International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Regulating the Fake News on Social Media Platforms: Analyzing the Impact of Indian Legal System and Legal System of Other Countries

Surya Sk[1], Ts Pavan[2]

[1,2]Law Student, Sastra Deemed University

ABSTRACT

Nowadays, there has been an increased use of social media platforms globally. Social media networks have become integral to modern communication, offering platforms where users can connect, share information, and engage with diverse content. Social media platforms have a greater reach, and a variety of people are utilizing these platforms. While social media has revolutionized information sharing and community building, it also presents challenges, particularly the spread of fake news.

The spread of fake news through social media networks involves the rapid and wide dissemination of false and misleading information. This raises the question of how to detect fake news and whether it should be curbed. If fake news is not curbed, what will be the impact?If it is curbed, how does this action contradict fundamental rights?

Social media networks act as intermediary platforms that host user-generated content. These intermediaries play a major role in sharing information, including fake news, on their platforms. However, the increasing impact of fake news has intensified scrutiny over whetherthese platforms should be more accountable and liable for the content they facilitate. This scrutiny ultimately raises the issue of intermediary liability for the spread of fake news throughtheir platforms. The obligation of intermediaries in managing and curbing misinformation involves several critical responsibilities.

This paper evaluates the technical aspects of these applications, obligations, fixation of liability, regulations, and implementation challenges, and provides a comparative analysis of intermediary liability under the Information Technology (Intermediary Guidelines and DigitalMedia Ethics Code) Rules 2021 and legal system of other countries.

KEYWORDS: Fake News, Dissemination of Fake News, Liabilities of Intermediaries, IT Act2000, IT Rules 2021.

BACKGROUND

The rise of social media has transformed communication, enabling widespread information sharing but also facilitating the rapid spread of fake news. This has had severe consequences for public trust, democratic processes, and societal stability, leading to an increased focus on intermediary liability—holding digital platforms accountable for the content shared on their networks. The background of this issue is explored through the lens of India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2023 (IT Rules 2023) and the legal systems of other countries.

Historically, fake news became a global concern, notably during events such as the 2016 U.S.presidential election, where disinformation significantly impacted political discourse. Prior to recent regulatory frameworks, many countries lacked sufficient legal tools to manage the responsibility of intermediaries in combating misinformation. Section 79 of India's Information Technology Act (2000) provided some protection for intermediaries but was largely insufficient in addressing the challenges of modern digital communication.

In response, the IT Rules 2023 and the legal systems of other countries introduced stricter obligations for intermediaries, including proactive content moderation and transparency in how harmful content is managed. These regulations aim to reduce the spread of fake news while balancing user rights, such as privacy and freedom of expression. However, concerns about censorship, privacy invasion, and governmental overreach persist.

Future challenges will likely involve refining automated moderation technologies like AI, which still struggle with accuracy and bias. Additionally, global cooperation is needed to harmonize regulations, as the internet's borderless nature complicates enforcement. Continued innovation and international collaboration are essential to further strengthen the regulation of fake news while ensuring the protection of democratic institutions and societal trust.

LITERATURE REVIEW

Literature Review 1 – "Fake news, disinformation, and misinformation in social media"[1]

The literature review in the paper 'Fake news, disinformation, and misinformation in social media' addresses the significant challenges posed by fake news in online social networks (OSNs). It highlights how social media facilitates the rapid spread of false information, makingdetection difficult due to the close resemblance of misleading content to the truth. While AI techniques are widely used for detection, they face limitations, as AI is also leveraged to createdeceptive content. The review draws on perspectives from social sciences, law, politics, and technology, examining definitions like misinformation, disinformation, and misinformation. Itunderscores the importance of social media literacy, credibility indicators, and behavioral interventions in helping users identify fake news. Although progress has been made, future research should focus on improving detection methods, understanding the dynamics of fake news propagation, and developing better AI training datasets. A multi-disciplinary approach isrecommended to address the evolving complexity of online deception.

Literature Review 2 – "Evolving Scope of Intermediary Liability in India"[2]

The literature review in the paper 'Evolving Scope of Intermediary Liability in India' analyzesthe legal evolution of intermediary liability, focusing on key regulations and court rulings. It highlights the Information Technology (IT) Act, 2000, particularly Section 79, which offers intermediaries protection from liability if conditions are met. The 2008-09 amendments and 2011 guidelines expanded responsibilities, while the 2021 Guidelines introduced stricter content moderation and the requirement to identify the "first originator," raising concerns overprivacy and encryption. The review underscores the need for clearer legal distinctions betweenpassive and active intermediaries, balancing privacy with regulatory demands. It suggests technology-driven solutions, like AI-based content moderation, as a way

[1] Aïmeur, E., Amri, S. & Brassard, G. Fake news, disinformation and misinformation in social media: a review. *Soc. Netw. Anal. Min.* **13**, 30 (2023). https://doi.org/10.1007/s13278-023-01028-5

[2] Indranath Gupta & Lakshmi Srinivasan (2023) Evolving scope of intermediary liability in India, International Review of Law, Computers & Technology, 37:3, 294-324, DOI: 10.1080/13600869.2022.2164838

for intermediaries tomeet their obligations without compromising safe harbor protections.

Literature Review 3 – "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code), 2021: A Critical Study"[3]

The literature review of 'Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code), 2021: A Critical Study' by Rupal Chhaya and Ahmar Afaq critically assesses the 2021 IT rules, focusing on intermediary liability, content regulation, and the tension between government oversight and fundamental rights. The authors note that these rules aim to regulate social media, digital platforms, and OTT content, responding to the rise of digital media during the pandemic. While the rules help control false information and offensive content, they raise concerns about censorship and infringing on free speech rights under Article 19 of the Indian Constitution. The study highlights issues with the broad responsibilities imposed on intermediaries and the vague nature of content restrictions, leadingto potential overreach and automated censorship risks. The authors recommend revisions to protect user rights and call for further study on the constitutional validity of the guidelines, suggesting expert consultations for future legal frameworks to ensure balanced regulation.

Literature Review 4 – Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency[4]

In *Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency*, Donato Vese explores the impact of stringent regulationsaimed at curbing fake news on social media, especially during the COVID-19 pandemic. The author highlights the tension between these regulations and the right to freedom of expression,cautioning that governments may misuse them for excessive censorship. Vese compares the EU's regulatory framework, which emphasizes self-regulation through initiatives like the European Commission's Code of Practice on Disinformation, with India's stricter laws under the Information Technology Act, which mandate rapid removal of fake news and the disclosureof information origins, raising privacy concerns. Vese argues that both regions face challengesin balancing disinformation control with free speech protection. The author advocates for user empowerment, media literacy, and reliability ratings on social media as more effective, less intrusive alternatives to heavy government control in future regulatory approaches.

RESEARCH PROBLEM

The spread of fake news on social media challenges public trust and democratic processes. India's IT Act, 2000 and 2021 IT Rules face issues like vague definitions and weak enforcement, allowing misinformation to thrive. Examining international models like Germany's NetzDG and Singapore's POFMA can help strengthen India's legal framework to better regulate and curb fake news.

RESEARCH QUESTION

1. What is Fake News? Why should Fake News be curbed?
2. What role does intermediary liability play in shaping their content moderation practices?
3. How effective is the Indian legal framework in addressing the dissemination offake news on social media platforms, and how does its approach compare to the legal systems of other countries in curbing

[3] R Chhaya, A Afaq (2021) Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code), 2021: A Critical Study

[4] Vese D. 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*. 2022;13(3):477-513. doi:10.1017/err.2021.48

misinformation online?
4. How Fake news influences the opinions of the general public?

RESEARCH OBJECTIVES

1. To analyze the current landscape of fake news and its impact on societal opinion and democratic processes.
2. To assess the effectiveness of the Indian legal framework in combating the dissemination of fake news on social media platforms.
3. To identify the gaps and limitations (lacunas) in the current Indian legal systemfor regulating fake news, including issues like ambiguous definitions, lack of clear liability for social media platforms, and inadequate enforcement mechanisms.
4. To compare India's legal approach with international best practices by examining legal frameworks from countries like Germany (NetzDG law), Singapore (Protection from Online Falsehoods and Manipulation Act – POFMA), and the European Union (Digital Services Act), to identify effective strategies that could be adapted for India.
5. To identify best practices and potential improvements for existing regulations to enhance the accountability of intermediaries in mitigating fake news.

