

ISSN: 2582-6433



INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed 6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis



IJLRA

EDITORIAL TEAM

EDITORS

Megha Middha



Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmanagarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmanagarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC - NET examination and has been awarded ICSSR - Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

IJLRA

SOCIAL MEDIA REGULATION: REVIEW OF THE FIELD AND ANALYSIS OF EMERGING TRENDS AND CHALLENGE

Authored By-Venkata Supreeth.K¹

I. Introduction

The subject of inquiry, in light of regulatory and judicial advancements, is the evaluation of the role of Social Media companies, who collect tremendous amount of data by means of enabling an 'attention economy' and mine the data of their users for commercial purposes. It is not the researcher's case that the conception of social media in itself is antithetical to democracy. On the contrary, the researcher's impetus lays on the fact that Social Media is rapidly becoming the platform by which democracy itself is being subverted in the absence of meaningful regulations. This fact had become evident in the recent past with a number of allegations concerning the subversion of the 2016 Presidential Elections of the United States by employing misinformation, the Cambridge Analytica scandal etc.² For example, hate speech and incitement for violence have been explicitly noted by the UN Officials tasked with investigating the atrocities against the Rohingya ethnic group in Myanmar.³ It is begrudgingly noted that we have moved away from entrusting the State with powers to censure its citizens and have instead entrusted Private corporations with the power to censure its customers. While the state can be held accountable for arbitrariness, private corporations cannot be held accountable in all instances. Furthermore, there is an imminent need to examine the impact of social media on the functioning of an electoral system which forms the bedrock of the Indian Democracy. The Constitution mandates a republican system of governance and the surest way to secure legitimacy for political parties is by free and fair elections.⁴ Recent analysis however portrays the trouble in keeping India's elections free and fair, where a top-down messaging infrastructure has been instituted to proceed with dubious political messaging, hate speech and misinformation which vitiates the very idea behind informed decision-making.⁵

¹ The Author is a final year Undergraduate student [Year V, B.A LL.B (Hons)] from Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba, Gandhinagar- 382421

² Allyson Haynes Stuart, 'Social Media, Manipulation, and Violence' (2019) 15 SCJ Int'l L & Bus 100, 106

³ Alexandra Stevenson, 'Facebook admits it was used to incite violence in Myanmar' (*New York Times*, 6 November 2018), available at < <https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html>> accessed on 14 September 2021

⁴ Union of India v. Association for Democratic Reforms & Ors, 2002 (3) SCR 294

⁵ Shruti Shikha and Nandita Mishra, 'Cyber Trooping Activities on Social Media and Its Impact on Elections in India' (2020) 7 Indian JL & Pub Pol'y 37, 40

2.3: Mere Falsehoods Cannot Be Restricted Unless Harm Is Demonstrated

To be specific, both India and U.S extend constitutional protection to falsehoods as well, unless outlawed in specific contexts due to the harm it generates (eg. to prevent offences of fraud, insider trading, defamation, hate speech etc). While India never had the opportunity to examine whether false speech is deserving of constitutional protection, the U.S Supreme Court in *U.S v. Alvarez*⁶ held that falsehoods are protected under First Amendment. Similarly, Canadian Supreme Court ruled that demonstrably false news is still protected and that the state cannot suppress such speech to limit its spread which would be an excessive measure.⁷ However, such protection does not extend to speech that can cause harm for example, incitement of violence against a visible minority.⁸

Before one can consider whether disinformation (specifically, electoral disinformation or ‘fake news’) can be legally regulated, one must note the distinction that mere falsity of certain piece of information does not warrant its censorship by the state as long as it does not have a proximate nexus with the specific harms caused to state interests identified under Article 19(2) of the Constitution of India. It is in this context that the burden on the State or the regulators seems to be higher, when dealing with Disinformation. Merely demonstrating that there is a malicious intent to interfere with the sanctity of the electoral process (free and fair method) is insufficient as long as there is no concomitant breach of, for example, public order or defamation.⁹

II. Electoral Disinformation: It’s Forms And Effects

Mechanism of Spread

Traditionally, political speech receives scant scrutiny from platforms. This is due to the fact that free flow of public discourse is *sine qua non* for instilling public confidence in the electoral process. However, with the rise of technology which removed traditional structures of editorial oversight over content that is disseminated, as well as the prevalence of user-generated content, political speech is increasingly proliferated by disinformation and hateful elements which eventually undermines public trust and places vulnerable communities in danger.¹⁰

Specific to election-related speech or political messaging, distorted or blatantly false election-related speech can induce algorithmically-enhanced virality, search engine bias, lopsided verification

⁶ U.S v. Alvarez, 132 S. Ct. 2537

⁷ R v. Zundel, [1992] 2 SCR 731

⁸ R v. Keegstra [1990] 3 SCR 697

⁹ Vasudev Devadasan, ‘Fake News and the Constitution’ (*Indian Constitutional Law and Philosophy*, 17 June 2020) <<https://indconlawphil.wordpress.com/2020/06/17/fake-news-and-the-constitution/>> accessed on 17 November 2021

