Page 632- 651 **DOI:** *https://doij.org/10.10000/IJLMH.1111049*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 6

2025

Balancing Liberty and Regulation: The Constitutional Paradox of Fake News Laws in India

DR. JAKEY KHAN[1]

ABSTRACT

In 2018, India's Prime Minister cautioned that "fake news has the power to finish democracy," underscoring the gravity of disinformation in the world's largest democracy. Recent statistics reinforce this concern: India continues to lead globally with over 150 internet shutdowns in 2023, while social media companies reported receiving more than 6,000 government takedown requests. At the same time, independent fact-checkers revealed that false narratives around elections, communal tensions, and public health routinely reached millions of users within hours. This dual reality presents a constitutional dilemma as to whether regulatory interventions truly safeguard democracy or imperil the very rights they claim to protect. This paper critically examines the extent to which India's statutory and regulatory interventions against "fake news," particularly the Information Technology Act, 2000, the IT Rules, 2021, and allied criminal provisions, represent necessary and proportionate restrictions under the Constitution. Anchored in the guarantees of freedom of speech and expression (Article 19(1)(a)), privacy (Article 21), and the implicit right to know, the analysis engages with the proportionality doctrine as developed in Modern Dental College, Shreya Singhal, and Puttaswamy. The findings reveal a paradox: interventions intended to protect democratic order often generate overbroad and arbitrary restrictions. Instances of Section 66A's misuse even after being struck down, opaque blocking orders, and government-controlled fact-checking bodies illustrate how regulation can chill speech, erode privacy, and narrow public access to contested information. The researcher recommends a recalibration of India's approach by establishing independent fact-checking bodies, embedding judicial oversight in content takedown processes, mandating transparency and accountability in platform governance, and aligning domestic law with international human rights standards. Only such reforms can ensure that efforts to combat disinformation do not themselves undermine the fundamental freedoms that sustain India's democracy.

Keywords: *Fake News, Freedom of Speech and Expression, Right to Privacy, Right to Know, Proportionality Doctrine, Digital Regulation, Human Rights Framework*

[1] Author is the Principal (In Charge) at J.B. Law College, India,

 [ISSN 2581-5369]

I. INTRODUCTION

In the contemporary digital age, the phenomenon of "fake news" and online disinformation has emerged as one of the most pressing challenges to democratic societies. In India, a country with over 880 million internet users and one of the largest social media populations in the world, the spread of false and misleading content has profound social, political, and legal consequences.[2] The Indian Prime Minister's 2018 warning that fake news possesses "the power to finish democracy" was not rhetorical hyperbole but a reflection of the real risks disinformation poses to electoral integrity, social cohesion, and public order.[3] The COVID-19 pandemic further revealed the scale of the crisis, where misinformation about vaccines and public health measures spread faster than official clarifications, amplifying distrust and confusion.[4] Against this backdrop, regulatory interventions have proliferated, with successive governments introducing statutory and administrative measures to combat the digital spread of falsehoods. However, this regulatory zeal has raised difficult constitutional questions about whether such interventions strike an appropriate balance with the fundamental rights guaranteed under Part III of the Constitution.

The Indian legal landscape reflects a growing reliance on statutory controls over online content. The Information Technology Act, 2000, and particularly the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have placed significant obligations on intermediaries, including content takedown mechanisms, traceability requirements, and the controversial establishment of government-appointed fact-checking units. Parallel criminal provisions under the Indian Penal Code and the recently enacted Bharatiya Nyaya Sanhita, 2023, continue to criminalise the dissemination of false or misleading information under broad categories such as public order, national security, or decency and morality. Together, these legal instruments are intended to curb disinformation, but they have also been critiqued for vagueness, overbreadth, and susceptibility to misuse. Judicial interventions, such as the landmark decision in *Shreya Singhal v. Union of India* (2015)[5], which struck down Section 66A of the IT Act for violating Article 19(1)(a), underscore the tension between state efforts to regulate online speech and the constitutional imperative to safeguard free expression.

---

[2] Md Sayeed Al-Zaman, 'Social Media Fake News in India' (2021) 9 Asian Journal for Public Opinion Research 25.

[3] 'India PM Narendra Modi Overturns Ministry Crackdown on Fake News' <https://www.bbc.com/news/world-asia-india-43625643> accessed 21 October 2025.

[4] Maria Mercedes Ferreira Caceres and others, 'The Impact of Misinformation on the COVID-19 Pandemic' (2022) 9 AIMS Public Health 262 <https://pmc.ncbi.nlm.nih.gov/articles/PMC9114791/> accessed 21 October 2025.

[5] Shreya Singhal v. Union of India (2015) 5 SCC 1

 [ISSN 2581-5369]

This tension gives rise to a deeper paradox. On one hand, combating disinformation is framed as a democratic necessity, essential to preserving electoral integrity, protecting vulnerable communities from communal violence, and ensuring access to reliable information in matters of public health and safety. On the other hand, the very measures adopted to address these concerns often risk undermining the same democratic values they are meant to protect. Mandatory traceability requirements infringe upon the right to privacy recognised in *Justice K.S. Puttaswamy v. Union of India* (2017)[6]. Government-controlled fact-checking units raise legitimate apprehensions about censorship and chilling effects on the press. Opaque and executive-driven blocking orders under Section 69A of the IT Act deprive citizens of the "right to know," a judicially recognised facet of Article 19(1)(a) articulated in cases such as *Union of India v. Association for Democratic Reforms* (2002)[7]. Thus, India's approach to regulating fake news reveals a constitutional paradox where measures designed to strengthen democracy may, in practice, erode its foundational freedoms.

The central aim of this paper is to interrogate whether India's current statutory and regulatory framework on fake news satisfies the constitutional tests of necessity and proportionality. Drawing upon doctrinal analysis of constitutional rights, statutory interpretation, and comparative perspectives from the European Union, the United Kingdom, and the United States, this research seeks to assess whether India's interventions conform to internationally recognised human rights standards. The paper also seeks to highlight the risks of over-criminalisation and executive overreach by examining concrete instances of misuse, including the persistence of Section 66A prosecutions years after its invalidation. In doing so, the study engages with the broader question of how democracies can effectively combat the harms of disinformation without dismantling the liberties that form the essence of democratic governance.

