression. It covers the three-layered tangle of human rights, disinformation, and technology in Pakistan. To that end, the focus is on setting out options that are realistic from a political perspective but capable of striking a proper balance between regulation of disinformation and freedom of expression, by analyzing them against internationally prescribed standards through a critique of existing regulatory frameworks.

Literature Review

1. Technology and the Amplification of Disinformation

The rapid evolution of digital technology has transformed the way information is created, disseminated, and consumed. While digital platforms have expanded access to information, they have also accelerated the spread and impact of disinformation. Disinformation, defined as the deliberate presentation of false or misleading information with the intent to deceive, has always existed; however, the digital era has amplified its reach and consequences through the speed, anonymity, and scale enabled by modern technologies. ([Alibašić, 2024](#))

Social media platforms, in particular, have played a significant role in the widespread dissemination of disinformation. The algorithms employed by these platforms prioritize engagement-driven content, often favoring sensationalized, misleading, or emotionally charged information over factual reporting. As a result, disinformation tends to spread more rapidly than verified news, contributing to what scholars describe as an 'information disorder' ([McKay & Tenove, 2021](#)). This disorder consists of three primary categories: (1) disinformation—deliberately false content intended to mislead, (2) misinformation—incorrect information shared without malice, and (3) malinformation—accurate information shared with harmful intent. Each of these

categories poses distinct challenges to democratic governance and societal cohesion.

The ability of digital technology to manipulate public perception has been demonstrated in numerous global events. Disinformation campaigns have influenced elections, shaped public discourse on critical issues, and incited social unrest. For example, during the COVID-19 pandemic, conspiracy theories about vaccines and public health measures spread rapidly online, undermining trust in medical institutions and government interventions ([Jia et al., 2024](#)). Similarly, the use of coordinated disinformation campaigns during electoral processes, as observed in the 2016 U.S. presidential election and India's national elections, has raised concerns about foreign interference, political polarization, and the erosion of democratic norms. ([Tenove, 2020](#); [George, 2024](#))

The anonymity and virality of digital interactions further complicate efforts to combat disinformation. Unlike traditional media, where content is subject to editorial oversight, digital platforms allow virtually anyone to create and distribute content with minimal accountability. Moreover, the use of deepfake technology, automated bots, and micro-targeted political advertisements has enabled malicious actors to manipulate public opinion at an unprecedented scale ([Helm & Nasu, 2021](#)). These technologies have not only made it difficult for users to distinguish between credible and false information but have also strained regulatory bodies' ability to enforce effective countermeasures.

Efforts to mitigate the spread of disinformation have led to regulatory interventions worldwide. The European Union's Digital Services Act (DSA) represents one of the most comprehensive approaches to addressing online disinformation while safeguarding freedom of expression. It mandates transparency in content moderation, imposes accountability on digital platforms, and ensures independent oversight ([Vese, 2022](#)). However, in countries like Pakistan, where digital literacy levels remain low, and regulatory frameworks such as the Prevention of Electronic Crimes Act (PECA) are criticized for their vague definitions and selective enforcement, the challenge remains acute. Addressing disinformation in such contexts requires a combination of policy reforms, enhanced digital literacy programs, and multi-stakeholder collaboration to balance free speech and online safety effectively.

2. Human Rights and Freedom of Expression

The UDHR and the ICCPR are among the most important international documents on human rights, along with several other key instruments. Both

these schemes protect freedom of expression as a right, recognizing its primacy in democratic societies ([Howie, 2018](#)). They also, however, recognize that such a right is not absolute and may be limited, so long as such limitations are lawful, necessary, and expedient. A key complication arises from the balance required between the restraint of misinformation and the protection of free speech. ([Klein & Klein, 2017](#); [Shou et al., 2024](#))

On the other hand, if disinformation is left to flow freely, then the right to seek information and the ability to make informed choices are both harmed ([Klein & Klein, 2017](#); [Vese, 2022](#)). According to Shou et al. ([2024](#)), excessive regulatory measures can suppress political opposition and constrain legitimate dissent in countries with fragile democratic institutions. This makes the balance between restraining misinformation and protecting free speech a key challenge. If, on the other hand, disinformation is allowed to flow freely, both the right to seek information and the right to make an informed choice are harmed. ([McKay & Tenove, 2021](#); [Helm & Nasu, 2021](#))

Furthermore, the growing presence of government-led regulatory frameworks, such as India's IT Rules of 2021 and Pakistan's PECA, has sparked debate over their effectiveness in curbing misinformation while preserving democratic values ([Shankar & Ahmad, 2021](#); [Iqbal et al., 2023](#)). Critics argue that poorly defined legal frameworks could serve as instruments of state control rather than genuine counter-disinformation measures ([Tenove, 2020](#); [Saleem et al., 2022](#)). To ensure alignment with international standards, regulatory measures should incorporate transparency, accountability, and independent oversight mechanisms, as modeled by the EU's Digital Services Act ([Kaushal et al., 2024](#); [Ness, 2024](#)).