¹⁰ Elizabeth F. Judge and Amir Korhani, ‘Disinformation, Digital Information Equality and Electoral Integrity’ 2020 (19) 2 Election Law Journal 240, 241

mechanisms, micro-targeting of political advertisements, doctored content, filter bubbles and echo chambers.¹¹ Algorithms are designed to attract maximum user engagement which is the *modus* by which Platforms generate revenue. However, the algorithms that enhance virality also customize a user's feed predicated on the inherent biases of the user. Coupling the two factors lead to the potentially disastrous outcome of amplifying a narrative that can statistically result in more user engagement, but reduces the exposure to nuance. This process involves confirming of the user's pre-existing beliefs with scant regard to the veracity of the narrative (Confirmation bias).¹²

A combination of human and AI generated tools can be employed to generate false narratives, which permeate the feeds. Of such content, videos designed to arouse the passions and emotions of the audience can be quickly viral, both on account of the persuasive value and the working of bots and sock-puppet accounts. Such content is consumed unsuspectingly, partly on account of their pandering to the confirmation bias of the users and partly due to the fact that truth-value is extremely hard to discern in the face of persuasiveness.¹³ The other cause of concern is that it is now established by empirical studies that 'fake news' (of which disinformation is a subset) disseminates at a faster rate on social media than accurate news, thus posing practical challenges to the theoretical justification offered to the oft-quoted 'marketplace of ideas' doctrine.¹⁴

Notable Examples Of Unchecked Use:

In the run-up to the Presidential Elections in Brazil, the instrumental role played by Whatsapp in spreading disinformation was noted. Researchers rely on the documents provided by the Federal Court for Electoral disputes in Brazil to argue how the operational structure of Whatsapp allowed a small, coordinated group of volunteers supporting the conservative factions, to target and influence more than 40% of the country's most devout Catholic population against incumbent President Jair Bolsonaro's chief opponent, the left-leaning Fernando Haddad. In a noted instance, a group of people circulated a mischaracterized news article of Haddad sharing the alleged 'gay kits' to teachers and volunteers in schools of Brazil in his role as the Education Minister. The article is misconstrued in the sense that there indeed was a distribution, however the material in question is a toolkit on sensitization of teachers and support staff across Brazil's public education system on homosexuality. What was mischaracterized is Haddad's stance on the issue which was portrayed by fake Whatsapp forwards as one actively

¹¹ Tufekci, Zeynep, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency," (2015) 13 Col. Tech L. J. 203, 217; Danaher, John, et al. "Algorithmic Governance: Developing a Research Agenda Through the Power of Collective Intelligence," (2017) Big Data & Society 4(2): 1–21

¹² Flaxman et.al. "Filter Bubbles, Echo Chambers, and Online News Consumption," (2016) 80 (1) Public Opinion Quarterly 298, 299

¹³ Neill Fitzpatrick, 'Media Manipulation 2.0: The impact of Social Media on News, Competition and Accuracy' 2018 (4) 1 Athens Journal on Mass Media and Communication 45, 48

¹⁴ Ekaterina Zhuravskaya et.al, "Political effects of Internet and Social Media" 2020 (12) Ann. Rev Econ 19.1, 19.14

promoting Homosexuality which has huge ramifications in a country with significant number of devout Catholics. The size and operation of the campaign proves that such attempts cannot be characterized as innocent online behavior but a well-coordinated disinformation campaign.¹⁵ The *Haddad* instance also points to the efficacy of Technology-based measures involving Artificial Intelligence to discern such messages accurately, by contextual analysis which a human may apply in passing judgment on the “truth-value” of a statement.

India and Brazil share a similar set of profile inasmuch as the diversity of the electorate is concerned. Both countries are diverse regions with large populations comprising different ethnic, racial and religious communities. The (mis)use of Whatsapp as a tool to disseminate fake news is well-documented in the run up to the 2019 General Elections in India as well¹⁶, and the pernicious impact that fake-news induced violence has on the life and liberty of political dissidents and religious minorities.¹⁷

Only in the rarest of instances did platforms decide to step in and impose sanctions on the free expression on the basis of the resulting harm, most notable amongst which is the immediate suspension of Former U.S President Donald Trump’s Social Media accounts after he had urged his supporters to ‘overturn’ the 2020 Presidential election. Interpreting his tweets led to armed groups attempting to enter the U.S Capitol on 6th January 2021, which resulted in vandalism, injury and death of the security personnel and rioters.¹⁸

Conundra In Regulating Online Disinformation:

In a *laissez-faire* or Self-regulating regime, the costs of these rare and dramatic events are borne exclusively by the society rather than the social media platforms themselves. Furthermore, the violent effects of disinformation are inherently stochastic. It is impossible to predict with certainty that a given collection of content will cause specific harm.¹⁹ Thus, in a self-regulation setup, platforms face no compelling reasons to prevent the spread of disinformation or to filter false information which is likely to cause specific harm. Further, platforms are not adequately incentivized to employ active methods of

¹⁵ Gustavo Ferreira Santos, 'Social Media, Disinformation, and Regulation of the Electoral Process: A Study Based on 2018 Brazilian Election Experience' (2020) 7 Revista de Investigações Constitucionais 429