RESEARCH HYPOTHESIS

The dissemination of fake news has a measurable negative impact on public trust in media and democratic institutions, shaping public opinion—especially on politically or emotionally charged issues—and hindering social cohesion and informed decision-making. Countries with legal frameworks that impose higher liability on intermediaries demonstrate more effective content moderation practices compared to the Indian legal system, which lacks specific regulations, robust enforcement mechanisms, and public awareness, limiting its success in mitigating misinformation online.

SCOPE AND LIMITATIONS

This paper focuses on the regulatory frameworks governing intermediary liability in India andthe legal system of other countries. It provides a comparative analysis of these legal approachesto address fake news, examining content moderation responsibilities and the protection of fundamental rights.

However, the study has several limitations. First, it is theoretical, relying on early-stage analysis, as both laws are relatively new with limited empirical data on their long-term effectiveness. Second, it does not include other influential frameworks, such as those in the Germany, France, etc., Third, while technological solutions like AI-driven moderation are mentioned, a detailed technical assessment is beyond this paper's scope. Despite these limitations, this study contributes to discussions on fake news regulation and intermediary liability.

RESEARCH METHODOLOGY

This study employs a primary research methodology, doctrinal research relying on an extensivereview of existing literature to explore research topic and questions. A systematic and comprehensive analysis of relevant studies, academic journals, books, and reputable online sources will be conducted to gather data. This survy uses a quantitative approach to assess theeffectiveness of India's legal system in addressing fake news on social media, based on a surveyconducted among law students and professors.

Sample Selection:

- Convenience sampling was applied to select 62 respondents (law students and law professors) from Indian legal institutions.

1. WHAT IS FAKE NEWS? WHY SHOULD FAKE NEWS BE CURBED?

1.1. Misleading Information: Misinformation, Disinformation and fake news:

1.1.1. Misinformation and Disinformation:

Misinformation, disinformation, and fake news are crucial concepts that require clarification. The Oxford English Dictionary (2020) defines misinformation as "wrongor misleading information," typically spread without malicious intent (Ireton & Posetti,2018). In contrast, disinformation is deliberately disseminated false information aimedat manipulating public opinion, often by governments or agents (Ireton & Posetti, 2018). Misinformation refers to false or inaccurate information that is mistakenly or inadvertently created or spread, without the intent to deceive. Disinformation, on the other hand, is "false information that is deliberately created and spread in order to influence public opinion or obscure the truth" (Merriam-Webster, n.d.)[5].

The European Commission (2018) and the U.S. State Department describe disinformation as intentional misinformation that poses threats to democratic processesand various business sectors (Nemr & Gangware, 2019). Disinformation can manifest through methods such as deceptive advertising and cyber operations (Fallis, 2009, 2015).

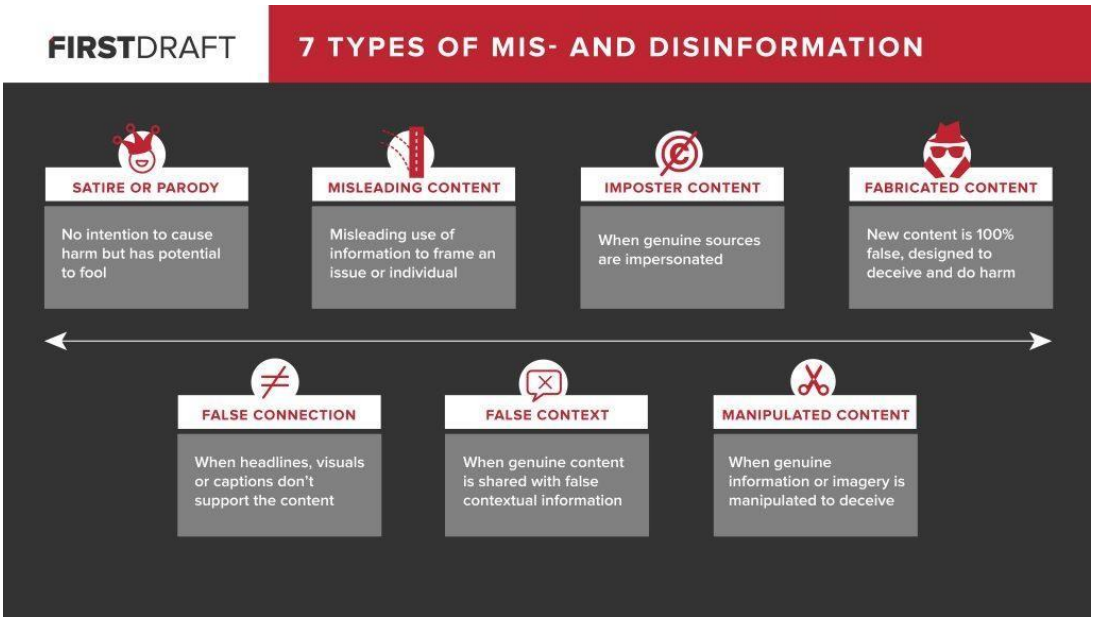


Fig. 1: seven distinct types of mis- and disinformation
Source: First Draft

A comprehensive breakdown of misinformation and disinformation is illustrated in Fig.1, outlining seven distinct types, including Satire or Parody, Misleading Content, Imposter Content, Fabricated Content, False Connection, False Context, and Manipulated Content. Understanding these categories is essential

[5] Reference: Merriam-Webster. (n.d.). Disinformation. In Merriam-Webster.com dictionary. Retrieved from https://www.merriam-webster.com/dictionary/disinformation

for addressing the broader issue of information disorder and its impact on public trust and discourse (First Draft, n.d.)[6].

1.1.2. What is Fake News?

The term "fake news" lacks a universally accepted definition, though it broadly refers to false, misleading, or fabricated information presented as news. The *Collins English
Dictionary (Cooke, 2017)[7] and Allcott & Gentzkow (2017)[8] define it as false news aimed at misleading readers. Nakov (2020)[9] notes the term's varied interpretations, including its use by politicians to label unfavorable coverage.

Scholars debate whether fake news should include satire, rumors, and conspiracy theories. Related terms such as disinformation (Kapantai et al., 2021)[10], misinformation(Wu et al., 2019), malinformation (Dame Adjin-Tettey, 2022)[11], and information disorder (Wardle & Derakhshan, 2017)[12] add complexity. Some see fake news as a formof misinformation (Allen et al., 2020)[13] or disinformation (Baptista & Gradim, 2022), while others view it as a blend of both (Wu et al., 2022).

Fake news gained global attention during the 2016 U.S. election (NATO, 2020)[14], andits impact intensified during the COVID-19 pandemic, with the WHO describing it as an "infodemic" of misinformation that threatened public health (WHO, 2020). Scholarslike Tandoc et al. (2018) categorize fake news into six types, such as satire, propaganda,and photo manipulation, some of which overlap with disinformation. This growing issue underscores the need for nuanced legal and regulatory responses to combat the rising cyberthreats linked to misinformation in global crises like COVID-19.