3. Global Legal Frameworks on Freedom of Expression and Disinformation

The challenges posed by disinformation have thus led to the creation of legal frameworks worldwide, among which the DSA of the European Union was considered one of the most significant, owing to its comprehensive strategy for balancing free speech with the containment of online harmful content such as misinformation ([Vese, 2022](#)). The DSA places great emphasis on accountability and transparency by requiring platforms to publish their content moderation guidelines, granting independent monitoring organizations greater powers, and ensuring effective regulatory action. The European Commission aims to establish a secure digital environment that respects user rights. This framework serves as a benchmark for balancing regulatory intervention with human rights

considerations ([Vese, 2022](#)). However, developing countries, of which Pakistan is a part, have instituted regulatory measures that are at times neither transparent nor accountable. Thus, the legitimate criticism and opposition have been silenced, reflecting the dangers of authoritarian overreach when regulatory systems are not suitably checked. Furthermore, the compulsion to trace the origin of injurious messages was imposed on social media platforms by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ([Shankar & Ahmad, 2021](#)). The move has been criticized for potential breaches in privacy and the threat of its abuse against journalists and campaigners. Rather than relying on its own initiatives, the United States relies primarily on platform self-regulation to address disinformation. ([Shankar & Ahmad, 2021](#))

Companies such as Facebook and Twitter have taken measures, including fact-checking and content labeling, to reduce disinformation. These, however, have been criticized for discrepancies in their approach, and the lack of transparency in their enforcement has highlighted weaknesses in leaving the regulation of misinformation to private entities alone ([Helm & Nasu, 2021](#)). The contrast between these two viewpoints leads us to weigh the balance. Stringent regulatory measures are in place to combat disinformation.

While there is a specific Prevention of Electronic Crimes Act, PECA, in place in Pakistan, which has been enacted to fight against cybercrimes and digital harm, it draws criticism for its overly broad prohibitions and vulnerability to abuse. Ambiguous terminology, such as "false information" and "offences against dignity," for example, creates loopholes that may be utilized to suppress the expression of dissent on the pretext of combating disinformation ([Iqbal et al., 2023](#)). This is because the law's ill-defined nature denies legitimacy and calls into question the legality of the standards set out in international conventions, such as the Rabat Plan of Action, which support proportional, necessary, and clearly defined legislative restrictions on bad speech. One main problem Pakistan faces is an ambiguous legal system. Although it is effective at preventing the spread of misinformation during crises, the Protection against Online Falsehoods and Manipulation Act (POFMA) in Singapore has been criticised for granting government agencies excessive discretionary power.

However, these measures must be designed to prevent misuse and ensure that fundamental freedoms, such as freedom of expression and privacy, are not violated. The failure of PECA to keep disinformation at bay and the attendant threat it has become for democratic values and human rights demonstrates how poorly defined legislation has become a nightmare, as is happening in Pakistan.

Meanwhile, a more open, responsible, and rights-respecting approach to digital governance will help Pakistan learn from international best practices.

4. Case Studies and Regulatory Challenges

Disinformation campaigns in digital environments have emerged as a pervasive global challenge, with significant social, political, and economic consequences. Examining case studies from around the world highlights how disinformation operates within specific contexts and its broader implications.

a. United States: Electoral Disinformation

The 2016 US presidential election has, in no small measure, thrown into the spotlight the most ubiquitous role disinformation plays in shaping election results. Coordinated disinformation efforts, primarily attributed to foreign organizations — most notably the Internet Research Agency of Russia — aimed to change how people believe and act toward an event, potentially discouraging participation in democratic undertakings and sapping democratic institutions of much-needed confidence. ([Tenove, 2020](#))

A wide array of tactics was used, including the spread of false narratives on social media platforms such as Facebook and Twitter. False stories about electoral fraud, candidates' personal scandals, and fabricated policy positions were circulated to undermine voter confidence and sow discord among political factions. Some disinformation campaigns aimed to discourage voter turnout among specific demographics by spreading false information about voting dates, registration requirements, and polling locations. A prime example was the claim that voters could cast their ballots via text message, a falsehood designed to mislead and disenfranchise targeted groups. ([Tenove, 2020](#))

The fallout of these disinformation campaigns highlighted critical vulnerabilities in digital media governance, particularly regarding the opacity of platform responsibility. Algorithms designed to prioritize engagement inadvertently amplified misleading content, while the lack of stringent content moderation policies allowed such misinformation to spread unchecked. Social media companies initially resisted regulatory oversight, arguing for the primacy of free speech. However, mounting pressure from lawmakers and civil society organizations eventually led to increased scrutiny and policy adjustments.

The long-term impact of electoral disinformation in the US extends beyond a single election cycle. It has contributed to persistent doubts about election integrity, heightened political polarization, and growing public distrust in

mainstream media. Subsequent elections, including the 2020 presidential race, saw further disinformation campaigns, this time not only from foreign actors but also from domestic sources. The Capitol riots of January 6, 2021, were fueled in part by disinformation narratives about election fraud, illustrating how unchecked falsehoods can have real-world consequences. ([McKay & Tenove, 2021](#))

To address these challenges, regulatory interventions such as the Honest Ads Act and increased transparency requirements for platforms have been proposed. Social media companies have also implemented fact-checking initiatives, labeled misleading content, and de-platformed accounts spreading false narratives. However, critics argue that these measures remain inconsistent and reactive rather than proactive. Lessons from the US case emphasize the need for multi-stakeholder collaboration, improved digital literacy, and robust regulatory frameworks that balance free speech with mechanisms to curb malicious disinformation.

b. India: Disinformation and Communal Tensions

Disinformation often results in disastrous consequences in India, exacerbating violence and communal tensions. A striking example of this is the fake news regarding child kidnappings, which spread rapidly across WhatsApp, leading to acts of mob lynching in rural areas. These incidents illustrate how misinformation can catalyze real-world violence, particularly in regions with relatively low digital literacy and existing social fault lines ([George, 2024](#)). Misinformation about the alleged criminal activities of certain groups, especially minorities, has fueled vigilantism, with deadly consequences. These trends highlight the potency of unverified digital content in a highly diverse and politically charged society.