This inquiry is significant not only in the Indian context but also in the global discourse on regulating online platforms. India, as the world's largest democracy and digital market, represents a test case for how emerging economies balance liberty and regulation in the face of digital disruption. The findings of this paper suggest that unless carefully recalibrated, India's legal framework may set precedents that normalise disproportionate restrictions, thereby weakening the constitutional fabric. The paper ultimately argues for a rights-respecting recalibration: independent fact-checking institutions insulated from government control, judicial oversight of takedown orders, transparent accountability mechanisms, and public digital literacy initiatives. Only such reforms can resolve the constitutional paradox and enable India to confront

[6] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
[7] Union of India v. Association for Democratic Reforms (2002) 5 SCC 294

 [ISSN 2581-5369]

the menace of fake news without sacrificing the freedoms that sustain its democratic order.

Statement of Problem

The rapid spread of fake news and online disinformation in India has prompted the state to adopt statutory and regulatory measures such as the IT Act, 2000, the IT Rules, 2021, and allied criminal provisions. While these interventions are intended to safeguard democracy, public order, and access to reliable information, they raise serious constitutional concerns. The problem lies in whether such measures constitute necessary and proportionate restrictions under Articles 19(1)(a), 21, and the implicit right to know, or whether they paradoxically undermine the very human rights framework they seek to protect.

Objectives of Research

The primary objective of this research is to critically examine the constitutional implications of India's statutory and regulatory interventions against fake news and online disinformation. It seeks to analyse the scope of fundamental rights under Articles 19(1)(a) and 21, with particular focus on freedom of speech, privacy, and the implicit right to know, and to evaluate whether the existing framework satisfies the test of necessity and proportionality. The study also aims to explore the paradox wherein measures intended to protect democracy may themselves erode democratic freedoms. In doing so, it strives to provide informed recommendations for recalibrating India's regulatory approach, ensuring that responses to disinformation remain effective, proportionate, and aligned with constitutional and international human rights standards.

II. CONSTITUTIONAL FRAMEWORK OF RIGHTS

The Indian Constitution lays down a robust framework of fundamental rights, within which any attempt to regulate speech, information, or privacy must be evaluated. In the context of fake news and online disinformation, three rights stand out as being directly implicated: the freedom of speech and expression under Article 19(1)(a), the right to privacy under Article 21, and the right to know, which the Supreme Court has recognised as an implicit extension of Article 19(1)(a).[8] These rights are not merely individual entitlements but form the lifeblood of democracy, ensuring that citizens have the liberty to express, the autonomy to make personal choices, and the information necessary to participate meaningfully in the democratic process. Any state measure that restricts or interferes with these rights, whether in the name of combating misinformation or protecting public order, must therefore withstand rigorous constitutional

[8] State of Uttar Pradesh v. Raj Narain AIR 1975 SC 2299

 [ISSN 2581-5369]

scrutiny.

The freedom of speech and expression, guaranteed under Article 19(1)(a), has long been recognised by the Supreme Court as the cornerstone of Indian democracy. From its earliest judgments such as *Romesh Thappar v. State of Madras* (1950)[9] and *Brij Bhushan v. State of Delhi* (1950)[10], the Court has underlined that free expression is essential to the functioning of democracy and that any restriction upon it must be carefully justified. The Court has also extended this freedom to encompass the liberty of the press in *Indian Express Newspapers v. Union of India* (1985)[11], acknowledging the press as a vital vehicle for disseminating information and acting as a watchdog on state power. Yet this freedom is subject to the reasonable restrictions enumerated in Article 19(2), which include grounds such as public order, sovereignty, and decency. The problem arises when the state invokes these grounds too broadly or too vaguely, thereby undermining the very essence of the right. This was starkly illustrated in *Shreya Singhal v. Union of India* (2015)[12], where the Supreme Court struck down Section 66A of the IT Act, 2000 for its overbroad language that criminalised online speech deemed "grossly offensive" or "menacing." The Court observed that such vague terms had a chilling effect on free expression and opened the door to arbitrary state action. Similarly, in *Bennett Coleman & Co. v. Union of India* (1973)[13], the Court invalidated restrictions on the import of newsprint on the ground that they directly curtailed the freedom of the press. These decisions reinforce the principle that while the state may regulate harmful speech, it cannot do so in a manner that disproportionately restricts legitimate dissent or debate.

The right to privacy, although not expressly mentioned in the Constitution, has been firmly established as a fundamental right under Article 21. The transformative judgment in *Justice K.S. Puttaswamy v. Union of India* (2017)[14] declared privacy as intrinsic to life and liberty, encompassing not only personal autonomy but also informational privacy. In the digital era, where communication and information exchange increasingly take place online, privacy assumes new dimensions. Mandatory traceability requirements under the IT Rules, 2021, which compel messaging platforms to identify the "first originator" of information, directly implicate the right to anonymity and confidentiality. The Supreme Court had earlier addressed similar issues in *People's Union for Civil Liberties v. Union of India* (1997)[15], the Telephone Tapping

[9] Romesh Thappar v. State of Madras AIR 1950 SC 124
[10] Brij Bhushan v. State of Delhi AIR 1950 SC 129
[11] Indian Express Newspapers v. Union of India 1985 SCC (1) 641
[12] Shreya Singhal v. Union of India (2015) 5 SCC 1
[13] Bennett Coleman & Co. v. Union of India AIR 1973 SC 106
[14] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
[15] People's Union for Civil Liberties v. Union of India (1997) 1 SCC 301

 [ISSN 2581-5369]

case, where it held that surveillance without adequate safeguards would amount to an invasion of privacy. Building upon this, *Puttaswamy* laid down a three-part test for any intrusion: there must be a law authorising the restriction, the restriction must pursue a legitimate aim, and the measure must be proportionate to that aim. These principles become critical in evaluating whether India's anti-disinformation measures, which often enable surveillance and monitoring, satisfy constitutional standards.