1.2. Why should Fake News be curbed?

1.2.1. Misleading information and cyber risks to business sectors

1.2.1.1. COVID-19, misleading information, and cyber risks to healthcare

The healthcare sector, deemed critical infrastructure (CISA, n.d.), has undergone significant digital transformation due to advancements in cloud computing and the Internet of Medical Things (Deloitte, 2020). However, this reliance on interconnected technologies has heightened cybersecurity challenges, leading to major concerns over the privacy and security of health information (Agarwal et al., 2010; Haggerty, 2017).Cyber threats, including data theft and ransomware attacks, have surged, with healthcare experiencing the highest average breach cost at $7.13 million (IBM, 2020).High-profile attacks and vaccine-related threats during the COVID-19 pandemic
further underscore the sector's vulnerability to state-sponsored disinformation and cyber campaigns

[6] Reference: First Draft. (n.d.). 7 types of mis- and disinformation. Retrieved from firstdraftnews.org.
[7] https:// www. colli nsdic tiona ry. com/ dicti onary/ engli sh/ fake- news,
[8] Allcott H, Gentzkow M (2017) Social media and fake news in the 2016 election. J Econ Perspect 31(2):211– 36. https:// doi. org/ 10. 1257/jep. 31.2. 211
[9] Nakov P (2020) Can we spot the “fake news” before it was even written?arXiv preprint arXiv: 2008. 04374 Nekmat E (2020) Nudge effect of fact-check
[10] Kapantai E, Christopoulou A, Berberidis C, Peristeras V (2021) Asystematic literature review on disinformation: toward a unified taxonomical framework. New Media Soc 23(5):1301–1326. https://doi.org/10.1177/1461444820959296
[11] Dame Adjin-Tettey T (2022) Combating fake news, disinformation, and misinformation: experimental evidence for media literacy education. Cogent Arts Human 9(1):2037229.https://doi.org/10.1080/23311983.2022.2037229
[12] Wardle C, Derakhshan H (2017) Information disorder: toward an interdisciplinary framework for research and policy making. Council Eur Rep 27:1–107
[13] Allen J, Howland B, Mobius M, Rothschild D, Watts DJ (2020) Evaluating the fake news problem at the scale of the information ecosystem. Sci Adv. https://doi.org/10.1126/sciadv.aay3539
[14] https://www.nato.int/cps/en/natohq/177273.htm, last access date: 26-12-2022.

(Cimpanu, 2020; Stubbs, 2020).

2. Media, digital transformation, and misleading information

The media industry has undergone significant transformations due to technological advances, notably marked by the rise of "yellow" journalism in the late 19th century, which popularized sensationalism and fake news (Martens et al., 2018; Oxford English Dictionary, 2020). Figures like Joseph Pulitzer and William Hearst exemplified this shift, impacting public opinion during events like the Spanish-American War (Daly, 2018; CITS, 2021). The digital age has further transformed the industry into multisidedonline platforms, with social media amplifying the spread of misinformation, especiallyduring the 2016 U.S. presidential election (Allcott & Gentzkow, 2017). While online platforms are central to disinformation, mainstream media also plays a significant role(Tsfati et al., 2020). Motivations for spreading fake news range from political manipulation to financial gain (Kshetri & Voas, 2017).

3. Misleading information and financial markets

The term "fake news" originated in the *Milwaukee Daily Journal*, where it related tothe mining industry, highlighting its impact on investors and stock prices (Zhang & Ghorbani, 2020). Fake news in financial markets can increase trading activity by over 50% and price volatility by 40% (Kogan et al., 2020), with negative effects on stock market returns during the COVID-19 pandemic (Cepoi, 2020). Cyberattacks targeting financial markets have surged, exacerbated by remote work (Krohn, 2020). Additionally, election-related news significantly influences market volatility (Wisniewski, 2015), with fake news potentially affecting the 2016 U.S. presidential election and its financial consequences (Allcott & Gentzkow, 2017).

4. Elections, disinformation, and geopolitical risks

During the 2016 U.S. presidential election, state actors employed social media disinformation campaigns to divide the electorate and undermine confidence in democratic institutions (NASEM, 2018). These efforts included spear phishing attacks

targeting government officials and voting infrastructure, as identified in the Mueller Report (2019). In response, the U.S. enacted geopolitical actions, such as expelling Russian intelligence operatives and imposing sanctions (Sanger, 2016). Advanced Persistent Threats (APTs), particularly from Chinese cyber espionage units, have beenused to steal intellectual property from numerous organizations (Ghafir & Prenosil, 2014). These cyber threats significantly impact geopolitics and trade, as highlighted inU.S.-China negotiations (Mitchell & Politi, 2019).

1.2.2. What do you think is the most significant consequence if fake news is notcontrolled?

- Erosion of public trust in media and institutions
- Increased political polarization and extremism
- Misinformed public leading to poor decision-making
- Social unrest and violence
- Economic damage to businesses and markets

2. WHAT ROLE DOES INTERMEDIARY LIABILITY PLAY IN SHAPING THEIRCONTENT MODERATION PRACTICES?

Intermediaries are vital in disseminating news, traditionally filled by journalists and editors who curate and verify stories, thus shaping public perception and discourse. Therise of digital platforms has expanded this role to include social media algorithms and influencers, leading to personalized news consumption that can create echo chambers.Intermediaries amplify news through rapid sharing and framing, influencing

public opinion by emphasizing specific narratives. They also facilitate public discourse, bridging local and global news gaps and combating misinformation through fact- checking efforts. Ultimately, intermediaries play an essential role in shaping, filtering,and spreading news in society.

Role of Intermediaries in spreading fake news:

Intermediaries significantly contribute to the spread of fake news, particularly in the digital age. Social media platforms and their algorithms prioritize engaging content, often amplifying sensational, misleading stories that attract attention. Influencers and bloggers, lacking verification resources, may unintentionally share false information, further spreading it among their followers. Traditional news outlets also contribute by publishing unverified content due to pressure for timely reporting. Echo chambers andfilter bubbles reinforce misinformation by exposing users to like-minded views. Malicious actors exploit these intermediaries, making it challenging to control the dissemination of fake news in today's media landscape.

Role of intermediaries in curbing fake news

Intermediaries play a vital role in combating fake news through detection methods, fact-checking, and promoting media literacy. They utilize fact-checking organizations like FactCheck.org and PolitiFact to verify information accuracy and develop algorithms toflag misleading content based on engagement patterns. User reporting mechanisms allow individuals to alert platforms about false content, which is then reviewed by moderators. Collaborative initiatives like the Trusted News Initiative (TNI) facilitate rapid responses to misinformation during critical events. Additionally, intermediaries educate the public on assessing sources and identifying manipulated content, empowering users to become discerning consumers of information in today's media landscape.

3. HOW EFFECTIVE IS THE INDIAN LEGAL FRAMEWORK IN ADDRESSING THE DISSEMINATION OF FAKE NEWS ON SOCIAL MEDIA PLATFORMS, AND HOW DOES ITS APPROACH COMPARE TO THE LEGAL SYSTEMS OF OTHER COUNTRIES IN CURBING MISINFORMATION ONLINE?

3.1 Regulation of Fake News Dissemination Through Social Media in the Indian LegalSystem

3.1.1 Information Technology Act, 2000 (IT Act)[15]

a. Section 69A of the IT Act[16]

The blocking powers under Section 69A are implemented by the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. This provision has been frequently invoked to block websites, URLs, and social media accounts disseminating fake news, especially in situations where the spread of misinformationthreatens national security or public peace. In this landmark case, *Shreya Singhal v. Union of India (2015)*[17] the Supreme Court of India upheld the constitutionality of Section 69A whilestriking down Section 66A of the IT Act[18] (which criminalized offensive online messages) for being vague and violative of Article 19(1)(a)[19] (Freedom of Speech). The Court found that Section 69A was a narrowly tailored provision with proper procedural safeguards, such as requiring reasons for blocking to be recorded in writing and orders issued by a competent authority. This case is pivotal in upholding the government's ability to block online content, including fake news.

[15] Information Technology Act, 2000, Act No. 21 of 2000, India Code (2000)
[16] Act No. 21 of 2000, India Code (2000).
[17] (2015) 5 SCC 1.
[18] Act No. 21 of 2000, India Code (2000).
[19] India Const. art. 19(1)(a).

b. Section 79 of the IT Act: Intermediary Liability and Safe Harbor Protection[20]

Section 79 of the IT Act, 2000, provides safe harbor protection to intermediaries, meaning they are not held liable for the third-party content posted on their platforms as long as they actas neutral intermediaries and follow the due diligence requirements. This protection issignificant in the context of fake news because it determines the extent to which platforms likeFacebook, Twitter, and WhatsApp can be held accountable for the spread of misinformation.However intermediary can be held legally liable for any unlawful or harmful content (including fake news) posted on its platform, making them subject to civil and criminal liability. Section 79 states that an intermediary is not liable for any third-party information, data, or communication hosted on its platform, provided:

- The intermediary's role is limited to providing access to a communicationsystem.
- The intermediary does not initiate, select, or modify the transmission of theinformation in question.
- The intermediary observes due diligence and complies with governmentnotifications or directions concerning illegal or harmful content.