Disinformation campaigns in India have not been limited to criminal hoaxes but have also played a critical role in electoral politics. In multiple election cycles, fabricated claims about minority communities allegedly conspiring against the majority have been systematically propagated to polarize voters. Social media platforms have become battlegrounds for politically motivated misinformation, with bots and troll farms actively amplifying divisive narratives. For instance, manipulated videos, photoshopped images, and out-of-context statements have been widely circulated to demonize political opponents and sway public opinion. The coordinated nature of these campaigns suggests a strategic effort to exploit religious and ethnic divides for electoral gains. ([Mansoor, 2024](#))

The consequences of such disinformation extend beyond electoral cycles, as they deepen societal divisions and erode trust in democratic institutions. During times of heightened communal tensions, misinformation has been used to incite riots and fuel sectarian clashes. The 2020 Delhi riots, for example, were partially fueled by inflammatory content shared on social media platforms, which spread misleading claims about violent activities from different religious groups. The rapid spread of these narratives contributed to escalating violence before law enforcement could intervene effectively.

In response, the Indian government has introduced regulatory measures to curb the spread of harmful misinformation. Platforms like Facebook, Twitter, and WhatsApp have been pressured to strengthen their content moderation policies, introduce fact-checking mechanisms, and implement forward limits on viral messages. The government also introduced stricter guidelines under the Information Technology ([Intermediary Guidelines and Digital Media Ethics Code Rules, 2021](#)), which mandate social media platforms to trace the origin of messages flagged as misinformation. However, these measures have been criticized for being reactive rather than proactive and for lacking a clear framework to distinguish between legitimate dissent and harmful disinformation. ([Mansoor, 2024](#))

Critics argue that some of these regulations have also been selectively enforced to suppress political dissent, with journalists and activists facing scrutiny under broad and ambiguously worded legal provisions. The need for a more structured, transparent, and independent regulatory framework is evident, as is the necessity of large-scale digital literacy campaigns. Educating citizens on identifying misinformation and encouraging responsible online behavior are critical steps to mitigating the impact of disinformation in a highly polarized society. The Indian case underscores the urgent need for proactive governance, accountability in platform policies, and collaborative efforts between tech companies, civil society, and government institutions to prevent the dangerous real-world effects of digital misinformation.

C. Philippines: Disinformation as a Political Weapon

Disinformation in the Philippines has been systematically employed as a political tool, particularly under the administration of Rodrigo Duterte. His tenure saw a significant expansion of digital propaganda, with government-backed "troll armies" playing a central role in manipulating public opinion. These operations aimed to bolster pro-government narratives while simultaneously discrediting critics, journalists, and human rights activists. Coordinated campaigns spread false or misleading material on social media platforms, often

portraying opposition leaders as corrupt, criminals, or foreign agents acting against national interests. ([Kusaka, 2022](#))

A notable example of such disinformation was the spread of fabricated allegations against opposition figures, including presidential candidates and outspoken critics of the Duterte administration. Social media platforms like Facebook, YouTube, and Twitter were flooded with coordinated messaging aimed at shifting public perception in favor of the ruling party. Fake news articles, doctored images, and deepfake videos were widely circulated to discredit opposition voices and silence dissent. Journalists investigating government misconduct were not only harassed online but also faced legal repercussions through fabricated charges, an extension of state-sponsored disinformation weaponized to control the narrative. ([Kusaka, 2022](#))

The consequences of this disinformation campaign extended far beyond political mudslinging. It led to the erosion of democratic norms, the suppression of freedom of speech, and an environment where public discourse was dominated by state-sponsored propaganda. The demonization of critics played a key role in justifying the government's aggressive actions, including its infamous "war on drugs," which resulted in thousands of extrajudicial killings. Social media disinformation fueled public support for these violent crackdowns by exaggerating crime statistics and framing dissenters as sympathizers of drug cartels. ([Mansoor, 2024](#))

A striking feature of the Philippines' disinformation landscape is the involvement of influencers and content creators who are co-opted into amplifying government messaging. Political vlogging and paid digital marketing strategies have been extensively used to shape public perception, often blurring the lines between state propaganda and grassroots support. These influencers receive direct funding or indirect incentives to promote government narratives, making it difficult to distinguish between authentic public opinion and manufactured consent. ([Mansoor, 2024](#))

Attempts to regulate disinformation in the Philippines have been largely ineffective due to a lack of political will. Despite calls for stronger digital governance and accountability measures, platforms have struggled to consistently and impartially enforce content moderation policies. The government's control over mainstream media further limits the effectiveness of fact-checking initiatives, as many independent watchdogs have faced intimidation and financial constraints. Legislative measures, such as the Anti-Fake News Bill, have been proposed. However, critics argue that these efforts are

often designed to criminalize dissent rather than genuinely address the disinformation crisis. ([Kusaka, 2022](#))

The case of the Philippines highlights the dangers of state-sponsored disinformation in an era of digital influence. It underscores the need for independent regulatory bodies, robust fact-checking institutions, and international collaboration in curbing digital manipulation. Without structural reforms and digital literacy initiatives, the unchecked spread of disinformation will continue to threaten democratic integrity and civic freedoms in the country.

d. European Union: Transparent and Inclusive Regulation

The European Union offers a comprehensive, structured approach to combating disinformation through regulatory mechanisms, such as the Digital Services Act (DSA). The DSA is a forward-thinking legislative framework designed to enhance transparency, accountability, and user protection within the digital ecosystem. Unlike many other global regulatory efforts, the EU's approach does not solely rely on punitive measures; instead, it emphasizes procedural fairness, platform accountability, and multi-stakeholder collaboration to ensure that online spaces remain both free and secure. ([Ness, 2024](#))

A key feature of the DSA is its requirement that digital platforms, huge online service providers, publicly disclose their content moderation policies, algorithms, and decision-making processes for harmful or misleading content. This requirement ensures that users and regulatory bodies can scrutinize how platforms handle disinformation and misinformation. Platforms are further mandated to publish regular reports detailing enforcement actions, providing transparency that is often missing in other regulatory environments ([Kaushal et al., 2024](#)). This approach contrasts sharply with more reactive or censorship-heavy methods seen in countries like India and the Philippines, where government authorities often exercise excessive control over content moderation.

