

State vs. Platforms: Rethinking Who Governs the Digital Public Sphere

Tousifa Shahin¹ 

¹MA Political Science from AMU, Aligarh

Abstract

In India, a WhatsApp rumour has ended lives. A tweet has triggered a sedition case. And a government order has made Twitter briefly vanish from millions of screens. These are not anomalies, they are symptoms of a deeper, unresolved question: in the world's largest democracy, who truly governs what people can say, see, and share online?

This paper examines the tense and often contradictory relationship between the Indian state and digital platforms in shaping the country's public sphere. From the IT Rules of 2021 to repeated internet shutdowns in Kashmir, and from Meta's content moderation failures during communal violence to the rise of WhatsApp as a primary news source for hundreds of millions — India offers a uniquely complex laboratory for understanding how platform power and state authority collide, overlap, and occasionally collude.

The paper argues that neither unchecked state regulation nor unaccountable platform self-governance is adequate for a society as linguistically diverse, politically charged, and digitally unequal as India. What is needed is a governance model rooted in constitutional values — one that protects free expression, holds platforms to public interest standards, and ensures that ordinary citizens, not just governments or corporations, have a meaningful voice in the rules that shape their digital lives.

Keywords: Platform Governance, Digital Public Sphere, IT Rules 2021, Internet Shutdowns, Free Expression, Content Moderation, India

Received: 05/05/2026 | **Accepted:** 30/06/2026 | **Published:** 20/07/2026

Corresponding Author: Tousifa Shahin (ORCID: 0009-0003-2348-1820) | **Email:** toshifashahin53423@gmail.com

© 2026 The Author(s). Published by Allahabad Academic Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

Introduction

There is something deeply unsettling about the way the internet works in India today. On one hand, it has become the nervous system of public life — the space where political opinions are formed, religious identities are asserted, business is conducted, and love is found. On the other hand, it is a space where a rumour forwarded through a family WhatsApp group can get someone lynched, where a satirical tweet can land its author in a police station, and where the government can simply switch off connectivity for an entire region for months at a stretch.

India's digital public sphere is not one thing. It is a vast, noisy, multilingual, often contradictory space that stretches from the urban professional scrolling through curated Twitter feeds to the first-generation internet user in rural Bihar who gets his news entirely through YouTube videos shared on WhatsApp. These vastly different users inhabit the same platforms, live under the same laws, and yet experience the internet in profoundly different ways. For some, it is a space of liberation — of access to information, of connection across caste and geography, of voices previously consigned to silence finally finding an audience. For others, it is a space of surveillance, misinformation, and violence.

The central question this paper wrestles with is one that has no easy answer: who should govern India's digital public sphere, and by what principles? The state argues that it has a legitimate interest in maintaining public order, national security, and social harmony. Platforms argue that they are private companies with their own community standards, operating in complex markets across multiple jurisdictions. And ordinary citizens — the actual inhabitants of this sphere are largely absent from the conversation about its governance. Their interests are invoked constantly, but their voices are rarely heard.

This paper moves through several layers of this problem. It begins by examining what we mean by the digital public sphere and why India presents a particularly distinctive case — a democracy with a constitutional commitment to free expression, yet one that has never fully shed the colonial legacy of sedition laws and executive overreach. It then looks at the evolving regulatory landscape, with particular attention to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, a watershed moment in Indian platform governance. It examines the practice of internet shutdowns, which India leads the world in deploying. It analyses the failures and tensions of platform self-governance, using specific Indian examples. And it concludes by sketching what a more democratic and rights-respecting model of governance might look like.

Throughout, the paper tries to resist the temptation of easy answers. The state is not simply a villain,

and platforms are not simply neutral conduits. The state has genuine obligations — to protect minorities from mob violence, to prevent the weaponisation of disinformation, to ensure the digital economy does not replicate offline hierarchies of power. Platforms, meanwhile, make consequential editorial choices every day, whether or not they acknowledge them as such. The reality is messier, more interesting, and ultimately more open to democratic re imagination than either position suggests.