The intermediary loses this protection if it fails to act on content that is illegal, harmful, or misleading after receiving actual knowledge or a government directive to remove or disable access to such content.

Several judicial decisions have clarified the application of Section 79 in regulating intermediaries' roles, particularly concerning fake news and harmful content on social media platforms: *MySpace Inc. v. Super Cassettes Industries Ltd (2017)*[21] this case involved allegations of copyright infringement on the MySpace platform. Though not directly related tofake news, the case helped clarify intermediary liability under Section 79. The Delhi High Court ruled that intermediaries could claim safe harbor under Section 79 only if they comply with the obligations set out in the IT Act and the Intermediary Guidelines. In this case, MySpace was required to take down infringing content upon notice. While primarily focused on copyright issues, the ruling reinforced that intermediaries could be held liable if they fail toremove harmful content after receiving notice. This principle applies to fake news as well: platforms must act when alerted to misinformation, or they risk losing their safe harbor protection. *Google India Pvt. Ltd. v. Visaka Industries (2020)*[22] this case centered on defamation claims against Google, holding the company responsible for hosting defamatory content. Google claimed safe harbor protection under Section 79. The Telangana High Courtruled that Google could not be held liable because it was merely an intermediary and had no control over the content posted by third parties. The court reiterated that intermediaries enjoy protection under Section 79, provided they act upon receiving knowledge of illegal content. This case highlights that platforms are not held liable for hosting false or defamatory content unless they fail to act on a legitimate notice. In the context of fake news, platforms are requiredto take action only after being notified, not proactively.

3.1.2 The Information Technology (Intermediary Guidelines and Digital Media EthicsCode) Rules, 2021[23]

1. Due Diligence by Intermediaries (Rule 3)[24]

- Prohibited Content: Intermediaries must inform users that hosting or sharing patently false or misleading content is prohibited (Rule 3(b)(v)). The Bombay High Court struck down the

[20] Information Technology Act, 2000, § 79, Act No. 21 of 2000, India Code (2000).
[21] MySpace Inc. v. Super Cassettes Indus. Ltd., 236 (2017) Delhi High Court
[22] Google India Pvt. Ltd. v. Visaka Indus. Ltd., (2020) 4 SCC 162.
[23] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[24] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).

establishment of the Fact Check Unit (FCU) as unconstitutional, citing vagueness in terms like "fake" and "misleading," overreach, and potential censorship.

- Takedown Mechanism: Platforms must remove unlawful content, including fake news, within 36 hours of receiving an order (Rule 3(d)).
- User Agreements: Platforms must notify users of prohibited activities, including disseminating false information (Rule 3(b)).
- Accountability: Platforms must terminate access for users violating platform rules and remove non-compliant content (Rule 3(c)).

2. Traceability of the First Originator (Rule 4(2))[25]

Significant intermediaries must enable the identification of the first originator of content, particularly if it threatens national security, public order, or incites violence, ensuring traceability without compromising message privacy.

3. Grievance Redressal Mechanism (Rule 3(2))[26]

- Platforms must appoint a Grievance Officer to handle complaints related to harmful or false content (Rule 3(2)(a)).
- Complaints must be resolved within 15 days, with urgent cases handled within 72 hours (Rule 3(2)(b)).

4. Additional Due Diligence for Significant Social Media Intermediaries (Rule 4)[27]

- Appointment of a Chief Compliance Officer to ensure compliance.
- Platforms must publish monthly compliance reports, outlining actions on complaints, including removal of fake news (Rule 4(d)).
- Platforms must use automated tools to identify and flag harmful content proactively (Rule 4(4)).

5. Blocking of Information in Emergency Cases (Rule 16)[28]

The government can direct intermediaries to block content threatening public order or national security without prior notice. Orders are issued by an Authorized Officer under MeitY.

6. Penalty for Non-Compliance (Rule 7)[29]

Non-compliance risks loss of safe harbor protection under Section 79 of the IT Act, exposing platforms to liability for user-generated content.

7. Grievance Appellate Committees (Rule 3A)[30]

Users dissatisfied with Grievance Officer decisions may appeal to government-established Grievance Appellate Committees.

8. Proactive Content Moderation and Reporting

Platforms must use automated tools to proactively block content that violates laws, especially during public interest events like elections (Rule 4(4)).

9. News Publishers and Aggregators (Rule 18)[31]

News platforms must register details with the Ministry of Information and Broadcasting and can receive verification marks.

[25] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[26] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[27] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[28] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[29] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).
[30] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3A, Gazette of India, pt. II sec. 3(i) (Oct. 28, 2022)
[31] Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021).

Facebook v. Union of India (2020)[32]**,** In this case, the Supreme Court examined the issue of whether intermediaries, such as social media platforms, can be held liable for the disseminationof unlawful content, including fake news. The Court emphasized the importance of striking a balance between privacy rights and accountability in content dissemination. It directed platforms like WhatsApp to enable traceability of the originator of harmful content while upholding privacy through encryption.

3.1.3 Indian Penal Code (IPC), 1860[33]

Several provisions of the Indian Penal Code (IPC) can be invoked to regulate the spread of fake news, particularly in cases where the content may incite violence, harm public order, or defame individuals.

a. Section 153A: Promoting Enmity Between Different Groups

- Section 153A criminalizes acts that promote enmity between different groupsbased on religion, race, or language and are likely to disturb public harmony. This section can be used to penalize those who create or disseminate fake news that incites communal violence or unrest.

b. Section 505: Statements Conducing to Public Mischief

- Section 505 deals with the dissemination of false statements or rumors that are likely to cause fear or alarm to the public or incite offenses against the state or publictranquility. This provision is critical in curbing fake news that causes panic, such as during public health crises (e.g., COVID-19) or elections. In the case of *Prashant Kanojia v. State of Uttar Pradesh (2019)*[34], the Supreme Court intervened after a journalist was arrested under Section 505 of the IPC for allegedly spreading fake newson social media. While the Court emphasized that individuals should not be unnecessarily detained for social media posts, it also recognized the state's power to regulate content that could disturb public peace. The judgment highlights the need for proportionality in handling fake news cases, emphasizing that the regulation of speechmust not infringe upon fundamental rights.

c. Section 499 and 500: Defamation

- Sections 499 and 500 deal with criminal defamation, where individuals can be prosecuted for spreading false and damaging information about another person. Fakenews that harms an individual's reputation can fall under these sections, and both criminal and civil defamation suits can be filed against the perpetrators. In the case of *Subramanian Swamy v. Union of India (2016)*[35], the Supreme Court upheld the constitutionality of the criminal defamation provisions under Sections 499 and 500. The Court reasoned that the right to free speech does not include the right to harm another's reputation through false information, providing legal grounds to prosecute fake newsthat defames individuals.

3.1.3 Disaster Management Act, 2005 and Epidemic Diseases Act, 1897[36]

During situations like the COVID-19 pandemic, fake news related to health information can have dire consequences. The Disaster Management Act, 2005, and the Epidemic Diseases Act, 1897, were invoked to tackle fake news during the pandemic.

a. Section 54 of the Disaster Management Act, 2005

- This section penalizes individuals who spread false alarms or misleading information that may cause

[32] (2020) SCC OnLine SC 757
[33] Indian Penal Code, 1860, Act No. 45 of 1860, India Code (1860).
[34] (2019) 7 SCC 1.
[35] (2016) 7 SCC 221.
[36] Disaster Management Act, 2005, Act No. 53 of 2005, India Code (2005);Epidemic Diseases Act, 1897, Act No. 3 of 1897, India Code (1897).

panic during a disaster. Authorities used this provision tocrack down on fake news related to COVID-19, including false cures, misleading dataon the virus's spread, and rumors about lockdowns.

b. Epidemic Diseases Act, 1897

- This act empowers the government to take special measures during epidemics,and it was used during COVID-19 to issue advisories warning the public against spreading false health information on social media platforms.