¹⁶ Anupam Das and Ralph Schroeder, 'Online Disinformation in the run-up to the 2019 Indian Election' 2020 (24) 12 Information, Communication & Society 1762, 1775

¹⁷ Snigdha Poonam and Samarth Bansal, 'Misinformation is endangering India's Elections' (*The Atlantic*, 01 April 2019) <<https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/>> accessed on 17 November 2021

¹⁸ Dan Burns, 'FBI, Other agencies did not pay heed to mounting warnings of Jan. 6 riot' (*Reuters*, 1 Nov 2021) <<https://www.reuters.com/world/us/fbi-other-agencies-did-not-heed-mounting-warnings-jan-6-riot-washington-post-2021-10-31/>> accessed on 17 November 2021

¹⁹ Shehroze Khan and James Wright, 'Disinformation, Stochastic Harm, and Costly Filtering: A Principal-Agent Analysis of Regulating Social Media Platforms' (2021) <<https://arxiv.org/abs/2106.09847>> last accessed 16 November 2021

screening contents, especially the viral ones, at the risk of losing user interaction and platform revenue. In such instances that the platforms do police themselves effectively, either by human means or technological devices, they are highly susceptible to failure for want of judgment²⁰ and lack transparency in decision-making and hence may adopt policies that are overreaching which suppress legitimate speech.

Despite the size and extent of disinformation campaigns mobilized on the social media, no effective consensus can be reached on the most-efficient and legally permissible methods for curbing the problem. The problem impacts democratic nations in a more acute manner than autocracies. Within the constitutional framework adopted by most democracies, researchers point out to the most plausible constitutional hurdles which any legislation attempting to curb fake news may encounter. For instance, the 'marketplace of ideas' doctrine received an institutional sanction in the First Amendment Jurisprudence in the U.S. The U.S Judiciary went to the extent of holding that truth must compete with falsehoods until truth prevails in the said marketplace of ideas.²¹ Within the context of Disinformation, any regulation which is based on the speaker's message is content-based regulation. Laws which draw a distinction based on the communicative content between acceptable and unacceptable speech are presumptively unconstitutional and may survive the scrutiny of First Amendment only if the government proves that the restrictions are narrowly tailored to serve a compelling state interest.²² Further, specifically in the US context, laws that decrease the reach (or amplification of speech) face the same strict scrutiny under the First Amendment as laws that ban speech outright.²³ Content-based regulations face the strictest judicial scrutiny under U.S Law.

However, content-based regulation in a general sense, which does not relate to any attendant harm or a compelling state interest is unconstitutional in most common law jurisdictions. It is here that the principle of stochastic harm is most important. Platforms have no meaningful method, irrespective of the kind of regulatory model in place, to effectively and accurately determine the possible impact of certain lawful but untrue content. Electoral Disinformation does not produce any tangible harm either. Most instances of disinformation do not precede imminent harm, however protracted periods of exposing the internet audiences to dubious political messaging, unverified hoaxes etc. can result in gradual erosion of trust in both public institutions and media as well, while leaving the civil society fractured and polarized into different echo chambers.²⁴ This situation may often lead to a situation of

²⁰ Maarten Sap et al., *The Risk of Racial Bias in Hate Speech Detection*, <<https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf>> last accessed 14 November 2021

²¹ N.Y. Times Co. v. Sullivan, 376 U.S. 254, 269-80 (1964))

²² Nina I Brown and Jonathan Peters, 'Say This, Not That: Government Regulation and Control of Social Media' (2018) 68 Syracuse L Rev 521, 533

²³ U.S v. Playboy, 529 U.S. 803, 812 (2000); see also Sorrell v. IMS Health Inc., 564 U.S. 552, 566 (2011)

²⁴ Jarred Prier, 'Commanding the Trend: Social Media as Information Warfare' (2017) 11(4) *Strategic Studies Quarterly* 50, 61

paralysis of the public opinion.²⁵

Viewed from a different perspective, models of regulation aiming to penalize actions of propagating lawful but harmful speech (which involve most instances of disinformation campaigns) tend to place the wrong incentives to the platforms in question which act as moderators. Since the determination of whether certain kinds of content should be allowed to be amplified is partly-judicial and partly-technical, companies tend to err on the side of caution and tend to over-enforce which leads to suppression of lawful speech on certain instances.²⁶

Disinformation Versus Arbitrariness

To summarize, most countries with an Authoritarian make are at more ease to shield themselves against the pernicious impact of Disinformation than Constitutional Democracies with guaranteed freedom of speech, since their political systems allow the state to play the role of the arbiter of truth. However, this does not downplay the threat posed by Disinformation to the collective of nations, none of whom are immune to the phenomenon of weaponization of Social Media which transcend domestic concerns of free speech and privacy and extend into humanitarian concerns.²⁷