Closely tied to these rights is the "right to know," which the Court has identified as an indispensable element of freedom of speech. In *State of Uttar Pradesh v. Raj Narain* (1975)[16], Justice Mathew famously observed that the people of this country have a right to know every public act by their public functionaries, since such knowledge ensures accountability in a democracy. This principle was later expanded in *Union of India v. Association for Democratic Reforms* (2002)[17] and *People's Union for Civil Liberties v. Union of India* (2003)[18], where the Court held that voters are entitled to know the antecedents, assets, and liabilities of candidates contesting elections. These judgments not only linked information with electoral democracy but also shaped the enactment of the Right to Information Act, 2005. In the digital era, the right to know extends to unfettered access to diverse viewpoints online. However, this right is increasingly curtailed by opaque executive orders under Section 69A of the IT Act, which empower the government to block content without meaningful transparency. While the Supreme Court in *Shreya Singhal* upheld Section 69A, it stressed that blocking orders must follow due process and provide adequate safeguards. The lack of transparency and overuse of such powers raise serious concerns about whether citizens are being deprived of their constitutionally recognised right to know.

Importantly, these rights like the right to freedom of expression, privacy, and the right to know, are interrelated and mutually reinforcing. Free expression allows citizens to voice dissent, privacy enables them to exercise that expression without fear of reprisal, and the right to know equips them with the information necessary to make choices in public life. Curtailing one inevitably affects the others. This interdependence has been recognised in *Anuradha Bhasin v. Union of India* (2020)[19], where the Supreme Court held that indefinite internet shutdowns are unconstitutional and that any restriction on internet access must be temporary, proportionate, and subject to review. The Court acknowledged that in the modern era, freedom of speech and

[16] State of Uttar Pradesh v. Raj Narain AIR 1975 SC 2299
[17] Union of India v. Association for Democratic Reforms (2002) 5 SCC 294
[18] People's Union for Civil Liberties v. Union of India (2003) 4 SCC 399
[19] Anuradha Bhasin v. Union of India AIR 2020 SC 1308

trade through the internet has constitutional protection and cannot be suspended arbitrarily. This judgment resonates strongly in light of India's global reputation as the country with the highest number of internet shutdowns, often justified on grounds of curbing disinformation but frequently criticised as disproportionate and overreaching.

The constitutional framework of rights in India strongly favours liberty and democratic participation. The freedom of speech under Article 19(1)(a), the right to privacy under Article 21, and the right to know as part of Article 19(1)(a) together create a shield against arbitrary state action. Jurisprudence from *Romesh Thappar* to *Puttaswamy* and *Anuradha Bhasin* underscores the principle that restrictions must always be necessary, proportionate, and accompanied by procedural safeguards. When viewed against this framework, regulatory measures against fake news that are vague, overbroad, or intrusive not only risk violating individual rights but also destabilise the very democratic order they are designed to protect.

III. STATUTORY AND REGULATORY INTERVENTIONS IN INDIA

India's regulatory response to the menace of fake news and disinformation has evolved through a patchwork of statutes, executive rules, and judicially endorsed mechanisms. Unlike the European Union's Digital Services Act or the United Kingdom's Online Safety Act, India does not yet have a dedicated statute on fake news. Instead, the legal framework relies on older provisions of the Indian Penal Code (now replaced by the Bharatiya Nyaya Sanhita, 2023), the Information Technology Act, 2000, and sector-specific regulatory bodies such as the Press Council of India and the Ministry of Information and Broadcasting. This fragmented architecture raises questions of coherence, proportionality, and adequacy in addressing the digital disinformation challenge.

The Information Technology Act, 2000 (IT Act) remains the backbone of India's digital governance regime. Section 69A of the Act empowers the government to block access to online content in the interest of sovereignty, security, public order, or decency. The Supreme Court in *Shreya Singhal v. Union of India* (2015)[20] upheld the constitutionality of Section 69A but stressed that its use must follow due process and be accompanied by procedural safeguards. Despite this, blocking orders have frequently been criticised for opacity, with little transparency on the criteria or rationale used. Notably, the now-struck down Section 66A of the IT Act, which criminalised offensive and menacing online speech, demonstrated how vague provisions could be weaponised against journalists and dissenters; its misuse continued even after the Supreme Court invalidated it, revealing the enduring institutional impulse toward over-regulation. In

[20] Shreya Singhal v. Union of India (2015) 5 SCC 1

 [ISSN 2581-5369]

addition, Section 79 of the IT Act provides conditional safe harbour to intermediaries, contingent on their due diligence in removing unlawful content, a provision that has been substantially reinterpreted by subsequent rule-making.

The most significant policy innovation in recent years has been the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under the IT Act. These Rules impose stringent obligations on social media intermediaries, digital news publishers, and OTT platforms.[21] Large intermediaries are required to establish grievance redressal mechanisms, appoint nodal officers, and enable traceability of the "first originator" of content such as an obligation that platforms like WhatsApp have challenged for its potential to break end-to-end encryption and violate privacy rights.[22] The Rules also empower the Ministry of Information and Broadcasting to regulate digital news publishers through a three-tier grievance redressal structure, which critics argue compromises editorial independence.[23] Most controversially, in April 2023, the government amended Rule 3(1)(b)(v) to authorise a government-notified fact-checking unit to identify and require the removal of "fake or false or misleading" content relating to the business of the Central Government.[24] This provision has been widely condemned as executive censorship cloaked in the language of regulation, raising fears of chilling effects on journalism and critical commentary.

Parallel to the IT framework, criminal law provisions have historically been used to prosecute disinformation. Under the Indian Penal Code, 1860 which is now repealed and replaced by the Bharatiya Nyaya Sanhita (BNS), 2023 various sections penalised the spread of false or inflammatory information. Section 153A (Section 196 BNS) criminalised promotion of enmity between groups, Section 295A (Section 299 BNS) penalised deliberate acts intended to outrage religious feelings, Section 505 punished statements conducing to public mischief, and Section 124A (Deleted under BNS) imposed sedition charges for speech against the State. The BNS largely retains and, in some respects, strengthens these provisions, with Section 113 criminalising speech that incites enmity and Section 150 addressing false statements prejudicial to national security and public order.[25] These broad provisions, though not explicitly drafted for

[21] 'The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' <https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> accessed 25 October 2025.