3.1.5 Election Laws

During election periods, the Election Commission of India (ECI) plays a pivotal role in preventing the spread of fake news that could influence voter behavior. The Representation of the People Act, 1951 contains provisions that deal with false statements in connection withelections.

a. Representation of the People Act, 1951[37]

- Sections of the Act prohibit the dissemination of false statements regarding candidates or political parties that could influence voters' decisions. The ECI, in collaboration with social media platforms, has developed mechanisms to monitor and remove political fake news during election periods.

3.2 LEGAL ISSUES AND LACUNAS IN THE INDIAN LEGAL SYSTEM FOR CURBING FAKE NEWS

India's current legal framework for regulating fake news, particularly on social media, has several gaps and challenges that limit its effectiveness. These lacunas revolve around the lack of clarity, vague definitions, inconsistent enforcement, and potential overreach by authorities, which create difficulties in effectively addressing the problem. Below are some ofthe key legal issues and how they can be addressed:

3.2.1 Lack of a Clear Definition of Fake News

There is no legal definition of fake news in Indian laws like the Information Technology Act, 2000 or the Indian Penal Code (IPC). The absence of a clear definition creates ambiguityin enforcement and makes it difficult to differentiate between legitimate content, satire, opinion, and deliberate misinformation. The Bombay High Court struck down the provision inthe 2021 IT Rules that established a Fact Check Unit, citing that terms like "fake," "false," and"misleading" were too vague and broad. The court held that such vague definitions could leadto arbitrary enforcement and excessive censorship.

Recommendation:

- **Introduce a Clear, Legal Definition**: Amend the IT Act or create newlegislation to provide a precise definition of fake news, focusing on misinformation that is deliberately false and intended to mislead or cause harm. This definition shoulddistinguish between innocuous falsehoods, satirical content, and malicious fake news that threatens public order or personal rights.
- **Context-Based Classifications**: Define different categories of fake news, such as:
  - Public Harm: Fake news that can incite violence, disturb public order,or affect public health (e.g., COVID-19 misinformation).
  - Political Disinformation: Fake news aimed at influencing elections orspreading false information about candidates.
  - Defamation: False news aimed at harming an individual or entity'sreputation.

3.2.2 Weak or Inconsistent Enforcement

The enforcement of laws targeting fake news, such as the IT Rules, 2021, has been inconsistent. There are

[37] Representation of the People Act, 1951, Act No. 43 of 1951, India Code (1951).

also concerns over delays in the judicial process and arbitrary takedowns, where content is removed without due process or adequate review, leading to over-censorship.

Recommendation:

- **Strengthen Enforcement Mechanisms**: Create a specialized body, like a **Digital Media Regulatory Authority (DMRA)**, to oversee enforcement of fake newsregulations. This authority should monitor social media platforms, handle complaints, and ensure compliance in a uniform and transparent manner.
- **Faster Grievance Redressal**: Ensure that the grievance redressal system in the 2021 IT Rules is streamlined, with clear timelines for responding to fake news complaints and a faster judicial process to review content takedown requests.
- **Introduce Penalties for Platforms**: Platforms that do not remove fake news promptly after being notified should face strict financial penalties, similar to the NetzDG law in Germany, where fines are imposed for non-compliance. These penalties should be proportional to the platform's global turnover to ensure compliance.

3.2.3 Lack of Accountability for Social Media Platforms

Under Section 79 of the IT Act, social media platforms enjoy safe harbor protections as intermediaries, meaning they are not held liable for user-generated content as long as they actswiftly to remove illegal content when notified. However, this provision often results in passivemoderation, where platforms delay action against fake news until it becomes a major issue.

Recommendation:

- **Modify Safe Harbor Provisions**: Amend Section 79 of the IT Act to impose stricter obligations on social media platforms. These should include:
- **Proactive Monitoring**: Require platforms to use AI-based systems todetect and flag fake news in real-time, preventing it from going viral.
- **Mandatory Fact-Checking**: Require platforms to partner with independent fact-checkers and make real-time corrections to false information. They should also be required to flag or label misinformation before it spreads widely.
- **Establish a Duty of Care for Platforms**: Introduce a "duty of care" standard,similar to the UK's Online Safety Bill, where platforms are required to take reasonable steps to prevent the dissemination of harmful content, including fake news.

3.2.4 Create a Specialized Regulatory Body

Establish a dedicated regulatory body to oversee the implementation of fake news laws and content moderation practices on social media platforms. This body could function similarly toGermany's Federal Office of Justice (which oversees NetzDG compliance) and ensureuniform enforcement of regulations.

Recommendation:

- **Digital Media Regulatory Authority (DMRA)**: Create a Digital Media Regulatory Authority responsible for overseeing the spread of fake news and ensuringcompliance with Indian laws. The DMRA could issue notices, correction orders, and take-down requests and also act as a dispute resolution body for complaints raised by users or platforms.
- **Independent Appellate Mechanism**: Establish an independent appellate bodywhere individuals or platforms can appeal against takedown or correction orders. This ensures due process and prevents abuse of powers by authorities.

3.2.5 Introduce Stiffer Penalties for Non-Compliance

India can draw inspiration from Germany's NetzDG and Australia's Criminal Code Amendment to introduce heavy penalties for non-compliance with fake news regulations.

Recommendation:

- **Fines Based on Global Revenue**: Introduce fines for social media companies that fail to remove fake news within a stipulated period. Penalties could be up to 10%of global turnover for serious or repeat offenses, as in Australia.
- **Individual Liability**: Hold individuals or influencers who deliberately spread fake news, especially with malicious intent, accountable under criminal provisions. For instance, under Section 505 of the IPC, individuals could face imprisonment or heavy fines if their misinformation causes public panic, violence, or loss of life.

3.2.6 Potential for Government Overreach and Censorship

The IT Rules, 2021 give the government powers to order the removal of content without judicial approval. This creates concerns about government overreach and the risk of arbitrary censorship, as vague terms such as "defamatory" or "obscene" could be misused tosuppress dissent or criticism.

Recommendation:

- **Judicial Review of Takedown Orders**: Introduce provisions for judicialoversight of government-issued content takedown orders. A system similar to France's Law Against the Manipulation of Information could be adopted, where judicial review ensures that only genuinely harmful content is removed and free speechis protected.
- **Independent Appeals Mechanism**: Create an independent appeals body where individuals or organizations can challenge content takedown orders. This ensuresfairness and due process, reducing the likelihood of arbitrary censorship.

3.2.7 Absence of Real-Time Prevention Mechanisms

Current laws focus on **reactive** measures, such as removal after notification, rather than proactive prevention. Once fake news goes viral, the damage is often already done, and removing the content afterward may have limited effect in curbing its impact.

Recommendation:

- **AI-Based Real-Time Detection**: Mandate social media platforms to implementAI-powered algorithms for real-time detection of fake news. These systems should be able to identify patterns of misinformation, such as manipulated images or viral hoaxes, and prevent the content from being shared or viewed widely before fact- checking.
- **Pre-Dissemination Fact-Checking**: Introduce a requirement for pre- dissemination fact-checking of certain categories of content, such as political ads or public health information. Platforms could be required to verify this content before allowing it to go live, reducing the spread of false information.

3.2.8 Inconsistent Enforcement and Jurisdictional Challenges

- **Inconsistent Enforcement**: Enforcement of laws related to fake news varies across states and regions in India. The lack of a centralized mechanism to regulate andrespond to fake news creates gaps in enforcement, leading to selective application of laws based on political or social pressures.
- **Jurisdictional Issues**: Fake news often originates from outside India, complicating enforcement. The IT Act, 2000 and related laws have limited extraterritorial jurisdiction, making it difficult to prosecute or take action against individuals or entities spreading fake news from foreign locations.

3.2.9 Privacy Concerns with Traceability and Encryption

The 2021 IT Rules require platforms like WhatsApp to enable the tracing of the first originator of messages, creating tension with end-to-end encryption. This raises concerns about user privacy and data security, as breaking encryption could compromise users' rightsto privacy.

Recommendation:

- **Encrypted Metadata for Traceability**: Rather than breaking encryption, Indiacould require platforms to use encrypted metadata tracking that retains users' privacywhile allowing authorities to trace the origin of harmful content when necessary. This would balance privacy concerns with the need to track fake news.
- **Judicial Authorization for Traceability**: Introduce a requirement that traceability requests can only be initiated with judicial approval, ensuring that users' privacy is not violated unnecessarily. This would limit the government's ability to misuse traceability for political or other non-legitimate purposes.