II. The Digital Public Sphere: What It Is and Why India Is Different

The idea of the public sphere comes from the German philosopher Jürgen Habermas, who described it as a space in democratic societies where private individuals come together to discuss matters of public concern and where, ideally, reason and argument prevail over power and money. For Habermas, the eighteenth-century European coffee house was the prototype: a place where bourgeois citizens could meet as equals and deliberate on political affairs.

The internet, in theory, should be the ultimate realisation of this ideal. It is vast, accessible, decentralised, and borderless. It allows anyone with a smartphone and a data connection to publish, broadcast, and participate in public conversation. And in many ways, it has delivered on this promise. Social media has been instrumental in anti-corruption movements, farmers' protests, climate activism, and countless other forms of civic engagement across the world.

But the actual internet — the one that exists today, dominated by a handful of American technology companies whose algorithms shape what we see, feel, and believe — looks very different from Habermas's ideal. As scholars like Shoshana Zuboff and Safiya Umoja Noble have argued, these platforms are not neutral. They are structured by commercial incentives that reward engagement over accuracy, outrage over nuance, and virality over truth. The public sphere they host is not a space of equal deliberation — it is a space shaped by code, commerce, and concentrated power.

India adds several additional layers of complexity to this picture.

2.1 Scale and Diversity

India has over 950 million internet users, making it the second-largest online population in the world. But this number conceals enormous diversity. India has twenty-two officially recognised languages and hundreds of dialects. The internet in India is not primarily an English-language space — it is a Hindi space, a Tamil space, a Bengali space, an Assamese space, and much more. Most content moderation systems, however, have been built for English. The result is a systematic failure to catch harm-

ful content in Indian languages, which proliferates largely unchecked. This is not merely a technical problem — it is a structural one. When platforms invest minimally in non-English language capacity, they are implicitly making a judgement about whose speech is worth governing carefully and whose is not. For a country as linguistically plural as India, this has serious consequences for public safety and democratic discourse alike..

2.2 Asymmetric Access

While India's internet user base is huge, the digital divide remains stark. Rural and urban access differs significantly, and gender gaps are pronounced — women in rural India are significantly less likely to use the internet than men. This means that the digital public sphere, despite its apparent openness, excludes large segments of the population from meaningful participation. These exclusions are not random; they track existing social hierarchies of class, caste, and gender. The voices that dominate online discourse in India tend to be urban, educated, and male — a demographic profile that shapes what issues get amplified, which grievances are treated as legitimate, and whose version of events becomes the default public narrative. A genuinely democratic digital public sphere would need to reckon seriously with these structural inequalities, not treat access as a problem already solved.

2.3 WhatsApp as Infrastructure

Perhaps most distinctively, WhatsApp has become something close to public infrastructure in India. With over 500 million users, it is where families communicate, small businesses operate, political parties organise, and crucially where news travels. Unlike Twitter or Facebook, WhatsApp is end-to-end encrypted and group-based. This makes it extraordinarily difficult to moderate, trace, or regulate. It also makes it a uniquely potent vehicle for misinformation.

The lynching epidemic of 2017–2019, in which dozens of people were killed by mobs acting on false rumours spread through WhatsApp, remains the most tragic demonstration of how unregulated private communication can translate into public violence. Cases from Jharkhand, Maharashtra, and Karnataka revealed a disturbing pattern: rumours about child kidnappers or cattle thieves would circulate through WhatsApp groups, travel to neighbouring villages in minutes, and mobilise violent mobs before any corrective information could spread. What made these episodes particularly difficult to address was the speed and intimacy of the medium — a message forwarded by a trusted family member or a local religious figure carried a credibility that no government fact-check could easily dislodge. WhatsApp's architecture, designed to protect privacy, had become an accelerant for collec-

tive violence.