[22] 'How the Intermediaries Rules Are Anti-Democratic and Unconstitutional.' <https://internetfreedom.in/intermediaries-rules-2021/> accessed 25 October 2025.

[23] 'Govt Reaffirms Commitment to Creative Freedom, Enforces OTT Oversight via IT Rules, 2021; Three-Tier Grievance Redressal Mechanism in Place to Regulate OTT Content' <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152954> accessed 25 October 2025.

[24] 'Challenge to the IT Rules 2023 - Supreme Court Observer' <https://www.scobserver.in/cases/challenge-to-the-it-rules-2023/> accessed 26 October 2025.

[25] 'Criminal Law Bills 2023 Decoded: Implications of Criminalising False and Misleading Information Under BNS

fake news, are often invoked to prosecute those accused of spreading disinformation, particularly during communal unrest or political agitation. The inherent vagueness of terms like "mischief" or "false statements" heightens the risk of arbitrary application, making them susceptible to abuse against journalists, activists, and political opponents.

Sector-specific regulators also contribute to the anti-disinformation landscape. The Press Council of India Act, 1978 empowers the Press Council to censure newspapers or journalists for spreading fake or inaccurate information, though its jurisdiction is limited to print media and it lacks enforcement teeth.[26] The Cable Television Networks (Regulation) Act, 1995 authorises the Ministry of Information and Broadcasting to regulate programme and advertising codes, which are occasionally invoked to penalise news channels for broadcasting misleading or sensationalist content.[27] The Programme Code under the Cable Television Networks Rules prohibits programmes that offend decency, promote communal disharmony, or spread false information, although enforcement remains sporadic and often politically contested. In addition, self-regulatory bodies such as the News Broadcasting & Digital Standards Authority (NBDSA)[28] and the Advertising Standards Council of India (ASCI)[29] play a limited but important role in maintaining ethical standards in news broadcasting and commercial advertising.

India has also relied on executive measures in times of crisis. The frequent use of internet shutdowns, particularly in Jammu & Kashmir and northeastern states, is officially justified as a means of curbing disinformation and preventing unrest. However, the Supreme Court in *Anuradha Bhasin v. Union of India* (2020)[30] held that indefinite suspension of internet services is unconstitutional and that restrictions must satisfy tests of necessity and proportionality. Despite this, India continues to hold the dubious distinction of leading the world in internet shutdowns, reflecting the gap between judicial principles and executive practice. During the COVID-19 pandemic, authorities invoked the Disaster Management Act, 2005 and the Epidemic Diseases Act, 1897 to combat misinformation, issuing advisories to social media

2023 ' <https://p39ablog.com/2023/10/criminal-law-bills-2023-decoded-9-implications-of-criminalising-false-and-misleading-information-under-bns-2023/> accessed 26 October 2025.

[26] 'Regulation of Media in India - A Brief Overview' <https://prsindia.org/theprsblog/regulation-of-media-in-india-a-brief-overview?page=49&per-page=1> accessed 26 October 2025.

[27] 'An Analysis of The Cable Television Networks (Regulation) Act, 1995 ' <https://blog.ipleaders.in/an-analysis-of-the-cable-television-networks-regulation-act-1995/> accessed 26 October 2025.

[28] 'Objects and Functions of NBSA - News Broadcasters & Digital Association' <https://www.nbdanewdelhi.com/objects-and-functions-of-nbsa> accessed 26 October 2025.

[29] 'What Is the Advertisement Standards Council of India (ASCI) and What Does It Do ' <https://blog.ipleaders.in/advertisement-standards-council-india-asci/> accessed 26 October 2025.

[30] Anuradha Bhasin v. Union of India (2020) 3 SCC 637

 [ISSN 2581-5369]

platforms to take down false content relating to public health.[31] While these interventions were arguably necessary in a public health emergency, they also demonstrated the state's increasing reliance on executive directives to regulate digital speech.

Complementing statutory law, India has also attempted to institutionalise a soft regulatory approach through the Press Information Bureau's Fact Check Unit (PIB FCU), established in 2019 to debunk false information relating to the government.[32] While this initiative has contributed to public awareness, its extension into a statutory authority under the IT Rules 2021 (via government-notified fact-checking powers) has raised concerns about concentration of power, executive bias, and lack of independent oversight.

The Digital Personal Data Protection Act, 2023, (DPDP Act) enacted on 11 August 2023, marks India's first dedicated parliamentary statute addressing digital personal data processing by recognizing both the individual's right to data protection and the state's legitimate interest in processing such data for "lawful purposes".[33] Unlike earlier regulatory frameworks limited to offline or sector-specific data, the Act applies to "digital personal data" processed in India, including data collected in digital form or digitized later. Core to the statute are duties placed on "data fiduciaries" (those who determine the purpose and means of processing) and "data processors", as well as rights granted to "data principals" (individuals whose data is processed) such as access, correction, erasure, porting, and objection. The framework is built on seven key processing principles consent, purpose-limitation, data minimization, accuracy, storage limitation, reasonable security safeguards, and accountability, drawing upon international norms.[34] Notable innovations include the establishment of the Data Protection Board of India (for adjudication of data breach complaints and imposition of penalties), the concept of "consent managers" (entities facilitating user consent exercise), and the imposition of significant financial penalties (including fines up to ₹200 crore+ for breaches relating to children's data or failure to notify breaches) to give the statute teeth. The Act also contains more stringent safeguards for children's data (requiring parent/guardian consent, banning behavioural monitoring and targeted advertising in respect of children) and tighter controls over cross-border data transfers, reflecting growing concerns about global data flows and minors' protection.