Another distinguishing characteristic of the EU's strategy is multi-stakeholder engagement, which fosters cooperation between governments, civil society organizations, technology companies, and independent regulatory bodies. This model ensures that regulatory actions are not unilateral but rather benefit from diverse perspectives, preventing undue government influence over content regulation. The EU Code of Practice on Disinformation, a self-regulatory framework developed alongside the DSA, requires online platforms to work with fact-checkers, researchers, and civil society groups to counteract false narratives

in a non-partisan manner ([Kaushal et al., 2024](#)). This collaborative method sets a high standard for global digital governance.

In the context of procedural fairness, the DSA requires digital platforms to provide clear avenues for users to appeal content moderation decisions. This ensures that individuals who believe their content has been wrongfully removed or flagged can seek redress through transparent, structured mechanisms. Such measures not only improve public trust in content moderation processes but also safeguard against overreach by governments or private entities ([Ness, 2024](#)). Moreover, the legislation introduces significant fines for non-compliance, reinforcing the necessity for digital companies to uphold ethical and responsible platform management.

The EU's regulatory framework also aims to counter algorithmic amplification of harmful content. Large platforms must implement risk assessment procedures to analyze how their algorithms contribute to the spread of disinformation. In cases where algorithms disproportionately boost false information, companies must make modifications to limit such distortions ([Vese, 2022](#)). This approach addresses the root causes of misinformation rather than merely penalizing offenders, making it a model for sustainable regulation.

Compared with the United States, India, and the Philippines, where disinformation regulation often faces political and enforcement challenges, the EU's DSA serves as a balanced regulatory model that simultaneously protects freedom of expression and curtails harmful online behavior. By focusing on transparency, procedural fairness, and accountability rather than outright censorship, the EU provides a replicable framework for other nations to refine their digital governance policies. Moving forward, the effectiveness of the DSA will depend on ongoing compliance monitoring and enforcement, but it already marks a significant step toward responsible digital regulation worldwide.

e. Pakistan Disinformation Challenges

Since the enactment of the Prevention of Electronic Crimes Act (PECA) in 2016, Pakistan's digital ecosystem has grappled with an escalating crisis of disinformation. Political polarization, low digital literacy, and the pervasive use of social media platforms have combined to create a perfect storm, enabling the rampant spread of false information ([Khan & Tehrani, 2019](#)). Disinformation campaigns have targeted key national concerns, including elections, public health, and minority communities, with far-reaching consequences for public trust, institutional credibility, and societal cohesion. ([Saleem et al., 2022](#))

During the 2018 General Elections, disinformation significantly undermined public confidence in the electoral process. False narratives about electoral fraud and the illegitimacy of candidates circulated widely on platforms such as WhatsApp and Facebook, fueling political divisions and eroding trust in democratic institutions. Beyond elections, disinformation has posed a grave threat to public health. Vaccine misinformation, particularly during the COVID-19 pandemic, spread rapidly on social media, with false claims about infertility and severe allergic reactions gaining traction ([Khan & Tehrani, 2019](#)). This fueled vaccine hesitancy, jeopardized public health campaigns, and strained already fragile institutional trust.

To counter the growing digital harms, Pakistan introduced PECA, a regulatory framework to combat cybercrime, including disinformation. However, PECA has faced extensive criticism for its broad scope and vague language. Terms like "false information" lack precise definitions, leaving the law open to selective interpretation and arbitrary enforcement ([Saleem et al., 2022](#)). Critics argue that PECA has been used repeatedly to suppress dissent rather than combat genuine online harm. Civil society organizations and legal experts have highlighted cases in which PECA was used to censor journalists, activists, and political opponents under the guise of regulating disinformation. ([International Commission of Jurists, 2022](#))

This misuse of the law has raised serious concerns about its impact on freedom of expression and democratic values. The most troubling consequence of PECA's implementation has been its chilling effect on free expression. Fear of legal repercussions has compelled many journalists and civil society organizations to engage in self-censorship, shrinking the space for critical discourse and public accountability. Democratic institutions have suffered as a result, as the suppression of dissent undermines the foundational principle of open debate. Furthermore, the selective application of PECA, often targeting opposition politicians and independent media, has fueled perceptions of government bias and authoritarianism ([Iqbal, 2023](#)). This erodes public trust and deepens societal divisions, compounding the damage caused by disinformation.

In conclusion, Pakistan faces a dual challenge: the widespread dissemination of disinformation and the misuse of broad regulatory measures like PECA. Disinformation campaigns threaten to widen societal fissures and erode institutional trust, while vague and overreaching laws risk silencing legitimate dissent and narrowing democratic space. Addressing these challenges requires urgent reforms to PECA to ensure clear definitions, proportional enforcement, and robust procedural safeguards. Simultaneously, greater public

awareness and accountability mechanisms are essential to restore confidence in democratic institutions. Combatting disinformation must be pursued without infringing upon fundamental rights, striking a balance between effective regulation and the preservation of freedom of expression.