The only method that the Indian government adopted thus far to counter the extreme effects of online disinformation is to impose internet shutdowns. India leads the world in the number of internet shutdowns in a given year.²⁸ This number had skyrocketed in the aftermath of the repealing of Article 370 of the Constitution of India, which is a provision granting autonomy in increased measure to the border state of Jammu and Kashmir. What followed was an internet shutdown in the region with the professed objective of culling down of protests and demobilize the extremist elements in the state. However, the Indian attempts to institute internet shutdowns were characterized as 'indiscriminate' which tantamount to censorship.²⁹ Similarly, China adopted a radical approach to retain social control either by outright banning of the websites of major social media companies, owned or established in the United States or European Union. Instead, the Chinese markets are serviced by domestic counterparts to popular apps. Further, China's infamous 'Great Firewall' blocks content hosted by Foreign Social Media companies to be accessed by Chinese citizens. Whatever little content created by foreign entities

²⁵ Pablo Barbera, 'Social Media, Echo Chambers and Political Polarization' in Nathaniel Persily and Joshua A. Tucker eds. *Social Media and Democracy: State of the field and Prospects for Reform* (Cambridge University Press 2020) 35, 36

²⁶ Daphne Keller, 'Amplification and its Discontent: Why regulating the reach of Online Content is hard' (*Knight First Amendment Institute*, 8 June 2021), available at <<https://knightcolumbia.org/content/amplification-and-its-discontents>> last accessed

²⁷ Mark Silverman, 'LikeWar: The Weaponization of Social Media' (2019) 101 *Int'l Rev Red Cross* 383, 385

²⁸ Anam Ajmal, '70% of global internet shutdowns in 2020 were in India: Report' (*Times of India*, 04 March 2021) <<https://timesofindia.indiatimes.com/india/70-of-global-internet-shutdowns-in-2020-were-in-india-report/articleshow/81321980.cms>> accessed on 17 November 2021

²⁹ Allyson Haynes Stuart, 'Social Media, Manipulation, and Violence' (2019) 15 *SC J Int'l L & Bus* 100, 120

and persons that percolates into the Chinese virtual ecosystem is closely monitored by State Agencies which enforce stringent laws against violators who defy the Chinese norms.³⁰

What is being noticed here is that Disinformation in itself is becoming a pretense or a ruse for either Governments to engage in direct acts of internet censorship or otherwise employ indirect methods such as overbroad or vague regulations (as noted by Supreme Court about the now struck-down Section 66A of Information Technology Act, 2000 in *Shreya Singhal v. Union of India*³¹), both of which are speech-intrusive measures which fall foul with constitutional guarantees.

Drawbacks Of The Legal Regime In India To Counter-Disinformation In Elections

i. Why sole reliance on the Platform's efforts cannot be placed

While disinformation may present a credible threat of foreign interference impacting the integrity of a sovereign state, it is disingenuous to frame the debate only along the lines of geopolitics. *Freedom House*, an international not-for-profit organization in its 2019 report observed the elections and referendums of 30 countries that year to conclude that domestic actors have abused information technology to subvert the electoral process. Three distinct forms of digital election interference were noted:

*“informational measures, in which online discussions are surreptitiously manipulated in favor of the government or particular parties; technical measures, which are used to restrict access to news sources, communication tools, and in some cases the entire internet; and legal measures, which authorities apply to punish regime opponents and chill political expression.”*³²

Content moderation is, but a piecemeal strategy to combat disinformation on Social media. Put simply, Content moderation is a routine practice undertaken by the Platforms to remove harmful content which is violative of the rights of the persons who may be concerned, or content which is violative of the community guidelines of the platform in question. In an ideal scenario, content moderators are concerned only with extreme forms of messaging, which is either affront to human dignity, defamatory, obscene or excessively violent and thus illegal. Content moderation is a complex process involving scores of employees enforcing the Platform's policy by reviewing content, which is undertaken with the assistance of both human operatives and technology-based tools. While content moderation is an effective solution to prevent hate speech or obscene conduct which is illegal everywhere (such as child

³⁰ Elizabeth C. 'The Great Firewall of China: Xi Jinping's internet shutdown' (*The Guardian*, 29 June 2018) <<https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>> accessed on 17 November 2021

³¹ *Shreya Singhal v. Union of India*, 2015 (5) SCC 1

³² Adrian Shahbaz and Allie Funk 'Freedom on the Net 2019: Crisis of Social Media' (*Freedom House*, 2019) <<https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>> accessed on 17 November 2021

pornography), revising the guidelines for content moderation to tackle electoral disinformation is not an effective solution, in light of the facts that political speech must be reviewed liberally and that falsehoods are constitutionally protected unless harm can be demonstrated by propagating such falsehoods. Past conduct of notable platforms like Facebook demonstrates that platforms have been historically reluctant to restrict political speech. Rules applied to state leaders are generally more lenient than those applied to govern the speech of others. Further, the process of formulating content-moderation policies are not participatory and highly opaque.³³