This creates a genuine and uncomfortable dilemma for regulators and civil society alike. Weakening encryption or mandating message traceability — as the Indian government has sought to do — would compromise the privacy of hundreds of millions of legitimate users, including journalists, activists, and abuse survivors who depend on secure communication. Yet doing nothing treats the platform’s design choices as beyond democratic scrutiny, even when those choices carry demonstrable costs in human lives. There is no clean answer here, only a set of hard trade-offs that demand honest public deliberation rather than either regulatory overreach or platform indifference.

III. The State and Its Instruments: Law, Rules, and Shutdowns

The Indian state’s relationship with digital platforms has always been ambivalent. On one hand, the government has enthusiastically promoted digital technology as a vehicle for economic growth and democratic participation — from the ambitious Digital India programme to the Unified Payments Interface (UPI), which has made India one of the world’s leaders in digital finance. On the other hand, it has increasingly sought to control the digital space through regulation, censorship, and outright shutdowns.

3.1 The IT Act and Its Evolution

The primary legal framework governing the internet in India is the Information Technology Act, 2000, which was amended substantially in 2008. Section 66A, which criminalised online speech deemed “grossly offensive” or “menacing,” was particularly notorious — it was used to arrest cartoonists, students, and ordinary citizens for posts that politicians found objectionable. In 2015, the Supreme Court struck down Section 66A in the landmark *Shreya Singhal v. Union of India* case, ruling it unconstitutional on grounds of vagueness and over-breadth.

The *Shreya Singhal* judgment was a genuine victory for free expression. But it did not resolve the underlying tension between the state’s desire to control online speech and citizens’ right to speak freely. New instruments of control emerged to fill the gap left by Section 66A.

3.2 The IT Rules of 2021: A Turning Point

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 represent the most significant regulatory intervention in India’s digital landscape since the IT Act itself. Notified in February 2021 in the immediate aftermath of a standoff between Twitter and the

government over content takedown demands — the Rules imposed sweeping new obligations on digital intermediaries.

The key provisions of the 2021 Rules include: a requirement for significant social media intermediaries — those with over five million users to appoint Indian resident grievance officers, compliance officers, and nodal contact persons; a 36-hour window to respond to government takedown orders; and most controversially — a requirement for messaging platforms to enable “traceability,” meaning the ability to identify the first originator of any message that authorities deem harmful.

The traceability provision drew immediate and widespread criticism from technologists, civil society organisations, and legal scholars. End-to-end encryption, which protects the privacy of billions of WhatsApp conversations, cannot coexist with a mandatory traceability requirement — enabling traceability would require building a backdoor into encryption, which would expose all users to potential surveillance. The Internet Freedom Foundation, one of India’s leading digital rights organisations, described the provision as a potential “mass surveillance” mechanism dressed up as a targeted law enforcement tool.

The Rules also created a three-tier grievance redressal framework for digital news media and OTT platforms, requiring them to adhere to a government-approved Code of Ethics. Critics noted that the Code gave the government significant discretion to intervene in editorial decisions — a power that was previously absent from India’s press regulation framework.

Twitter (now X) was perhaps the most public resister to the 2021 Rules. The platform initially refused to appoint the required compliance personnel, citing concerns about freedom of expression. The government responded by stripping Twitter of its safe harbour protections under the IT Act — a move that would have exposed the platform to direct legal liability for all user-generated content. Twitter eventually complied, but the episode revealed the significant coercive power that governments can wield over platforms through the threat of safe harbour withdrawal.

3.3 Internet Shutdowns: The Bluntest Instrument

If the IT Rules represent the regulatory edge of state power over the internet, internet shutdowns represent its bluntest, most brute instrument. (India has, for several years running, been the world’s leading perpetrator of internet shutdowns — a distinction that the government has never seemed particularly troubled by.)

Internet shutdowns in India are authorised under Section 144 of the Code of Criminal Procedure and

the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017. In practice, they are imposed with minimal judicial oversight, often on vague grounds of “public safety” or “law and order,” and frequently remain in force for weeks or months.