B. METHODS

This research design is qualitative, focusing on case studies and content analysis to critically examine the complex relationship between disinformation regulation and freedom of expression in Pakistan. These methods are applicable to ensure a systematic and contextual understanding of the effectiveness of Pakistan's regulatory frameworks, such as the Prevention of Electronic Crimes Act (PECA), and to assess their alignment with international human rights conventions. This approach ensures that the socio-political implications of disinformation regulation are explored in an evidence-based manner, focusing on specific incidents and analyzing relevant legal and policy documents.

Case studies have been purposively selected to represent high-impact incidents that demonstrate the implications of disinformation across societal and political domains, as well as the application of the Prevention of Electronic Crimes Act. These include the 2018 general elections, when coordinated disinformation campaigns undermined public confidence in democratic processes; COVID-19 vaccine misinformation, which brought to the fore the role of false narratives in derailing public health initiatives; and the suppression of dissent, in which PECA has been used to target journalists and activists. Complementing the case studies, content analysis systematically examines legal and policy documents, including PECA and its amendments, procedural guidelines issued by the PTA, and reports from advocacy groups such as Amnesty International. Additionally, the digital content of social media has been included in the paper, focusing on specific narratives related to incidents of disinformation. These were coded for themes, including legal ambiguities, enforcement proportionality, and the socio-political effects of disinformation, enabling an in-depth look at Pakistan's regulatory landscape from the perspective of best global practices. Taken together, these case studies and content analyses provide a nuanced, evidence-based foundation for assessing the efficacy of regulatory frameworks and their adherence to international human rights standards.

C. RESULTS

The integration of case studies with content analysis provides evidence of a deep understanding of the complex dynamics of disinformation in Pakistan. These findings show how far-reaching the consequences of disinformation are to public trust, democratic processes, and institutional stability, while noting limitations and misuses within the regulatory framework under the Prevention of Electronic Crimes Act.

1. Impact of Disinformation

a. Effects on Public Trust, Media, and Institutions

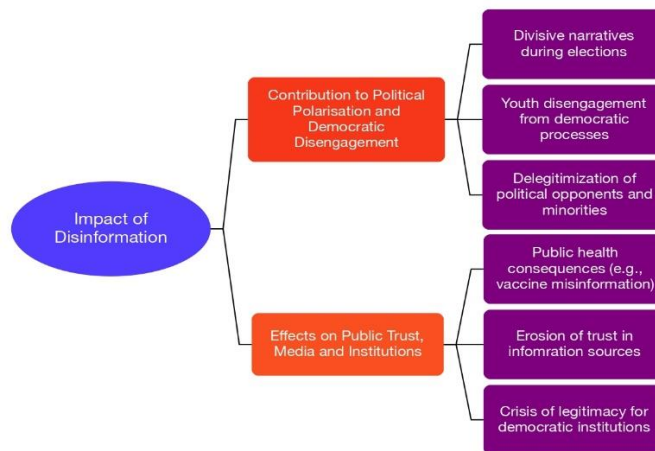


Fig 1. Impact of disinformation on public trust, media, and institutions

Information has eroded public trust in the media, government institutions, and democratic processes in Pakistan. From the content analysis of digital platforms and public narratives, an increased level of skepticism towards credible sources of information was evident, corroborated by the widespread propagation of false or misleading content. Case studies, such as the spread of misinformation about vaccination during the COVID-19 pandemic, have illustrated how disinformation hampered public health by fostering fear and skepticism about vaccination. For instance, WhatsApp messages claimed that vaccines caused infertility; such baseless stories led to lower vaccination rates in rural areas and added to the public health resource strain.

This has generally led to a loss of confidence in media institutions, too, as disinformation blurred the line between factual reporting and partisan propaganda. The content analysis of significant disinformation-related events,

such as those surrounding the 2018 General Elections, demonstrated how false narratives about electoral fraud and institutional corruption further polarized the public. This is what contributes to a situation in which democratic institutions are losing legitimacy, furthering a crisis of governance and political instability. Furthermore, disinformation has resulted in the deepening of political polarization by magnifying divisive narratives against opposition groups and minority communities. Case studies even reveal organized campaigns that use fabricated stories during election periods to defame opponents. Included are sensationalized, fake stories about the candidate's personal life and financial scandals that emerged on social media during the 2018 elections; these stories trend on anonymous accounts, shape voters' views, and fuel political polarization.

This is one of the ways democratic disengagement occurs. With so many voices speaking conflicting truths, there is a sense in which citizens are withdrawing from participation, citing feelings of disillusionment and confusion. According to a content analysis of social media trends, disinformation has greatly facilitated disengagement among young voters—people who should be of particular significance in democratic renewal. This trend has, in the long run, threatened Pakistan's democratic system.