ii. India's tryst with Self-Regulation: right intentions, wrong measures

At present, the statutes in India do not recognize disinformation as either a crime or a corrupt electoral practice. However, in view of the pernicious impact it has on democracy, certain efforts have been attempted in the recent past. The Election Commission of India ('ECI') is a constitutional body tasked with exercising oversight over the electoral process.³⁴ In discharge of this mandate, the ECI may prescribe the Model Code of Conduct which are in the nature of guidelines. Notably, in 2019 the ECI extended the application of the Model Code of Conduct to the social media practices of political parties and individual candidates contesting in the elections. Further, the publication of political advertisements on Social Media platforms is to be pre-certified and the expenses incurred in such distribution must be reported to the ECI³⁵ As a manner of self-regulation, the ECI allowed Social Media Companies to adopt a 'voluntary code of ethics' with the Internet and Mobile Association of India (IAMAI) acting as a representative to Social Media companies in India and the chief liaison agent. Pursuant to the voluntary code of ethics, major Social media sites have agreed to report to the ECI on violations being reported by users under Section 126 of the RPA. However, as things stand, IAMAI acts as a buffer between the ECI and social media companies. Under this model, there can be no accountability on Platforms, despite being direct parties to disinformation, nor can there be an enforceable obligation for failure to report unlawful contents.³⁶ Critics point out to the model of self-regulation co-opted by the ECI-IAMAI by drawing parallels to the Code of Ethics and Broadcasting Standards³⁷ applicable to Commercial News television. The said code is adopted by the News Broadcasters & Digital Association ('NBDA'), which is a professional body of private news broadcasters. In response to the growing calls for direct

³³ Kai Reimer and Sandra Peter, 'Algorithmic Audiencing: Why we need to rethink Free Speech on Social Media' 2021 (36) 4 Journal of Information Technology 409, 417

³⁴ Constitution of India 1949, art.324

³⁵ Nitish Kashyap, 'No Political Ads without Pre-certification, Code of Conduct being evolved in consultation with IAMAI and Social Networking sites, ECI tells Bombay High Court' (*Livelaw*, 11 March 2019) <<https://www.livelaw.in/news-updates/no-political-ads-without-pre-certification-code-of-conduct-iamai-and-social-networking-sites-eci-bombay-hc-143471>> last accessed 17 November 2021

³⁶ Udupa, Sahana, 'Digital Disinformation and Electoral Integrity: Benchmarks for Regulation' 2019 (54) 51 (*EPW* 28 December 2019) <<https://www.epw.in/engage/article/digital-disinformation-and-election-integrity>> accessed on 17 November 2021

³⁷ Code of Ethics and Broadcasting Standards, (NBDA 01.04.2008) <<http://www.nbanewdelhi.com/code-of-ethics-and-broadcasting-standards>> accessed on 17 November 2021

governmental regulation, the NBDA adopted peer-surveillance mechanisms in 2008. Since then studies have demonstrated that the NBDA failed to take punitive action against violators. Criticism had also been levied against the Press Council of India, a statutory body devoid of any meaningful legal powers to punish violators or evolve a system of journalistic rules. Experience demonstrates that self-regulation models may result in subjugation of regulations in furtherance of business goals in light of the evolving cross-media ownership models in India.³⁸

To complicate the matters still, organized disinformation on Social Media happens through indirect means. The problem arises, in part due to structural concerns surrounding the conduct of elections in general, more particularly due to the absence of oversight over campaign funding. Political parties engage volunteers, think tanks, consultancies and corporations, as shown in the *Cambridge Analytica* instance, which makes dubious political messaging untraceable to a certain individual or a political party. Neither is there any requirement to report the expenses incurred in engaging third-parties or money spent by third parties on a candidate's behalf.³⁹ Section 77 of RPA Act only regulates the expenditure of only 'individual candidates' and not 'political parties'. Hence there is no ceiling on the campaign expenditure incurred by parties. Anonymous donations to parties are possible by means of Electoral bonds. This implies that candidates can benefit from substantial illicit spending incurred on part of other actors who are legally exempt from oversight.⁴⁰

India does not have a comprehensive Data Protection regime in place at the moment, unlike its enforceable counterpart in EU General Data Protection Regulation ('GDPR') or other privacy-protecting statutes in force in certain states in the U.S. In absence of a statute providing enforcement mechanisms for the rights of Data principals against unauthorized use of their personal data by the fiduciaries, corporations are at a liberty to transfer personal data within the economy to interested parties which employ measures such as demographic profiling or micro-targetting to swing the elections in their favour.⁴¹ However, the Draft Data Protection Bill is currently in the works, being mooted by the Indian Parliament which may result in curbing of such systemic factors to certain extent which aid unscrupulous actors engaging in coordinated disinformation practices. Further reforms are awaited which may declare certain aspects of "Cyber-trooping" such as operation of troll-farms, transparency in election funding and use of disinformation as corrupt electoral practices, aided by consistent jurisprudence on the subject.