Kashmir offers the most extreme case. Following the revocation of Article 370 in August 2019, the Kashmir Valley experienced what is believed to be the longest internet shutdown in the history of any democracy — lasting over 550 days in various forms. During this period, residents were cut off from information, businesses collapsed, students could not access educational resources, and journalists were unable to report. The human cost was immense and largely invisible to the rest of the country.

In *Anuradha Bhasin v. Union of India* (2020), the Supreme Court held that internet access is a fundamental right under Article 19 of the Constitution and that shutdowns must be proportionate, necessary, and subject to judicial review. But the judgment’s practical impact has been limited. Shutdowns have continued during communal tensions in Manipur, during farmers’ protests in Haryana, during exam seasons in Rajasthan. The legal standard of “proportionality” has proven elastic enough to accommodate almost any government justification.

IV. Platforms and Their Failures: The Limits of Self-Governance

If the Indian state’s approach to digital governance is characterised by overreach and bluntness, digital platforms’ approach is characterised by inconsistency and opacity. Platforms like Meta (which owns Facebook, Instagram, and WhatsApp), Google (which owns YouTube), and Twitter have constructed elaborate systems of content moderation — community standards, artificial intelligence filters, human review teams, and oversight bodies. In practice, these systems have failed India repeatedly and in predictable ways.

4.1 The Facebook–Hate Speech Controversy

In August 2020, the Wall Street Journal reported that senior Facebook executives in India had overruled their own policy team’s recommendation to remove posts by a BJP politician that clearly violated the platform’s hate speech policies. The politician, T. Raja Singh, had made statements calling for violence against Rohingya Muslims — content that Facebook’s own reviewers had flagged as dangerous. According to the report, company executives were reluctant to take action because they feared it would damage Facebook’s commercial and regulatory relationships with the ruling party.

The controversy illuminated a structural problem with platform self-governance in politically asymmetric environments: when platforms have significant business interests in a country, and when the

ruling party has significant regulatory power over platforms, truly impartial content moderation becomes extremely difficult. The incentives for platforms to accommodate state pressure, or simply to avoid provoking it are enormous.

Facebook subsequently commissioned a civil rights audit and expanded its local language content moderation capacity. But the fundamental conflict of interest identified in the controversy has not been structurally resolved. A private company cannot simultaneously serve as a neutral forum for public expression and a commercially motivated actor in a high-stakes political economy.

4.2 YouTube and the Misinformation Ecosystem

YouTube is India's most-watched video platform and, for many users, the primary source of news and current affairs information. It hosts content in dozens of Indian languages, much of which is produced by independent creators with little editorial oversight. It has also become a significant vehicle for misinformation, conspiracy theories, and communally inflammatory content.

(The 2023 violence in Manipur, which saw ethnic conflict between the Meitei and Kuki-Zo communities claim over 200 lives and displace tens of thousands,) was accompanied by — and in some ways accelerated by a torrent of inflammatory videos on YouTube and Facebook. Investigators and journalists documented how algorithmically amplified content spread fear, hardened identities, and made reconciliation more difficult. Neither platform had adequate capacity to moderate content in Meitei or Kuki languages.

This language gap is not incidental — it is structural. The economics of content moderation mean that platforms invest most heavily in moderating high-traffic English language content. Smaller language communities are effectively unmoderated. In India, where hundreds of millions of internet users primarily use regional languages, this gap has life-or-death consequences.

4.3 The Oversight Board Experiment

Meta's creation of the Oversight Board — an independent body of academics, lawyers, and former politicians empowered to overrule Meta's content moderation decisions was presented as a bold experiment in platform governance. The Board has issued several significant decisions, including some that touched on Indian cases involving political speech and COVID-19 misinformation.