[31] 'Measures Taken in India to Deal with Fake News amidst Covid-19 Outbreak' <https://blog.ipleaders.in/measures-taken-in-india-to-deal-with-fake-news-amidst-covid-19-outbreak/> accessed 26 October 2025.
[32] 'Press Information Bureau - Fact Check Unit' <https://www.pib.gov.in/FAQ_fact.aspx> accessed 26 October 2025.
[33] 'The Digital Personal Data Protection Act, 2023' <https://www.lloydlawcollege.edu.in/blog/digital-personal-data-protection-act-2023.html> accessed 26 October 2025.
[34] 'Seven Principles of the Digital Personal Data Protection Act,2023' <https://amlegals.com/seven-principles-of-the-digital-personal-data-protection-act2023/> accessed 26 October 2025.

 [ISSN 2581-5369]

However, the DPDP Act also includes broad exemptions like processing necessary for enforcing legal rights/claims, for courts or tribunals, for investigation of offences, or in connection with company restructurings may be exempted.[35] The DPDP Act has relevance in two critical ways. Firstly, it imposes stronger obligations on intermediaries and platforms handling personal data, which may intersect with regulation of social media, traceability, originator identification and content moderation; secondly, the law's interplay with privacy and informational autonomy creates an additional constitutional layer, any regulation of online content which involves personal data processing must navigate this new data-protection regime. In short, the DPDP Act significantly expands India's regulatory architecture in the digital domain and its implications for free expression, privacy, and information access warrant careful examination in the context of combating misinformation.

India's regulatory landscape against fake news is sprawling, covering the IT Act and Rules, criminal statutes under the IPC and now the BNS, sector-specific laws like the Cable Television Networks Act and Press Council Act, as well as executive orders and advisories under special legislation like the Disaster Management Act. The framework is marked by overlapping jurisdictions, expansive executive discretion, and limited safeguards for transparency or accountability. While these measures reflect the state's commitment to addressing disinformation, they often blur the line between legitimate regulation and unconstitutional restriction. Their vagueness, overbreadth, and reliance on executive control risk undermining the very freedoms like speech, privacy, and the right to know that the Constitution is meant to protect.

IV. COMPARATIVE INTERNATIONAL FRAMEWORK (EU, UK, US, UN/OHCHR)

Across jurisdictions, the dominant trend is to regulate the systems that amplify disinformation recommendation algorithms, ad targeting, reporting and redress, rather than to criminalise "fake news" as a speech category. The European Union's Digital Services Act (DSA) is the most architected expression of this shift. It imposes tiered duties on intermediaries and, for "very large online platforms" (VLOPs) and search engines, requires annual systemic-risk assessments and mitigation specifically for risks to civic discourse and electoral processes (where disinformation is treated as harmful but often *lawful* speech).[36] The DSA couples these obligations with strong transparency duties (e.g., ad libraries, data access for vetted researchers,

[35] 'Digital Personal Data Protection Act, 2023 DPDPA SECTION 17 WITH INTERPRETATION' <https://dpdpa.com/dpdpa2023/chapter-4/section17.html> accessed 28 October 2025.

[36] 'The EU's Digital Services Act' <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 28 October 2025.

auditability) and empowers the European Commission to enforce directly against VLOPs, including through formal proceedings and potentially fines up to 6% of global turnover.[37] In practice, the Commission has opened cases scrutinising TikTok's ad transparency and systemic-risk mitigation, and has continued public enforcement activity into 2025; independent analyses of first-wave DSA transparency reports show divergent platform taxonomies ("misinformation," "illegal or harmful speech," etc.), underscoring both the DSA's disclosure leverage and the need for methodological convergence to make those reports usable for researchers.[38] Together with the revised (voluntary) Code of Practice on Disinformation, now knitted into DSA compliance expectations, the EU model emphasises *procedural* accountability over speech criminalisation, while preserving room for national criminal laws where content crosses into illegality (e.g., hate speech).

The United Kingdom's Online Safety Act 2023 (OSA) takes a cognate but distinct route: it creates statutory duties of care for user-to-user and search services, enforced by Ofcom via binding codes and enforcement powers. Since late 2024 and into 2025, Ofcom has been rolling out draft and then operative codes, first on illegal content, with platform duties (as of 17 March 2025) to assess risks, implement proportionate safety measures, and remove illegal material rapidly.[39] Although the Act is less explicit than the DSA about "lawful but harmful" disinformation for adults (a politically contested category), parliamentary and regulatory materials emphasise service-level risk assessments, transparency reporting, researcher access, and special protections for children, thereby addressing disinformation's vectors (recommendation engines, virality, provenance) rather than creating a free-standing "fake news" offence.[40] Ongoing UK debates highlight perceived gaps around AI-generated content and the scope of Ofcom's remit, with committees urging stronger action after the 2024 unrest linked to inflammatory online material; the Government has largely maintained that the OSA already covers such risks, while Ofcom's programme focuses on staged implementation. The UK thus represents a compliance-through-systems model, with democratic accountability channelled through a sector regulator rather than through direct ministerial takedown powers.

By contrast, the United States remains anchored in the First Amendment and Section 230's

[37] 'Enforcing the Digital Services Act: State of Play | Epthinktank | European Parliament' <https://epthinktank.eu/2024/11/21/enforcing-the-digital-services-act-state-of-play/> accessed 28 October 2025.
[38] 'Commission Opens Formal Proceedings against TikTok under DSA' <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487?utm_source=chatgpt.com> accessed 28 October 2025.
[39] 'Online Safety Act' https://www.nortonrosefulbright.com/en/knowledge/publications/0b658a5a/online-safety-act <https://www.nortonrosefulbright.com/en/knowledge/publications/0b658a5a/online-safety-act> accessed 28 October 2025.
[40] 'Online Safety Act 2023' <https://www.legislation.gov.uk/ukpga/2023/50?utm_source=chatgpt.com> accessed 28 October 2025.