³⁸ Mathew, Meera, 'Media Self-regulation in India: A Critical Analysis' 2016 ILJ L. Rev 25, 33

³⁹ Rajesh Serupally, 'Are Political Consultancies a threat to Indian Democracy?' (*The Wire*, 17 June 2019) <<https://thewire.in/politics/elections-2019-political-consultants-democracy>> accessed on 17 November 2021

⁴⁰ Milan Vaishnav, 'Political Finance in India: Déjà vu all over again' (*Carnegie Endowment for International Peace*, 31 January 2019) <<https://carnegieendowment.org/2019/01/31/political-finance-in-india-d-j-vu-all-over-again-pub-78280>> accessed on 17 November 2021

⁴¹ Shruti Shikha and Nandita Mishra, 'Cyber Trooping Activities on Social Media and Its Impact on Elections in India' (2020) 7 Indian JL & Pub Pol'y 37, 46

Iv. Efforts By Other Jurisdictions To Combat Disinformation And Hate Speech

Both the EU and UK authorities have discarded the theoretical framework and rationale behind pursuing ‘fake news’ which is an umbrella term in common parlance including all kinds of falsities of varying proportions, ranging from lopsided journalism to doctored images or videos. Instead, the EU and UK governments adopt an intent-based classification to streamline regulatory measures. Under this paradigm, the government or the regulatory entity ought to concern itself, only with the “deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain.”⁴² Hence, misinformation which is the inadvertent sharing of false information, unaccompanied by intent can be excluded altogether. Similarly, the High Level Expert Group of the European Union adopted an intent based classification to combat disinformation.⁴³

As against the self-regulation model currently in force in India, two other options available to Indian Government is to engage either in comprehensive regulation of content, following the lead of France and Germany, or to enter a regime of co-regulation as characterized by the approach of the United Kingdom. In the first option of Strong government regulation, the German government enacted the Network Enforcement Act of 2017 (‘NetzDG’)⁴⁴. The statute enforces responsibility on the Social Media platforms for illegal content hosted by them and hate-speech, placing a ‘notice-and-takedown’ regime which gives the platform 24 hours or to face heavy fines. The regime relies on the determination by the platform on the legality of the content which again, rises concerns about over-regulation by the platform to err on the side of caution. Similarly, France enacted a law⁴⁵ criminalizing the dissemination of fake news during elections. The French law imposes certain obligations and constraints on Platforms, including mandatory transparency obligation on the source of financing for political advertisements, the use of personal data and expenses incurred in dissemination.⁴⁶ While the German law encountered criticism on grounds of theoretical concerns surrounding censorships in the hands of private corporations, the benefit of adopting a hands-off model prescribing liability on platforms is that the State incurs minimal cost of enforcement. Its efficacy, however, is still a matter of academic review.

In the second option of Co-decided Accountability or Limited regulation, the Platform has a higher role to play in devising systems to counter disinformation, but shall operate under the oversight of

⁴² Digital, Culture, Media and Sport Committee, *Disinformation and ‘fake news’* (HC 2017-19 1791) para 12

⁴³ Carme Colomina et.al, ‘The impact of Disinformation on democratic processes and human rights in the world’ (*European Parliament DROI Sub-committee*, 22 April 2021) : QA-02-21-559-EN-N

⁴⁴ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Federal Law Gazette I, p. 3352 ff. (1 October 2017)

⁴⁵ Organic Law No. 2018-1201 of 22 December 2018 Regarding the Fight Against Information Manipulation

⁴⁶ Zachary Young, ‘French Parliament passes law against ‘fake news’’ (*Politico*, 04 July 2018) <

<https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/>> accessed on 17 November 2021

autonomous public institutions with a defined mechanism for escalation and grievance redressal which aims to cater to multiple stakeholders. This may involve the State certifying the codes of practice rather than being left to the decision of exclusively professional bodies of media persons, engineers or BigTech executives. This model is inspired by the principles of controlled pluralism, transparency and engagement with civil society in the decision-making process. In the British Model, the Office of Communications (Ofcom) exercises autonomous oversight over the implementation of certified codes which prescribe a statutory duty of care to platforms in screening illegal or harmful conduct. The co-decided accountability model relies on human instruments as market players wish to minimize the risk of regulation while collaborating with the civil society while addressing the content moderation policies.⁴⁷ In this model, a Certified code of Practice can be implemented which address concerns surrounding the internal governance of the platforms such as resources allocated for content moderation, adherence to industry standards, deployment of technical measures, training of content moderators and public feedback

V. Concluding Comments

A potentially useful method of ensuring healthy cyber-governance is to adopt a principles-based approach than a rules-based approach. A rules based approach relies on the prescriptions of the regulator a list of do's and don'ts which cannot account for all possible contingencies to effectively guide the day-to-day activities of the platform in question. The said approach results in both high costs of compliance as well as high costs of regulation and is thus inefficient. Instead, certified codes of practice must embrace the core principles (a model followed by GDPR with respect to Privacy , transparency and individual autonomy for example) as the latter imposes a general standard of conduct, which leaves discretion with the regulators to decide on whether a particular conduct must trigger sanction.