But critics have noted that the Board's jurisdiction is narrow. It can only review individual posts, not policies or algorithms, its membership reflects Global North perspectives, and its decisions are not always implemented promptly or consistently. It is, at best, a partial and imperfect accountability

mechanism useful for generating publicity, but insufficient as the primary mode of platform governance in a country of India's scale and complexity.

4.4 WhatsApp's Structural Dilemma

WhatsApp occupies a unique and particularly difficult position in India's digital governance landscape. Its end-to-end encryption makes it genuinely private not just from governments, but from Meta itself. This is both its greatest strength (privacy protection) and its greatest weakness (inability to moderate harmful content). The platform has introduced several measures to limit viral spread, capping the number of times a message can be forwarded, labelling frequently forwarded messages but these are partial solutions to a structural problem.

The deeper question is whether a private messaging platform, operating at the scale of public infrastructure, should be subject to different governance norms than a more traditional social media platform. There is a reasonable argument that a platform carrying the communications of 500 million people in a single country has acquired a public character that warrants a different regulatory approach, one that protects both privacy and safety.

V. Constitutional Values and the Governance Deficit

India's Constitution provides a remarkably rich framework for thinking about digital governance, even though it predates the internet by half a century. Article 19(1)(a) guarantees freedom of speech and expression, but Article 19(2) allows the state to impose "reasonable restrictions" on this freedom in the interests of, among other things, public order, decency, morality, national security, and sovereignty. The history of Indian free speech jurisprudence is, in many ways, the history of the struggle to define what counts as a "reasonable restriction."

The Supreme Court's intervention in *Shreya Singhal* established that the state cannot use vague, overbroad restrictions to silence online speech. The *Anuradha Bhasin* judgment established that internet access is a fundamental right. These are significant doctrinal advances. But constitutional values extend beyond free speech — they include equality, dignity, and the right to be free from discrimination and violence. A governance framework that protects speech without addressing the ways in which unregulated speech can threaten dignity and safety is constitutionally incomplete.

5.1 The Missing Middle: Citizens in Governance

One of the most striking features of India's current platform governance landscape is the complete ab-

sence of ordinary citizens from the conversation. The IT Rules were drafted without any meaningful public consultation. Platforms' community standards are written by corporate lawyers in California. The Oversight Board, despite its aspirations to global legitimacy, was constituted without transparent democratic input from the communities it claims to serve.

This democratic deficit is not merely a procedural concern — it has substantive consequences. Rules made without the input of affected communities are less likely to reflect those communities' needs, values, and contexts. A content moderation policy developed without the participation of Dalit activists, Kashmiri journalists, or LGBTQ+ individuals from small towns is unlikely to adequately protect their speech or safety. Governance without representation is, at its core, a form of power exercised without accountability.

5.2 The Equality Dimension

Digital governance in India has a profound equality dimension that is rarely acknowledged in mainstream policy debates. Misinformation and hate speech on digital platforms have disproportionately targeted religious minorities, Dalits, women, and LGBTQ+ individuals. The failure to moderate this content effectively is not a neutral failure — it systematically disadvantages already marginalised groups. A rights-respecting governance framework must take this distributive dimension seriously.

At the same time, government overreach in content moderation has also disproportionately affected marginalised groups. Section 66A was overwhelmingly used against political dissidents, Dalit activists, and critics of the ruling party. Internet shutdowns have fallen most heavily on communities in conflict zones — Kashmir, Manipur, Jharkhand — which are already among the country's most economically and politically vulnerable. Any reform of platform governance must reckon with the state's own record as an actor in digital inequality.

VI. Toward a Democratic Model of Platform Governance

The preceding analysis suggests that both state-centric and platform-centric models of digital governance are inadequate for India. The state's record includes censorship, surveillance, shutdowns, and the weaponisation of law against dissent. Platforms' record includes algorithmic amplification of hatred, inconsistent enforcement, and a fundamental conflict between commercial incentives and public interest values. What is needed is a different model — one that is more democratic, more rights-respecting, and more attentive to India's specific social and political context.