 [ISSN 2581-5369]

liability shield, producing the most speech-protective baseline of the major democracies. There is no federal statute targeting "disinformation" per se; instead, the constitutional constraint falls on *government pressure* itself. In Murthy v. Missouri (2024)[41], the Supreme Court set aside a broad injunction against federal officials' communications with platforms, holding the plaintiffs lacked standing, but the litigation spotlighted the line between permissible government notification and unconstitutional "jawboning." In practice, US doctrine makes it difficult for the state to compel platforms to remove lawful speech, pushing policy toward transparency, media literacy, and targeted enforcement against clearly illegal categories (fraud, incitement, defamation) rather than a general anti-disinformation law.[42] This model maximises breathing space for speech but leaves systemic amplification challenges largely to platform self-governance and state-level experiments, and it relies heavily on post-hoc remedies rather than ex-ante systems duties.

Council of Europe/ECtHR jurisprudence supplies a useful *rights* counterweight to the EU's regulatory technique. In Delfi AS v. Estonia, the Grand Chamber upheld limited intermediary liability for clearly unlawful user comments in circumstances where the portal retained a degree of control, signalling that proportionate, narrowly tailored liability can be compatible with Article 10 ECHR.[43] More recent ECtHR strands continue to recognise platform responsibilities while warning against overbroad measures that chill public debate, mapping a path where procedural and contextual duties (notice-and-action, responsiveness to manifestly unlawful content) are favoured over blanket censorship. In short, the Strasbourg line complements the DSA's systems-risk logic by insisting that restrictions remain necessity- and proportionality-bound within a robust freedom-of-expression framework.

Finally, UN/OHCHR standards articulate a floor of global best practice: the 2017 Joint Declaration on freedom of expression and "fake news" and the 2021 Special Rapporteur's report on disinformation reject criminalisation of "false news" as a category and urge states to address drivers, opaque curation, concentrated ad markets, data-brokerage, and information vacuums, through transparency, independent oversight, media pluralism, and digital literacy. These instruments press the canonical tripartite test (legality, legitimacy, necessity/proportionality) and caution against state-run "truth ministries," recommending co-regulatory models, auditable platform processes, and safeguards for journalists, researchers, and civil society fact-checkers.[44]

[41] Murthy v. Missouri 548 U.S. 817 (2024)
[42] Jeff Kosseff, 'First Amendment Protection for Online Platforms' (2019) 35 Computer Law & Security Review 105340 <https://linkinghub.elsevier.com/retrieve/pii/S0267364919303103> accessed 2 November 2025.
[43] 'DELFI v. ESTONIA - The Future of Free Speech' <https://futurefreespeech.org/delfi-v-estonia/?utm_source> accessed 2 November 2025.
[44] 'Special Rapporteur on Freedom of Expression and Opinion | OHCHR' <https://www.ohchr.org/en/special-

In operational terms, OHCHR's guidance aligns closely with the EU's systems-accountability paradigm and with UK-style regulator-led schemes, while serving as a reminder, particularly salient for India, that any anti-disinformation regime must be structured to minimise collateral interference with the rights to speak, to receive information, and to enjoy privacy.

V. DOCTRINAL ANALYSIS: NECESSITY AND PROPORTIONALITY

The doctrine of proportionality has become the central analytical tool through which Indian constitutional courts scrutinise restrictions on fundamental rights. Rooted in European and international human rights jurisprudence, proportionality was explicitly adopted into Indian constitutional law in *Modern Dental College v. State of Madhya Pradesh* (2016)[45], where the Supreme Court observed that any restriction on a fundamental right must be balanced against the legitimate aim sought to be achieved by the State. The Court articulated a four-pronged test: first, the measure must pursue a legitimate aim; second, it must be suitable for achieving that aim; third, there must not be any less restrictive but equally effective alternative (the necessity test); and fourth, the measure must strike a proper balance between the rights of the individual and the interests of the community (balancing or proportionality stricto sensu). This doctrinal framework has since been reiterated in *K.S. Puttaswamy v. Union of India* (2017)[46], which elevated privacy to the status of a fundamental right and clarified that all state intrusions into privacy must meet the legality, necessity, and proportionality standards. The *Puttaswamy* judgment in particular laid down that the means adopted by the State must be the least intrusive and proportionate to the object pursued, creating a strong shield against arbitrary digital surveillance and data-retention regimes.

When applied to India's regulatory interventions against fake news, the proportionality doctrine exposes deep constitutional vulnerabilities. The legitimacy of the aim is largely uncontested: countering disinformation to safeguard democracy, public order, and public health is undoubtedly a pressing state interest. Yet, the second prong, suitability, raises difficult questions about whether current measures are empirically effective. For instance, internet shutdowns, often justified as tools to curb rumours and fake news, have been shown to be ineffective in actually preventing misinformation; instead, they disrupt livelihoods, impede access to essential services, and even fuel rumours in the absence of official channels of communication. In Anuradha Bhasin v. Union of India (2020)[47], the Supreme Court stressed that suspension of

procedures/sr-freedom-of-opinion-and-expression/resources?utm_source> accessed 2 November 2025.

[45] Modern Dental College v. State of Madhya Pradesh (2016) 7 SCC 353

[46] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

[47] Anuradha Bhasin v. Union of India (2020) 3 SCC 637

 [ISSN 2581-5369]

internet services must be temporary, proportionate, and subject to judicial review, signalling judicial unease with blanket restrictions that fail the suitability test. Similarly, empowering a government-appointed fact-checking unit to declare content "false" may serve the stated aim of combating disinformation, but it creates a risk of executive overreach and bias, undermining the legitimacy of the process.

The necessity test requires the State to adopt the least restrictive measure available. Here, many provisions of the Information Technology Rules, 2021, and criminal law provisions under the Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023) falter. Criminalising disinformation under broad categories such as "statements conducing to public mischief" or "false statements prejudicial to national security" imposes harsh restrictions on speech when less intrusive measures, such as independent fact-checking partnerships, transparent labelling of contested content, or co-regulation with platforms, would suffice. In *Shreya Singhal v. Union of India* (2015)[48], the Court's striking down of Section 66A was precisely on the ground that the provision was vague, overbroad, and unnecessary, given that existing penal laws already addressed incitement and defamation. By analogy, the creation of overlapping offences against "false" or "misleading" information today appears unnecessary when narrower provisions against incitement, hate speech, or fraud already exist. The persistence of such duplication suggests a failure of the State to respect the necessity limb of proportionality.