Within the U.S, arguments have been initiated by interest-groups to promote competition within the virtual world which currently operates in a state of state-sanctioned monopoly, considering the fact that the use of social media is ingrained into our daily lives. This concern arises, not as a retort to the systemic infringement of fundamental rights but out of humbler concerns about abuse of market position and anti-trust laws. Breaking-up of major conglomerates such as the Facebook group, coupled with consistent enforcement of industry standards promote competition and offer users the choice and also provide platforms with an incentive to moderate the discourse. Potential loss of engagement from the breach of industry standards places a fiscal incentive on Platforms to comply with industry

⁴⁷ Emiliana De Blasio and Donatella Selva, 'Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era' 2021 65 (6) American Behavioral Scientist 825, 837

standards. However, breaking up of such corporations, most of which are predominantly based in the U.S depends on the approach taken by the U.S Lawmakers towards the problem and the Judiciary in appreciating and upholding the antitrust concerns raised by the interest groups.⁴⁸

At present, there are no regulations preventing targeted advertising which involve processing of personal data and sensitive personal data collected without consent. The law can either prohibit such actions or provide the users with a choice from opting-out from targeted advertising. Further, since India does not have a comprehensive data protection regime in place, collection, processing or dissemination of data without the user's consent is not penalized. Within the legal vacuum concerning both data protection and campaign financing, unscrupulous electoral practices are thriving. Ample evidence, as demonstrated in the preceding chapters, suggest that the industry's calls for self-regulation must be viewed suspiciously, in view of the past performance of such mechanisms in electronic media. A systematic approach which alters the incentive matrix is the most plausible method for constitutional democracies to pursue without raising concerns about free speech infringement.⁴⁹

Finally, specific to combatting electoral disinformation, the legal system governing elections as a whole must be reformed. Greater transparency into campaign financing and mandatory disclosures of the role played by political consultancies and think-tanks is the need of the hour. Concerning Electoral disinformation, raising the liability of platforms within the Indian context seems to be counter-productive while at the same time, allowing the Government to promulgate overbroad regulations may result in self-censure and chilling effect which stifles free expression. While the 2021 IT Rules have moved away from *laissez-faire* approach of intermediary regulation, certain concerns still abound, particularly with respect to the provision in 2021 rules which allows the government, in course of an investigation, to compel messaging services to 'trace the first-originator'. For instance, *Whatsapp* has taken objection to the provision, terming it to be 'overbroad' and violative of the Right to Privacy of its users, since its services are used by the users in light of the end-to-end encryption that *Whatsapp* offers. A constitutional challenge to the 2021 IT rules has already been instituted.

In view of the preceding discussions, it is concluded as thus:

1. Disinformation is protected under the Constitution of India unless the State can demonstrate the narrow grounds on which lawful but dubious or false speech must be regulated by demonstrating the harms
2. Disinformation has been used as a ruse to incorporate regulations which are overbroad, employ vague terms and may result in chilling effect of self-censure

⁴⁸ Alex Rothenfort, 'Regulating Social Media Platforms: A Comparative Policy Analysis' 2020 (25) Comm. L & Pol. 225, 254

⁴⁹ Israr Khan, 'How can States effectively regulate Social Media Platforms?' (*Oxford Business Law Blog*, 13 January 2021) < <https://www.law.ox.ac.uk/business-law-blog/blog/2021/01/how-can-states-effectively-regulate-social-media-platforms> > accessed on 17 November 2021

3. In a self-regulatory regime, the mix of incentives do not push the Platforms to engage in greater scrutiny of political speech fearing censure and loss of user engagement. Hence self-regulation must be complemented by accredited industry standards and oversight by regulators, peer groups and academia.
4. The model adopted by India in regulating Disinformation suffers from severe structural drawbacks and thus there is an imminent need to reform the law.

Bibliography

Books

- Bhatia, Gautam, *Offend, Shock or Disturb: Free Speech under the Indian Constitution*, (2016 Oxford University Press 1 ed)
- Pablo Barbera, 'Social Media, Echo Chambers and Political Polarization' in Nathaniel Persily and Joshua A. Tucker eds. 'Social Media and Democracy: State of the field and Prospects for Reform' (Cambridge University Press 2020)

Command Papers:

- Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news'* (HC 2017-19 1791)
- Carme Colomina et.al, 'The impact of Disinformation on democratic processes and human rights in the world' (European Parliament DROI Sub-committee, 22 April 2021) : QA-02-21-559-EN-N
- Law Commission of India, *Electoral Reforms*, (Law Com No. 255)
- Code of Ethics and Broadcasting Standards, (NBDA 01.04.2008)

Journal Articles

- Alex Rothenfort, 'Regulating Social Media Platforms: A Comparative Policy Analysis' 2020 (25) *Comm. L & Pol.* 225
- Allyson Haynes Stuart, 'Social Media, Manipulation, and Violence' (2019) 15 *SC J Int'l L & Bus* 100
- Anupam Das and Ralph Schroeder, 'Online Disinformation in the run-up to the 2019 Indian Election' 2020 (24) 12 *Information, Communication & Society* 1762,
- Ekaterina Zhuravskaya et.al, "Political effects of Internet and Social Media" 2020 (12) *Ann. Rev Econ* 19.1