This section sketches the broad outlines of such a model, drawing on emerging thinking in comparative platform law, civil society proposals, and India's own constitutional traditions.

6.1 Statutory Baseline with Constitutional Guardrails

India needs a clear statutory framework for platform governance that is grounded in constitutional values — not just security concerns. Such a framework should establish a baseline of rights that platforms must respect: the right to free expression, the right to privacy, the right to non-discrimination, and the right to effective remedy when these rights are violated. It should establish clear procedural requirements for government takedown demands — including mandatory judicial authorisation for demands affecting large numbers of users — and should create meaningful penalties for platforms that fail to enforce their own stated rules consistently.

Critically, such a framework should contain explicit constitutional guardrails against state overreach. Internet shutdowns should require High Court authorisation and should be subject to automatic sunset clauses. Government takedown demands should be publicly disclosed through a mandatory transparency report. The weaponisation of platform governance mechanisms against political opponents and journalists should be explicitly prohibited and subject to judicial review.

6.2 Independent Regulatory Authority

Content moderation decisions at the scale of Indian social media cannot be effectively reviewed by courts in real time. What is needed is an independent regulatory authority — analogous to the Press Council of India but with genuine enforcement powers — that can review platform decisions, investigate systemic failures, issue binding orders, and impose meaningful financial penalties.

This authority should be structurally independent from both the government and the platforms. Its members should be appointed through a transparent process that involves the judiciary, civil society, and technical experts. It should have the capacity to conduct algorithmic audits — examining not just what content platforms remove, but what content their recommendation systems amplify. And it should be required to produce regular public reports on platform governance in India, in multiple languages.

6.3 Meaningful Public Participation

Democratic platform governance requires meaningful public participation at every stage — from the drafting of rules to their implementation and review. This is not merely a procedural nicety; it is a substantive requirement of the constitutional values at stake. Decisions about what speech is accept-

able in India's digital public sphere are, ultimately, political decisions — and political decisions in a democracy should reflect the views of those affected.

Practical mechanisms for public participation might include: mandatory public consultation processes before major regulatory changes, with adequate notice and accessible formats; representation of civil society and affected communities on regulatory and oversight bodies; and the creation of local digital rights ombudsmen at the state level, who can receive and investigate complaints from ordinary citizens about both government and platform conduct.

6.4 Platform Obligations Calibrated to Risk and Reach

Not all platforms are equal, and not all content poses the same risks. A sensible governance framework should calibrate platform obligations to their actual reach and the actual risks their systems create. Large platforms with more than fifty million Indian users should be subject to the most demanding obligations — including algorithmic transparency, language-specific moderation capacity, and mandatory human review of high-stakes decisions. Smaller platforms, local language applications, and individual creators should face lighter-touch regulation.

Particular attention should be paid to the specific risks posed by messaging platforms like WhatsApp. The balance between privacy (which end-to-end encryption protects) and safety (which traceability might serve) is a genuinely hard problem. The answer is unlikely to be either mandatory backdoors — which would destroy encryption and expose hundreds of millions of users to surveillance — or complete inaction. More promising approaches include digital literacy initiatives, investment in rapid response debunking networks, and greater transparency about how viral content spreads, without compromising individual message privacy.

6.5 Investment in Digital Literacy

No governance framework, however well designed, can substitute for a digitally literate citizenry. India's rapid internet expansion has brought hundreds of millions of first-time users online without adequate preparation for the information environment they encounter.

Investments in digital literacy — not just technical skills, but critical media literacy, the ability to evaluate sources and identify misinformation — are essential complements to regulatory reform.

Civil society organisations, media literacy NGOs, and educational institutions have all developed models for digital literacy education that are contextually appropriate and practically effective. Scaling these initiatives, with government support but without government editorial control, should be a

priority for any serious reform programme.