2. Regulatory Framework Evaluation

a. Scope, Strengths, and Criticisms of PECA

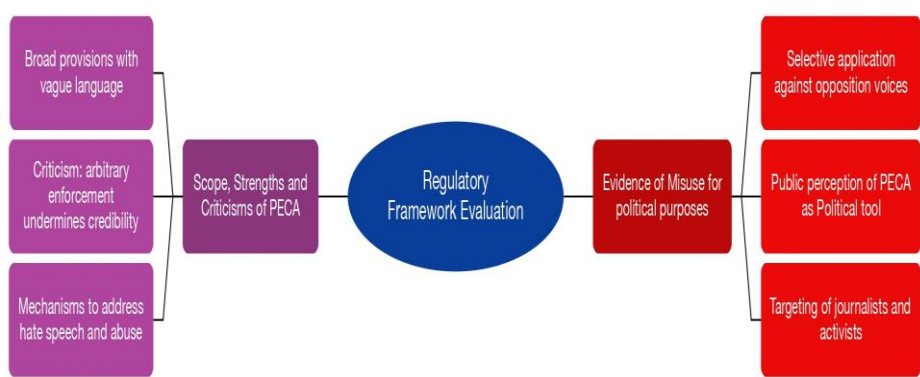


Fig 2. Scope, Strengths, and Criticisms of PECA

The Prevention of Electronic Crimes Act (PECA) was enacted as a comprehensive legal framework to regulate cybercrimes, including disinformation, in Pakistan. Content analysis of the Act and its subsequent amendments indicates that it was designed to "engage in harmful content while securing digital spaces." However, PECA has faced widespread criticism for its broad, vague language, particularly in the definitions of terms such as "false information" and "offenses against dignity." The lack of precise definitions has made the law susceptible to arbitrary enforcement, raising concerns about its credibility and effectiveness in addressing cybercrimes without infringing on fundamental rights.

b. Strengths of PECA

Mechanisms to Address Hate Speech and Abuse: One of PECA's significant strengths is its ability to address cybercrimes, online harassment, and hate speech. The law provides legal recourse against individuals engaging in malicious online activities, including cyberbullying, identity theft, and defamation. This has been beneficial in curbing digital abuse and providing victims with legal protections.

Reporting and Complaint Mechanisms: The Act establishes formal complaint channels that allow individuals to report instances of digital harassment, defamation, and cyber fraud. These mechanisms have played a role in safeguarding vulnerable groups, particularly women, journalists, and activists, who are often the target of online abuse.

Legal Provisions for Digital Security: PECA introduces penalties for unauthorized access to personal data, hacking, and online financial fraud, making it a crucial legal instrument in Pakistan's digital governance landscape. The law also grants law enforcement agencies investigative authority, enabling them to combat serious cyber threats effectively.

c. Criticisms and Weaknesses of PECA

Broad and Vague Provisions: One of the most significant criticisms of PECA is its overly broad language, which allows for subjective interpretation and selective enforcement. Terms such as "false information" and "offenses against dignity" are not clearly defined, allowing authorities to apply the law arbitrarily.

Arbitrary and Disproportionate Enforcement: Legal experts and human rights organizations have highlighted how PECA is often used disproportionately against journalists, activists, and political opponents, rather than focusing solely on cybercriminals. Cases have emerged where journalists

and dissenting voices have been charged under PECA for reporting on corruption or criticizing government policies, eroding press freedom and shrinking democratic space.

Undermining Freedom of Expression: While PECA aims to regulate harmful digital content, it has been criticized for restricting free speech rather than effectively targeting disinformation. The ambiguity in the law's provisions has created a chilling effect, where individuals self-censor to avoid legal repercussions.

Lack of Procedural Safeguards: The absence of clear procedural safeguards has made it easier for the law to be exploited for political and personal gains. Unlike global best practices, PECA lacks independent oversight mechanisms, which has led to concerns about selective enforcement and political misuse.

Erosion of Public Trust in Digital Regulation: Due to the frequent misuse of PECA, public confidence in digital governance frameworks has declined. Citizens and advocacy groups have called for legal reforms to refine the law's scope, ensuring it targets genuine cybercrimes rather than serving as a tool for suppression.

3. Evidence of Misuse for Political Purposes

Case studies reveal that PECA has frequently been misused to suppress dissent and stifle criticism of government policies. For example, journalists reporting on corruption or governance failures have faced legal action under PECA's provisions. This misuse not only violates constitutional guarantees of freedom of expression but also undermines public confidence in the law's impartiality.

Content analysis of enforcement practices reveals a pattern of selective targeting, in which opposition voices are more likely to face legal repercussions than government allies. This selective application amplifies the public perception of PECA as a political tool rather than a valid regulatory framework. Such practices, therefore, erode the credibility of both the law and the institutions tasked with its enforcement.