The final limb balancing asks whether the overall intrusion into fundamental rights is justified by the benefit to public interest. In this dimension, the chilling effect of India's fake news regulation becomes stark. Mandatory traceability requirements under the IT Rules, 2021, for example, compromise user privacy and weaken encryption, undermining the autonomy and security of millions of users. Even if the aim is to identify originators of harmful content, the impact is disproportionately borne by all users whose communications are subjected to potential surveillance. Similarly, opaque blocking orders under Section 69A of the IT Act compromise the right to know by denying citizens access to contested information without disclosure of reasons or the opportunity to challenge decisions. The Supreme Court has long cautioned against such overreach: in *S. Rangarajan v. P. Jagjivan Ram* (1989)[49], it emphasised that restrictions on speech must be necessary to prevent a "clear and present danger" and not merely speculative harms. Current Indian practice, however, often imposes restrictions pre-emptively, tipping the balance against liberty rather than in its favour.

[48] Shreya Singhal v. Union of India (2015) 5 SCC 1
[49] *S. Rangarajan v. P. Jagjivan Ram* 1989 (2) SCC 574011

 [ISSN 2581-5369]

Comparatively, proportionality review in other jurisdictions reinforces this critique. The European Court of Human Rights in *Delfi AS v. Estonia*[50] upheld limited intermediary liability only in circumstances where content was manifestly unlawful and safeguards were in place, highlighting that broad state powers without procedural protections are incompatible with Article 10 of the European Convention. Similarly, the German Federal Constitutional Court in *Lüth* (1958)[51] and later in cases on internet surveillance has consistently required strict balancing to protect free expression and privacy. The UN Human Rights Committee, in its General Comment No. 34 on freedom of expression, has stressed that restrictions must be necessary and proportionate to a legitimate aim, and laws criminalising "false news" are inherently prone to abuse.[52] Against this backdrop, India's reliance on executive fact-checking units, criminal sanctions, and internet shutdowns appears both overbroad and under-protected.

VI. FINDINGS AND ANALYSIS

The examination of India's statutory and regulatory framework on fake news and online disinformation reveals a troubling pattern: while the stated objectives of these measures are legitimate and aligned with the democratic imperative to safeguard public order, electoral integrity, and public health, the manner in which they are crafted and implemented often undermines constitutional guarantees. The analysis shows that India's interventions pass the first limb of the proportionality test—that of pursuing a legitimate aim—but falter on suitability, necessity, and balancing. The result is a paradoxical framework that claims to protect rights while in practice eroding them.

First, it is evident that the freedom of speech and expression under Article 19(1)(a) suffers from vague, overbroad, and duplicative provisions. Criminal law offences under the Indian Penal Code and the Bharatiya Nyaya Sanhita penalise "false" or "mischievous" statements without precise definitions, creating space for arbitrary enforcement. The misuse of Section 66A of the IT Act, even after its judicial invalidation in *Shreya Singhal v. Union of India* (2015), exemplifies how laws framed to target harmful speech can instead be wielded against journalists, activists, and dissenters. This overbreadth produces a chilling effect on speech, leading citizens to self-censor out of fear of reprisal, thereby undermining the vibrancy of democratic discourse.

[50] Delfi AS v. Estonia [2015] ECHR 586

[51] 'The Lūth Case, 7 BVerfGE 198 (1958): Case Brief Summary | Quimbee' <https://www.quimbee.com/cases/the-luth-case> accessed 2 November 2025.

[52] 'General Comment No.34 on Article 19: Freedoms of Opinion and Expression | OHCHR' <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and> accessed 2 November 2025.

Second, the right to privacy under Article 21 is compromised by regulatory requirements such as mandatory traceability under the IT Rules, 2021. While justified as a means of tracking the origin of viral disinformation, traceability fundamentally undermines encryption, thereby exposing all users to potential surveillance. This fails the necessity test because less intrusive alternatives, such as metadata-based investigations or voluntary disclosure upon judicial order, are available. Instead of narrowly targeting harmful actors, the regulation imposes a systemic intrusion into the privacy of millions of law-abiding users, thereby overbalancing state interests against individual autonomy.

Third, the right to know, an essential facet of Article 19(1)(a), is frequently compromised through opaque executive blocking powers under Section 69A of the IT Act. While the Supreme Court upheld this provision in *Shreya Singhal*, it insisted on procedural safeguards such as reasoned orders and limited scope. In practice, however, blocking orders are often secretive and non-transparent, leaving citizens uninformed about the nature of the restricted content or the grounds of its removal. This lack of transparency corrodes public trust, restricts access to diverse viewpoints, and undermines the electorate's ability to make informed decisions. The paradox is that a mechanism designed to protect citizens from harmful disinformation often results in depriving them of valuable information, including journalistic reporting that is inconvenient to the State.

Fourth, the reliance on internet shutdowns as a blunt instrument of regulation highlights the gap between judicial principle and executive practice. Despite the Supreme Court's ruling in *Anuradha Bhasin v. Union of India* (2020) that indefinite suspensions are unconstitutional, India continues to lead the world in internet shutdowns. Evidence shows that such shutdowns are ineffective in curbing disinformation; rather, they amplify rumours by cutting off access to official clarifications, while simultaneously crippling livelihoods, education, and health services. This illustrates not only a failure of suitability but also a gross imbalance between the rights of citizens and the aims of the State.

Finally, the institutional design of regulatory interventions exacerbates the paradox. The establishment of government-controlled fact-checking units under the IT Rules raises legitimate concerns about executive overreach. When the State assumes the role of arbiter of truth, the independence of information is compromised, and the risk of censorship increases. Unlike the European Union's Digital Services Act or the United Kingdom's Online Safety Act, which emphasise systemic accountability, independent oversight, and transparency, India's approach relies heavily on executive discretion. This lack of independence and accountability heightens the risk that disinformation regulation will be misused for political ends, thereby weakening the

 [ISSN 2581-5369]

democratic values it purports to protect.