3.2.10 Promote Collaboration Between Platforms and Fact-Checkers

The spread of fake news can be curbed by fostering collaboration between social media platforms and fact-checkers. Public-Private Collaboration: Create a framework for collaboration between the government, social media platforms, and independent fact- checkers to implement pre-emptive action against fake news. This could include systems forreal-time detection and content moderation to address fake news before it spreads widely.

Recommendation:

- **Incentivize Platform-Fact Checker Partnerships**: Mandate that social mediacompanies work closely with fact-checking agencies to verify suspicious content. Platforms could provide real-time access to third-party fact-checkers who can quicklyverify or debunk viral content.
- **AI-Powered Fact-Checking Tools**: Encourage platforms to invest in AI-basedfact-checking tools that can flag and filter false information before it gains traction. Algorithms could prioritize high-risk categories, such as fake news related to public health, elections, or communal tensions.

3.2.11 Public Awareness and Digital Literacy

India's legal framework does not currently emphasize public education or digital literacy as a tool to combat fake news. Without a well-informed public, laws alone are not enough to curb the problem. Focus on Education and Fact-Checking Instead of Content Takedown. Reactive Rather than Proactive Approach: The current legal framework focuses largely on content takedown rather than fact-checking and digital literacy. While removing harmful content is important, a long-term solution requires greater emphasis on educating the public about how to identify fake news, promoting fact-checking initiatives, and encouraging critical thinking among social media users.

Recommendation:

- **National Media Literacy Campaign**: Launch a nationwide digital literacy campaign to educate the public on how to identify fake news, cross-check information,and understand the risks of spreading misinformation. This could be modeled on Finland's media literacy programs, which have proven effective in curbing the impact of fake news.
- **Media Literacy in School Curriculums**: Incorporate **media literacy** into school curricula, teaching students how to critically evaluate online content and recognize fake news. Educating the next generation will create long-term resilience against misinformation.

3.2.12 Election Period-Specific Regulations

To prevent fake news from disrupting democratic processes, India can introduce election- specific fake news regulations.

Recommendation:

- **Election Misinformation Task Force**: Create an Election Misinformation Task Force that would monitor and address fake news specifically during the electionperiod. This task force could work with social media platforms, election officials, andindependent watchdogs to take real-time action on election-related disinformation.
- **Increased Transparency for Political Ads**: Mandate social media platforms to disclose the source and funding of political advertisements. This will help users identify potential bias or manipulation and prevent foreign or anonymous actors fromspreading false information during elections.

3.3 REGULATION OF FAKE NEWS DISSEMINATION THROUGH SOCIAL MEDIA IN OTHER FOREIGN COUNTRIES

Several countries have implemented effective legal frameworks to curb fake news and impose liability on individuals and platforms. These provisions focus on prevention, real-time intervention, and accountability and could be adapted to the Indian context.

3.3.1 Germany's Network Enforcement Act (NetzDG)[38]

Key Provisions: NetzDG mandates platforms to remove "manifestly unlawful" content, including fake news, within 24 hours or 7 days for less obvious cases. Non-compliance results in fines up to €50 million. Users can flag harmful content for quick action.

Adaptation for India: India can adopt AI-based detection systems for real-time monitoring and mandate collaboration with fact-checkers for verified corrections to reduce misinformation without resorting to censorship.

3.3.2 Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA)[39]

Key Provisions: POFMA empowers authorities to issue "stop communication orders" and correction notices to prevent fake news from spreading. Proactive measures stop falsehoods before they escalate.

Adaptation for India: India could introduce mandatory correction notices for flagged content and stop orders for viral misinformation, especially in contexts like public health or elections.

3.3.3 France's Law Against the Manipulation of Information (2018)[40]

Key Provisions: This law emphasizes fake news prevention during elections, allowing courts to remove false content within 48 hours. It also requires transparency in political ads.

Adaptation for India: India could implement election-specific frameworks for monitoring fake news and introduce judicial oversight for content takedown orders to ensure transparency and accountability.

3.3.4 Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act2019[41]

Key Provisions: Platforms must remove violent or harmful content swiftly or face significant fines. Authorities can issue prevention orders for harmful misinformation.

Adaptation for India: Introduce strong penalties for platforms failing to act on harmful misinformation and preemptive blocking orders for content inciting violence or communal unrest.

[38] Network Enforcement Act (NetzDG), 2017, Bundesgesetzblatt [BGBl.] I at 3352 (Germany).
[39] Protection from Online Falsehoods and Manipulation Act (POFMA), 2019, (Act No. 8 of 2019) (Singapore)
[40] Law Against the Manipulation of Information, 2018, No. 2018-1202 (France).
[41] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, No. 58, 2019 (Austl.).

3.3.5 European Union's General Data Protection Regulation (GDPR) - Model forTransparency[42]

Key Provisions: GDPR mandates transparency in data usage and algorithmic accountability for content prioritization.

Adaptation for India: India could require platforms to disclose algorithmic processes and create a user-centric system to report and track fake news complaints.

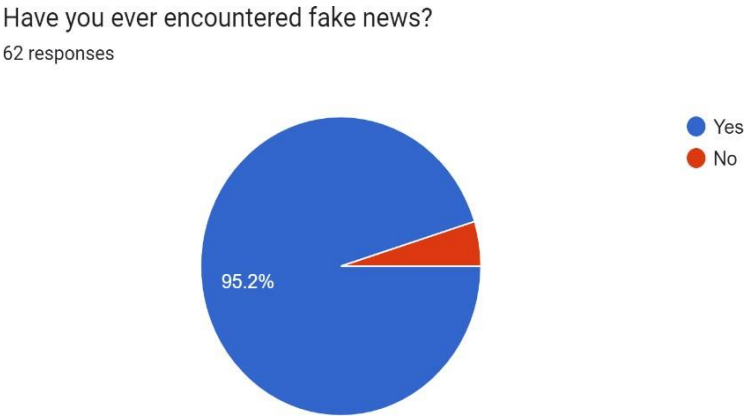
3.3.6 Brazil's Law No. 13.834 (Fake News Law - Election Specific)[43]

Key Provisions: Criminalizes the dissemination of fake news during elections, with penalties including fines and imprisonment. Platforms must monitor and remove disinformation.

Adaptation for India: Introduce criminal liability for spreading election-related fake news, targeting both individuals and platforms to protect democratic processes.

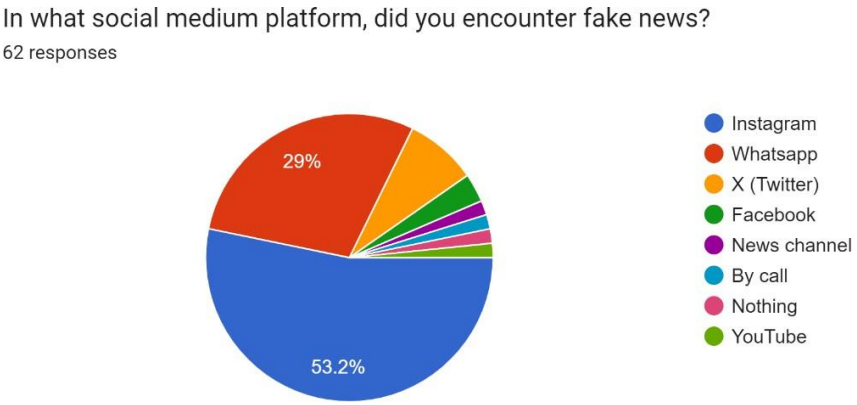
4. DATA ANALYSIS FOR RESEARCH PAPER: DISSEMINATION OF FAKE NEWS THROUGH SOCIAL MEDIA AND HOW FAKE NEWS INFLUENCES THE OPINIONS OF THE GENERAL PUBLIC?

4.1 Encounter with Fake News



The survey reveals that **95.2%** of respondents have encountered fake news, indicatingthat misinformation is highly prevalent across social media platforms. Only **4.8%** reported not encountering it, suggesting that avoiding fake news is nearly impossible inthe current digital environment.