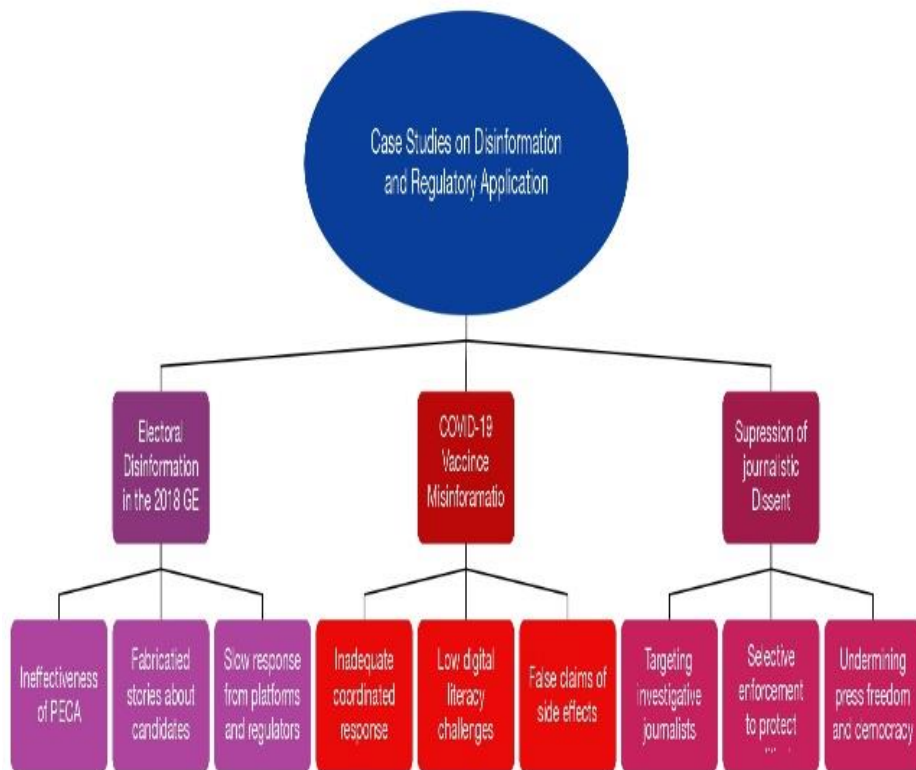


Fig 3. Case-based evidence: Political misuse of PECA to control disinformation

Case 1: Misinformation Regarding COVID-19 Vaccination

The COVID-19 pandemic has been a very fertile ground for health-related misinformation. Case analysis identified some vaccine side-effect claims that have been widely trending on social media platforms, including Facebook and WhatsApp. Low digital literacy and the general lack of public trust in state-led initiatives have meant that efforts to counter these narratives through public awareness campaigns have not helped the government contain their spread. PECA has been applied to a limited extent to remove harmful content; however, this spasmodic approach by platforms and the regulator has reflected broader shortcomings in enforcement.

Case 2: Electoral Disinformation in the 2018 General Elections

The disinformation in the 2018 elections involved both major political parties, hence undermining the credibility of the electoral process. Meanwhile,

social media had been dominated by fabricated stories accusing candidates of corruption and moral misconduct, shaping public perception. Case analysis indicates that although some content was flagged or removed, much remained accessible because both platforms and regulatory bodies acted very slowly. PECA was rarely enforced in these instances, raising questions about its effectiveness in managing politically sensitive disinformation. ([Baloch & Yousafzai, 2019](#))

Case 3: Suppression of Journalistic Dissent

Several high-profile cases have been documented that highlight how PECA has been applied to put people behind bars for raising voices in discord in the journalism arena. Consider, for example, that under the statutes of PECA, groups of investigative reporters exposing alleged government corruption have been charged, among others, with disseminating "fake news." An analysis of selected content in these cases demonstrates that legislation has been applied one-sidedly solely to serve political interests; it fails to address clear-cut instances of misinformation. Such misuse undermines the press's role as a pillar of democracy and reinforces fears of authoritarianism.

E. DISCUSSION

The findings reflect the tension between curbing disinformation and safeguarding freedom of expression in Pakistan. While the Prevention of Electronic Crimes Act is a milestone in regulating undesirable online content, its imprecise provisions and overly expansive enforcement mechanisms fail to meet the requirements of legality, necessity, and proportionality under international human rights norms as enshrined in the ICCPR. For instance, terms like "false information" are ill-defined and apt to be used to suppress political speech rather than actually fight disinformation, as highlighted by Khan and Tehrani ([2019](#)). Terms such as "false information" remain undefined, leading to concerns about selective application and the suppression of dissent. ([Khan & Tehrani, 2019](#)) This tension between regulation and rights reflects a broader global challenge. The European Union's Digital Services Act (DSA), for instance, provides a regulatory model that emphasizes transparency, accountability, and proportionality. By mandating platforms to disclose their content moderation policies and ensuring user rights, the DSA strikes a balance between combating harmful content and safeguarding freedom of expression. ([Kaushal et al., 2024](#)); ([Husovec, 2024](#))

To enhance PECA's efficacy while aligning with international standards, reforms should include narrowing its scope, clarifying definitions, and

incorporating procedural safeguards. Such measures would prevent misuse while addressing genuine online harms ([Iqbal, 2023](#)). Additionally, Pakistan can draw lessons from the EU's approach to regulating digital ecosystems to ensure that both disinformation and freedom of expression are addressed equitably. This comparative analysis underscores the necessity for a balanced regulatory framework that mitigates online harm without encroaching upon fundamental rights.

These findings point to the tension between fighting disinformation and protecting freedom of expression in Pakistan. Whereas the Prevention of Electronic Crimes Act, or PECA, was a milestone in regulating harmful online content, its vaguely worded provisions and broadly exercised enforcement mechanisms depart from the principles of legality, necessity, and proportionality set out in international human rights standards under the ICCPR. For instance, words like "false information" are so ill-defined that they can easily turn into a pretext for suppressing political speech rather than combating disinformation.

Application of PECA against those speaking out against the government underscores the need to strike a balance between regulating disinformation and protecting civic space. The current practice tends to undermine public confidence in the frameworks used outside democratic processes. Refinement of the legal frameworks so that the flow of disinformation is stemmed while legitimate dissent is not repressed involves:

1. Institutionalized and Strengthened-Procedural Safeguards: Provide for mechanisms such as judicial review and so on, along with the establishment of other independent oversight forms to oversee the application of PECA.
2. Greater Accountability: Greater transparency into takedown and prosecution decisions about content, to make it harder for political interests to cloud judgment.
3. Aligning with International Standards: Ensuring that regulatory measures meet international benchmarks, such as those outlined in the Rabat Plan of Action, to avoid infringing on fundamental freedoms.

PECA must be revised to align with international standards by: The use of ambiguous terms was narrowed, for example, "false information; Incorporating judicial safeguards for non-arbitrary enforcement; and establishing independent oversight bodies that would monitor the regulatory practices, especially misuse.