- Elizabeth F. Judge and Amir Korhani, 'Disinformation, Digital Information Equality and Electoral Integrity' 2020 (19) 2 Election Law Journal 240
- Emiliana De Blasio and Donatella Selva, 'Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era' 2021 65 (6) American Behavioral Scientist 825
- Flaxman et.al. "Filter Bubbles, Echo Chambers, and Online News Consumption," (2016) 80 (1) Public Opinion Quarterly 298
- Gustavo Ferreira Santos, 'Social Media, Disinformation, and Regulation of the Electoral Process: A Study Based on 2018 Brazilian Election Experience' (2020) 7 Revista de Investigacoes Constitucionais 429
- Jarred Prier, 'Commanding the Trend: Social Media as Information Warfare' (2017) 11(4) *Strategic Studies Quarterly* 50
- K.D Gaur, 'Constitutional Rights and Freedom of the Media in India' (1990) 11 J Media L & Prac. 44
- Kai Reimer and Sandra Peter, 'Algorithmic Audiencing: Why we need to rethink Free Speech on Social Media' 2021 (36) 4 Journal of Information Technology 409,
- Mark Silverman, 'LikeWar: The Weaponization of Social Media' (2019) 101 Int'l Rev Red Cross 383
- Mathew, Meera, 'Media Self-regulation in India: A Critical Analysis' 2016 ILJ L. Rev 25,
- Neill Fitzpatrick, 'Media Manipulation 2.0: The impact of Social Media on News, Competition and Accuracy' 2018 (4) 1 Athens Journal on Mass Media and Communication 45
- Nina I Brown and Jonathan Peters, 'Say This, Not That: Government Regulation and Control of Social Media' (2018) 68 Syracuse L Rev 521
- Shehroze Khan and James Wright, 'Disinformation, Stochastic Harm, and Costly Filtering: A Principal-Agent Analysis of Regulating Social Media Platforms' (2021)
- Shruti Shikha and Nandita Mishra, 'Cyber Trooping Activities on Social Media and Its Impact on Elections in India' (2020) 7 Indian JL & Pub Pol'y 37,
- Tufekci , Zeynep, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency," (2015) 13 Col. Tech L. J 203, 217; Danaher , John, et al. "Algorithmic Governance: Developing a Research Agenda Through the Power of Collective Intelligence," (2017) Big Data & Society 4(2) 4-21
- Udupa, Sahana, 'Digital Disinformation and Electoral Integrity: Benchmarks for Regulation' 2019 (54) 51 (*EPW* 28 December 2019)

Online Sources/ Newspaper Articles

- Adrian Shahbaz and Allie Funk 'Freedom on the Net 2019: Crisis of Social Media' (Freedom House, 2019) <<https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>>
- Alexandra Stevenson, 'Facebook admits it was used to incite violence in Myanmar' (New York Times, 6 November 2018), available at <<https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html>>
- Anam Ajmal, '70% of global internet shutdowns in 2020 were in India: Report' (Times of India, 04 March 2021) <<https://timesofindia.indiatimes.com/india/70-of-global-internet-shutdowns-in-2020-were-in-india-report/articleshow/81321980.cms>>
- Dan Burns, 'FBI, Other agencies did not pay heed to mounting warnings of Jan. 6 riot' (Reuters, 1 Nov 2021) <<https://www.reuters.com/world/us/fbi-other-agencies-did-not-heed-mounting-warnings-jan-6-riot-washington-post-2021-10-31/>>
- Elizabeth C. 'The Great Firewall of China: Xi Jinping's internet shutdown' (The Guardian, 29 June 2018) <<https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>>
- Israr Khan, 'How can States effectively regulate Social Media Platforms?' (Oxford Business Law Blog, 13 January 2021) <<https://www.law.ox.ac.uk/business-law-blog/blog/2021/01/how-can-states-effectively-regulate-social-media-platforms>>
- Maarten Sap et al., The Risk of Racial Bias in Hate Speech Detection, <<https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf>>
- Milan Vaishnav, 'Political Finance in India: Déjà vu all over again' (Carnegie Endowment for International Peace, 31 January 2019) <<https://carnegieendowment.org/2019/01/31/political-finance-in-india-d-j-vu-all-over-again-pub-78280>>
- Nitish Kashyap, 'No Political Ads without Pre-certification, Code of Conduct being evolved in consultation with IAMAI and Social Networking sites, ECI tells Bombay High Court' (Livelaw, 11 March 2019) <<https://www.livelaw.in/news-updates/no-political-ads-without-pre-certification-code-of-conduct-iamai-and-social-networking-sites-eci-bombay-hc-143471>>
- Rajesh Serupally, 'Are Political Consultancies a threat to Indian Democracy?' (The Wire, 17 June 2019) <<https://thewire.in/politics/elections-2019-political-consultants-democracy>>
- Snigdha Poonam and Samarth Bansal, 'Misinformation is endangering India's Elections' (The Atlantic, 01 April 2019) <<https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/>>
- Vasudev Devadasan, 'Fake News and the Constitution' (Indian Constitutional Law and Philosophy, 17 June 2020) <<https://indconlawphil.wordpress.com/2020/06/17/fake-news-and-the-constitution/>>

- Zachary Young, ‘French Parliament passes law against ‘fake news’’ (Politico, 04 July 2018) <
<https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/>>

Statutes and Rules

- Constitution of India, 1949
- Indian Penal Code, 1860
- Representation of People’s Act, 1951
- Information Technology Act, 2000
- Information Technology (Intermediary guidelines and Digital Media Ethics Code) Rules 2021, G.S.R. 139(E)
- Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Federal Law Gazette I, p. 3352 ff. (1 October 2017)
- Organic Law No. 2018-1201 of 22 December 2018 Regarding the Fight Against Information Manipulation