4.2 Platforms of Dissemination:

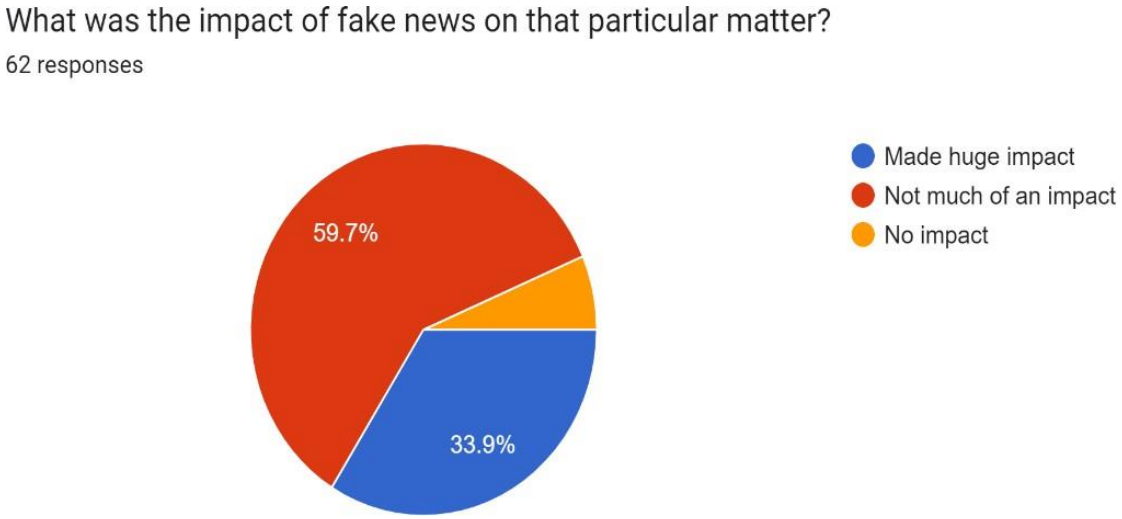


[42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016 O.J. (L 119) 1.

[43] Law No. 13.834, Jan. 4, 2019 (Brazil).

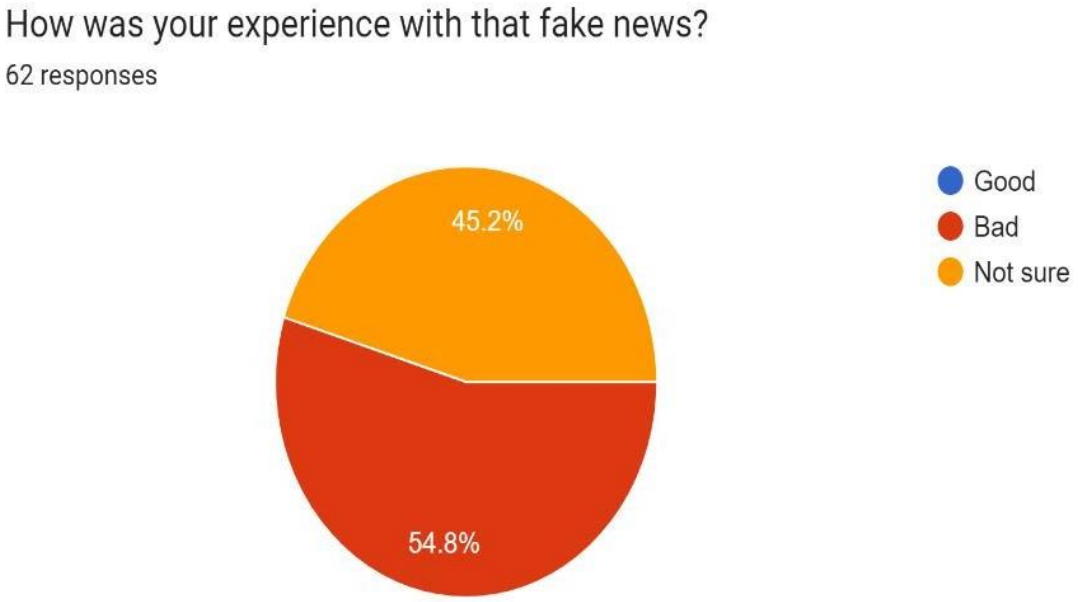
Fake news is most frequently encountered on Instagram (**53.2%**), followed by WhatsApp (**29%**), X (formerly Twitter) (**8.1%**), Facebook (**3.2%**), YouTube (**1.6%**), and news channels (**1.6%**). This highlights how social media is a primary vehicle for misinformation,with Instagram and WhatsApp playing the largest roles.

4.3 Impact of Fake News:



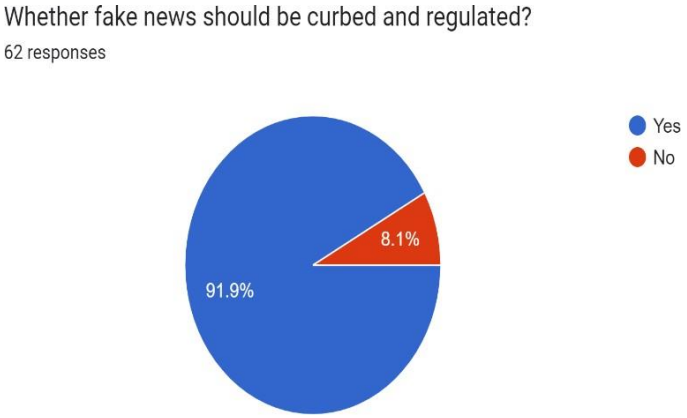
A significant **59.7%** of respondents believe that fake news had a "huge impact" on the particular matter they encountered. This demonstrates how misinformation can sway publicperception, while **33.9%** felt it had "not much impact," and only **6.5%** said it had "no impact."

4.4 Experience with Fake News:



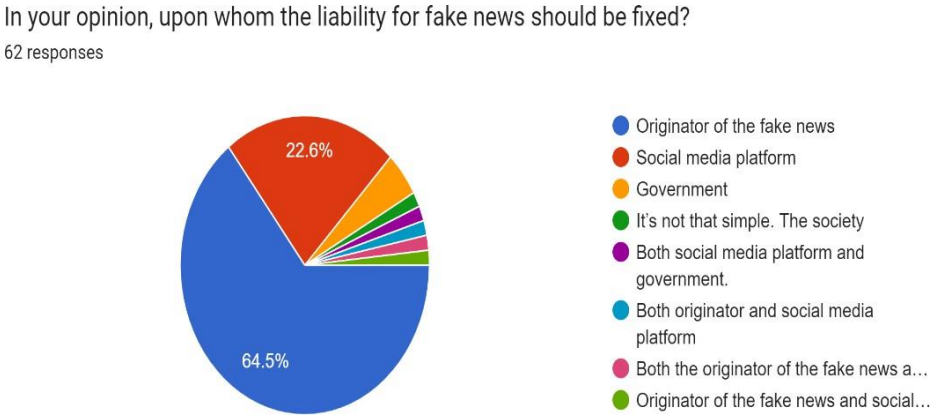
Over half of respondents (**54.8%**) had a "bad" experience with fake news, with **45.2%**unsure of how to categorize their experience. This suggests that the emotional and cognitive toll of dealing with misinformation is significant.

4.5 Desire for Regulation:



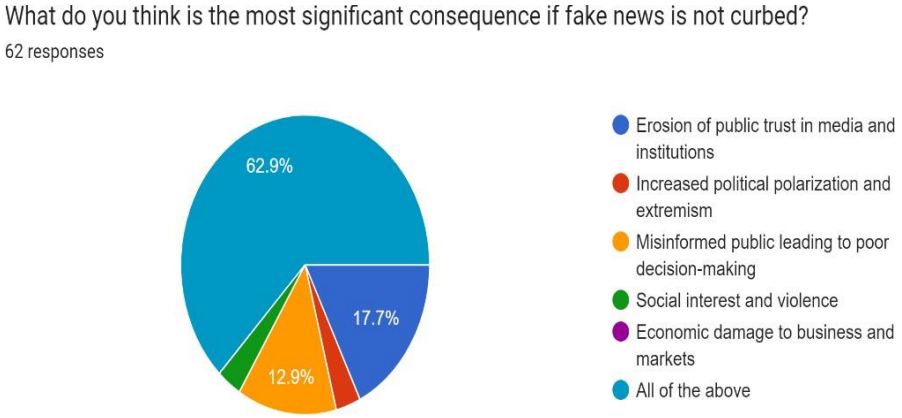
A substantial **91.9%** believe fake news should be curbed and regulated, underscoring apublic demand for stronger legal and regulatory frameworks to combat misinformation.