VII. Conclusion: Democracy's Unfinished Business

The question of who governs India's digital public sphere is, at its heart, a question about the kind of democracy India wants to be. It is a question about whether the promise of the Constitution — free expression, equal dignity, democratic participation — extends to the spaces where public life increasingly happens. And it is a question about power: who has it, how it is exercised, and whether ordinary people have any meaningful say in the rules that shape their digital lives.

This paper has argued that neither the state nor the platforms have provided satisfactory answers to these questions. The state has used its regulatory power to silence dissent, shut down connectivity, and impose opaque obligations on platforms that threaten privacy and free expression. Platforms have built systems that are commercially optimised rather than democratically accountable — systems that amplify harmful content in Indian languages, serve the interests of powerful actors, and exclude ordinary users from governance decisions that directly affect them.

The path forward is not simple. It requires building new institutions — a genuinely independent regulatory authority, participatory rule-making processes, accessible remedy mechanisms — that do not currently exist. It requires platforms to invest seriously in local language moderation and to open their algorithmic systems to external scrutiny. It requires the state to accept meaningful constitutional constraints on its own power to shut down, surveil, and silence. And it requires all of us — citizens, scholars, journalists, activists — to participate in the conversation about what kind of digital public sphere we want.

India's internet is not yet fully formed. The norms, institutions, and power arrangements that will govern it for the next generation are being contested right now — in courtrooms, parliamentary committees, corporate boardrooms, and civil society forums. The stakes could hardly be higher. A digital public sphere that works for India — for all of India, not just its most powerful citizens and institutions — is both possible and worth fighting for.

What India ultimately needs is not a choice between the state and the platforms. It needs a governance model that holds both accountable to the people whose lives and voices they shape.

That is the unfinished business of Indian democracy in the digital age.

Works Cited

1. Anuradha Bhasin v. Union of India. 2020. (2020) 3 SCC 637. Supreme Court of India.
2. Banaji, Shakuntala, and Ramnath Bhat. 2019. "WhatsApp Vigilantes: An Exploration of Citizen
3. Reception and Circulation of WhatsApp Misinformation Linked to Mob Violence in India."
4. London School of Economics and Political Science
5. Bhandari, Vrinda, and Tanaya Bindal. 2020. "Online Speech and the Constitutional Framework in India." Vidhi Centre for Legal Policy. <https://vidhilegalpolicy.in>.
6. Fraser, Nancy. 1990. "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy." *Social Text* 25/26: 56–80.
7. Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press.
8. Gurumurthy, Anita, and Nandini Chami. 2022. "Governing Platforms in the Public Interest: Frameworks for Accountability." IT for Change. <https://itforchange.net>.
10. Habermas, Jürgen. 1989. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: MIT Press.
11. Human Rights Watch. 2019. "Violent Cow Protection in India: Vigilante Groups Attack Minorities." <https://www.hrw.org>.
12. Human Rights Watch. 2023. "India: Ethnic Violence, Displacement in Manipur." <https://www.hrw.org>.
13. Internet and Mobile Association of India. 2023. *Digital in India 2023*. IAMAI. <https://www.iamai.in>.
14. Ministry of Electronics and Information Technology. 2021. "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021." Government of India. <https://www.meity.gov.in>.
15. Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
16. Oversight Board. 2023. "Case Decisions and Policy Advisory Opinions." Meta Oversight Board. <https://www.oversightboard.com>.
17. Shreya Singhal v. Union of India. 2015. (2015) 5 SCC 1. Supreme Court of India.
18. Shrivastava, Preetika, and Newley Ghoshal. 2020. "Facebook India Head of Public Policy Favoured Exemptions for BJP Politician's Hate Speech." *Wall Street Journal*, August 14, 2020.

19. Software Freedom Law Centre. 2021. "Internet Shutdown Tracker India." <https://internetshutdowns.in>.
20. Suzor, Nicolas P. 2019. *Lawless: The Secret Rules That Govern Our Digital Lives.* Cambridge: Cambridge University Press.
21. Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New frontier of Power.* New York: PublicAffairs.