The study underscores the importance of public education as a key tool in the fight against misinformation. Recommendations include: Initiating national campaigns on digital literacy to evaluate online content critically; Engaging

education stakeholders to integrate media literacy into the curriculum; Utilizing social media platforms to disseminate fact-based information to counter disinformation narratives.

The regulatory measures will need to be developed in collaboration with the government, civil society, and technology platforms to ensure they are genuinely effective and inclusive. Some of the recommendations that stand out are: establishing advisory committees representative of all stakeholder groups to review and refine disinformation policies; encouraging technology platforms to localize their moderation policies to address Pakistan-specific issues; and promoting public-private partnerships to fund and implement digital literacy programs.

E. CONCLUSION

This research identifies the multidimensional set of challenges related to the spread of disinformation in Pakistan. It erodes public trust, increases political polarization, and contributes to democratic disengagement. The challenges imposed are such that even the legislation on the anvil, PECA, enacted to meet them, has overly broad provisions, ill-defined definitions, and the potential for misapplication, all of which undermine its credibility and effectiveness.

International comparative research will show, for example, that something like the EU's Digital Service Act should compel better-balanced measures in its design, including transparency and accountability, as well as stakeholder consultations at different levels. These observations demonstrate that an urgent course of legal reforms is well elaborated in an act that defines the ambit of PECA, thereby strengthening the procedural protective guarantees and aligning its provisions with international human rights standards. Of relevance: digital literacy, multi-stakeholder partnerships to protect freedom of expression while helping diminish the spread of disinformation.

This means that future research is needed to assess quantitatively public perceptions of disinformation and regulatory frameworks, to understand society's response better, and to identify where policy implementation falls short. It would also be important to measure changes in public trust levels and engagement as regulatory measures change, using surveys and longitudinal studies. Further, how the programs for digital literacy fare in both rural and urban areas would provide additional insight into scalability and effectiveness. Further research into the role and responsibilities of technology platforms in content moderation and their interaction with governments may also yield ways

to refine strategies to address disinformation. Building on this research, broader and more profound work will be used to develop more effective, inclusive, and rights-respecting approaches to digital governance in Pakistan and beyond.

REFERENCES:

- Alibašić, H. (2024). The Post-Factual Polity: Ethical, Governance, Administrative, and Policy Crises in the Disinformation Era. IAP.
- AZAM, M. (2021). Pakistan's International Law Obligations and Curtailment of Freedom of Expression: Balancing Legitimate Competing Interests or a Case of Violation?. *PLR*, 12, 37.
- Butt, M. N., Riaz, M., & Rabbani, A. W. (2023). Countering Fake News in Pakistan: Challenges Faced by Newsrooms and Regulators. *MAIRAJ*, 2(2), 79–87.
- George, A. S. (2024). Weaponizing WhatsApp: Organized Propaganda and the Erosion of Democratic Discourse in India. *Partners Universal Multidisciplinary Research Journal*, 1(1), 22–36.
- Helm, R. K., & Nasu, H. (2021). Regulatory responses to 'fake news' and freedom of expression: Normative and empirical evaluation. *Human Rights Law Review*, 21(2), 302–328.
- Howie, E. (2018). Protecting the human right to freedom of expression in international law. *International journal of speech-language pathology*, 20(1), 12-15.
- Inobemhe, K., & Asemah, E. S. Media Literacy and Critical Thinking as Tools for Combating Disinformation. *COMMUNICATION AND MEDIA DYNAMICS*, 11.
- Iqbal, M., Talpur, S. R., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan. *Siazga Research Journal*, 2(4), 273–282.
- Jia, C., Lee, A. Y., Moore, R. C., Decatur, C. H. S., Liu, S. X., & Hancock, J. T. (2024). Collaboration, crowdsourcing, and misinformation. *PNAS nexus*, 3(10), page: 434.
- Kaushal, R., Van De Kerkhof, J., Goanta, C., Spanakis, G., & Iamnitchi, A. (2024, June). Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1121–1132).

- Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. *Journal of Management Info*, 6(2), 7–11.
- Klein, A., & Klein, A. (2017). Hate speech in the information age. *Fanaticism, racism, and rage online: Corrupting the digital sphere*, 25–39.
- Kusaka, W. (2022). Fake News and State Violence: How Duterte Hijacked the Election and Democracy in the Philippines. In *Fake News and Elections in Southeast Asia* (pp. 145–165). Routledge.
- Mansoor, S. I. U. (2024). Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft. *Central University of Kashmir Law Review*, 4, 65–92.
- Mckay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political research quarterly*, 74(3), 703–717.
- Ness, S. (2024). The Balance Between Gatekeeper Rules and Free Speech in the EU under the Digital Markets Act and Digital Services Act. *Journal of Modern Law and Policy*, 4(3).
- Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, 1–29.
- Saleem, H., Jan, J., & Areej, A. (2022). Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges. *Society, Law and Policy Review*, 1(1), 10–22.
- Shankar, R., & Ahmad, T. (2021). Information Technology Laws: Mapping the Evolution and Impact of Social Media Regulation in India. *DESIDOC Journal of Library & Information Technology*, 41(4).
- Shou, Y., Kuru, O., Newman, E., & Smithson, M. (2024). Mis-and Disinformation. In *Oxford Research Encyclopedia of Natural Hazard Science*.
- Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/Politics*, 25(3), 517–537.
- Vese, D. (2022). Governing fake news: the regulation of social media and the right to freedom of expression in the era of emergency. *European Journal of Risk Regulation*, 13(3), 477–513.