In sum, the findings reveal that India's regulatory framework against fake news is marked by a constitutional paradox: interventions designed to safeguard democracy instead produce overbroad restrictions that chill speech, intrude upon privacy, and obstruct the public's right to know. The analysis underscores the urgent need for recalibration, where legitimate state interests are pursued through proportionate, transparent, and rights-respecting mechanisms. Without such reforms, the regulatory response to fake news risks becoming more dangerous to democracy than the disinformation it seeks to contain.

VII. RECOMMENDATIONS

The analysis of India's current framework to regulate fake news demonstrates that while the objectives pursued are legitimate, the methods employed are constitutionally and democratically problematic. To resolve the paradox of rights restriction and to ensure that interventions against disinformation remain effective yet rights-respecting, India must recalibrate its approach across institutional, procedural, technological, and societal dimensions.

First, there is a pressing need to establish independent fact-checking mechanisms insulated from executive control. A government-appointed fact-checking unit, as envisaged under the IT Rules, 2021, creates the risk of censorship, bias, and misuse against dissent. Instead, India should consider statutory creation of an autonomous and multi-stakeholder fact-checking authority, with representation from civil society, academia, journalists, and technologists. Such a body, much like independent election commissions or information commissions, could function with statutory safeguards ensuring independence, transparency, and accountability. The fact-checking process must be auditable, and its determinations should be subject to judicial review, thereby reducing the risk of arbitrary censorship while still addressing disinformation effectively.

Second, judicial oversight and procedural safeguards must be embedded in blocking and takedown mechanisms. Section 69A of the IT Act empowers the government to block content, but in practice, such orders are often opaque and shielded from public scrutiny. To align with constitutional standards, all blocking orders should be accompanied by written reasons, publicly disclosed wherever possible, and subject to ex post facto review by a judicial or quasi-judicial authority. This would harmonise India's framework with global best practices, such as the EU Digital Services Act, which emphasises transparency and researcher access, and the UK's Online Safety Act, which places systemic duties on platforms while ensuring regulator accountability. Transparency is not a procedural luxury but a constitutional necessity to

 [ISSN 2581-5369]

safeguard the citizen's right to know.

Third, India must move away from criminalisation of disinformation under vague penal provisions and instead adopt proportionate civil remedies and platform-level responsibilities. The experience with Section 66A demonstrates the dangers of vague provisions that invite misuse. Broad criminal sanctions for "false" or "mischievous" statements should be repealed or narrowed, and disinformation that does not meet the threshold of incitement or defamation should not attract penal liability. Civil remedies, including fines, mandated corrections, or platform-driven disclosures, provide more proportionate alternatives. Simultaneously, platforms must be required to establish robust content moderation frameworks, transparency reports, and user appeals mechanisms, ensuring that harmful content is addressed without undue state coercion.

Fourth, the privacy and autonomy of citizens must be safeguarded against disproportionate surveillance measures. The traceability requirement under the IT Rules, 2021, threatens to dismantle encryption and undermine privacy for millions of users. This measure fails the proportionality test and should be withdrawn. Instead, the State should rely on less intrusive methods, such as targeted metadata analysis subject to judicial approval, or collaboration with platforms in exceptional cases where serious crimes are involved. The enactment of the Digital Personal Data Protection Act, 2023, provides an opportunity to integrate data protection principles, such as data minimisation, purpose limitation, and necessity, into content regulation. Any intervention against disinformation must be harmonised with the fundamental right to privacy and the statutory safeguards of the DPDP Act.

Fifth, India should invest in digital literacy and public awareness programmes as long-term structural responses to disinformation. Criminalising speech or shutting down the internet cannot uproot the problem of misinformation, which thrives on low levels of media literacy and high levels of distrust. Digital literacy campaigns, integrated into school curricula and public awareness initiatives, can empower citizens to critically assess information sources and resist disinformation. Comparative experience shows that countries which have invested in media literacy and fact-checking partnerships, such as Finland and Taiwan, have achieved greater resilience to fake news than those that rely solely on punitive state interventions.

Finally, India must align its regulatory framework with international human rights standards. The UN Human Rights Committee in General Comment No. 34 and the Joint Declarations of UN and regional rapporteurs on freedom of expression have consistently warned against criminalisation of "false news" and emphasised that restrictions must meet the tests of legality,

 [ISSN 2581-5369]

legitimacy, necessity, and proportionality. India, as the world's largest democracy, should set a global example by embedding these standards in its regulatory architecture. This includes adopting sunset clauses for emergency measures such as internet shutdowns, requiring periodic legislative review of content regulation policies, and ensuring that independent regulators, not executive ministries, oversee compliance.

Combating fake news in a democracy cannot mean replicating the logic of authoritarian information control. The path forward lies in creating institutions and processes that address disinformation without silencing legitimate expression, in embedding accountability in state action, in safeguarding privacy, and in empowering citizens through literacy and transparency. Only by embracing this rights-respecting recalibration can India resolve the paradox of rights restriction and ensure that its fight against disinformation strengthens, rather than weakens, its constitutional democracy.

VIII. Conclusion

The challenge of regulating fake news and online disinformation in India lies not in the legitimacy of the aim but in the proportionality of the means employed. The analysis shows that while the State is right to recognise disinformation as a serious threat to democracy, social harmony, and public health, the chosen instruments like criminalisation under vague laws, government-controlled fact-checking, opaque blocking orders, mandatory traceability, and frequent internet shutdowns, undermine the very rights they are intended to protect. This creates a constitutional paradox in which the pursuit of democracy's preservation erodes its foundational freedoms of speech, privacy, and the right to know. Comparative global frameworks, from the EU's systemic accountability model to the UN's human rights standards, demonstrate that the more effective and sustainable approach lies in transparency, independence, proportionality, and citizen empowerment rather than executive overreach. India's way forward, therefore, must be to recalibrate its regulatory framework—shifting from punitive to preventive, from opaque to transparent, and from executive-driven to independent and participatory models. Only such a rights-respecting recalibration can resolve the paradox and ensure that the fight against disinformation strengthens, rather than weakens, the democratic order.

*****

 [ISSN 2581-5369]