4.6 Liability for Fake News:



An overwhelming **95.2%** think liability for fake news should be fixed, with the majority placing responsibility on social media platforms (**47.2%**). **40%** believe the originator of the fake news should be liable, and **8%** favor joint liability between both.

4.7 Consequences of Uncurbed Fake News:



Respondents highlighted multiple risks if fake news is not addressed, with **62.9%** citing"all of the above," which includes **erosion of public trust**, **political polarization**, **misinformed public**, **social unrest**, and **economic damage**. The most significant standalone concern was **erosion of public trust** (**17.7%**).

Despite existing regulations, the survey shows that fake news continues to spread, especially through

social media platforms like Instagram and WhatsApp. This pervasive issue can have far-reaching social, political, and economic consequences, leading to a strong call for regulatory action and liability frameworks.

The survey responses reveal a strong consensus on the pervasive and harmful impact of fake news, particularly due to its rapid dissemination through social media. Many respondents viewfake news as a powerful tool used to manipulate public opinion, distract people from importantissues, and sometimes even sway political outcomes. The ease with which false or misleadinginformation spreads, often without verification, leads to widespread confusion and poor decision-making among the public.

A significant concern raised by respondents is the erosion of trust in credible news sources, media institutions, and democratic processes. Fake news is seen as a driver of societal polarization and division, further undermining the public's faith in legitimate information channels. Respondents also highlight the absence of effective verification mechanisms on social media, where users tend to share unverified information, fuelling the spread of misinformation. The lack of accountability for the originators of fake news is seen as a major contributing factor to its rampant spread.

The societal consequences of fake news are seen as particularly severe. It can create unnecessary public commotion, defame individuals or groups, and disrupt social harmony by inciting violence or creating dangerous misconceptions. Many respondents believe that the spread of misinformation leads to societal imbalance and damages the social fabric.

There is a clear call for accountability, with many advocating for holding both individuals andsocial media platforms responsible for the creation and spread of fake news. However, respondents emphasize the need for a balanced approach that ensures regulatory measures do not infringe on freedom of speech. Alongside regulation, respondents recommend stronger verification processes and improved public awareness through media literacy initiatives to combat the spread of misinformation effectively.

In conclusion, the survey underscores the serious impact of fake news on society and the pressing need for a more robust regulatory framework to address its spread. At the same time,it calls for a balanced approach that protects free speech while fostering accountability and verification in media platforms.

CONCLUSION:

The rapid growth of social media has transformed how information is disseminated, but it has also amplified the spread of fake news and misinformation. This paper explored the role of intermediaries, such as social media platforms, in both enabling and curbing the disseminationof misleading content. The analysis focused on two key regulatory frameworks: India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2023and the legal system of other countries.

Through a comparative lens, it is evident that both regulatory regimes aim to strike a balance between enforcing intermediary accountability and safeguarding fundamental rights, such as freedom of speech and privacy. While the IT Rules 2023 emphasize content moderation and traceability in India, the legal system of other countries introduces a more tiered and nuanced approach, particularly with the regulation of Very Large Online Platforms (VLOPs). Both frameworks highlight the growing need for intermediaries to adopt proactive measures to detectand prevent the spread of fake news.

However, despite the progress in regulating intermediary liability, significant challenges remain. The complexity of distinguishing between harmful and benign content, concerns overcensorship, and the technical difficulties in monitoring vast amounts of user-generated content pose ongoing hurdles. Moreover, the global and borderless nature of the internet complicates enforcement across jurisdictions.

To mitigate these challenges, a more harmonized international approach may be necessary, onethat balances the need for accountability with the protection of user rights. Additionally, investing in technological innovations, such as AI-driven moderation tools, and promoting digital literacy can further strengthen the fight against fake news.

In conclusion, intermediary liability plays a crucial role in shaping the future of online contentregulation. While both India's IT Rules and the legal system of other countries represent significant steps forward, continued refinement and cooperation are essential to effectively curb fake news while protecting the core principles of open communication and democracy.

FUTURE DIRECTIVES:

As the spread of fake news continues to pose significant challenges to societies, future researchshould explore several key areas. First, more comprehensive studies on the effectiveness of automated content moderation systems, such as artificial intelligence (AI) and machine learning algorithms, are essential. These technologies hold the potential to detect and flag fakenews in real-time, but their limitations in distinguishing nuanced misinformation from legitimate content need further examination. Future research should also delve into the ethicalimplications of these technologies, particularly regarding potential biases and censorship concerns.

Second, cross-border cooperation is critical in addressing the global nature of fake news. As platforms operate across multiple jurisdictions, developing international regulatory frameworks that ensure uniformity and enforceability while respecting regional legal standardswill be a crucial future directive. Research should explore how regulatory harmonization couldbe achieved and what role multilateral organizations could play in shaping these global standards.

Third, future studies should assess the impact of digital literacy initiatives in combating fake news. Understanding how educational programs that enhance users' ability to critically evaluate online content influence the spread of misinformation will provide valuable insights into long-term strategies for reducing fake news.

Finally, as both the Information Technology Rules 2023 and the legal system of other countriescontinue to evolve, ongoing research is needed to evaluate their real-world effectiveness. Thisincludes analyzing how platforms adapt to these regulations and whether these laws successfully curb fake news without disproportionately infringing on user rights such as free expression and privacy.

REFRENCES:

1. Fake news, disinformation and misinformation in social media: a review | SocialNetwork Analysis and Mining
2. What is Fake News? - Fake News and Information Literacy - Research Guides atUniversity of Oregon Libraries
3. What is "Fake News"? - "Fake News," Lies and Propaganda: How to Sort Fact fromFiction - Research Guides at University of Michigan Library
4. Misinformation, disinformation, and fake news: Cyber risks to business -ScienceDirect
5. Misinformation, disinformation, and fake news: Cyber risks to business -ScienceDirect
6. Disinformation and misinformation triangle: A conceptual model for "fake news"epidemic, causal factors and interventions | Emerald Insight
7. Full article: Misinformation, disinformation, and fake news: lessons from an interdisciplinary,

systematic literature review
8. Misinformation, disinformation, and fake news: lessons from an interdisciplinary,systematic literature review
9. "Intermediary Liability and the Battle Against Fake News: Analyzing the Impact of
10. Role of intermediary in spreading information - Fake News - Google Scholar
11. Combatting Fake News: Alternatives to Limiting Social Media Misinformation andRehabilitating Quality Journalism
12. The digital transformation of news media and the rise of disinformation and fakenews
13. The theater of fake news spreading, who plays which role? A study on real graphs ofspreading on Twitter - ScienceDirect
14. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 06.04.2023)-.pdf
15. IT(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 English.pdf
16. Gazettes | Ministry of Electronics and Information Technology, Government of India
17. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 06.04.2023)-.pdf
18. Chhaya, Rupal, & Afaq, Ahmar. (2022). Information technology (guidelines forintermediaries and digital media ethics code), 2021: critical study. Journal of thePatent and Trademark Office Society, 102(4), 623-635.
19. Buiten, M. C. (2021). The digital services act from intermediary liability to platformregulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 12(5), 361-380.
20. Elena Broda & Jesper Strömbäck (2024) Misinformation, disinformation, and fakenews: lessons from an interdisciplinary, systematic literature review, Annals of the International Communication Association, 48:2, 139-166.
21. Aïmeur, E., Amri, S. & Brassard, G. Fake news, disinformation and misinformation insocial media: a review. Soc. Netw. Anal. Min. 13, 30 (2023). https://doi.org/10.1007/s13278-023-01028-5.