

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 6

2025

© 2025 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Speech Regulation in the Algorithmic Age: An Indian Perspective

DR. ABHIJIT ROHI¹

ABSTRACT

The shift of public discourse onto digital platforms, now curated by algorithms, presents fundamental challenges to free speech under Article 19(1)(a) of the Indian Constitution. With over 800 million internet users, social media is crucial for Indian democratic deliberation. The paper argues that algorithmic governance has destabilized the 'safe harbour' distinction between a 'publisher' and a 'passive conduit'. Modern platforms actively prioritize and amplify content, engaging in a form of automated editorial control that erodes their immunity. This positive control has also rendered the traditional 'push' and 'pull' media classifications redundant, replaced by a 'predictive push' model. India's response, through the IT Rules, 2021, shifts the legal framework to a 'compliance-first' model. This requires 'Significant Social Media Intermediaries' (SSMIs) to exercise 'due diligence' and deploy automated filtering tools. However, this assertive state regulation, coupled with private algorithmic curation, risks a 'chilling effect' through automated censorship and intermediary liability. Key algorithmic practices such as shadow banning, context collapse and bias, personalisation etc. violate constitutional rights. The current Indian 'command-and-control' approach, focused on swift takedowns, contrasts with the systemic oversight and transparency required by the EU's Digital Services Act (DSA). The paper concludes that an 'Indian perspective' must reject both data colonialism and digital authoritarianism, striving for a 'digital constitutionalism' to protect the right to speak, be heard, and dissent

Keywords: *Algorithmic Governance, Safe Harbour, Free Speech, IT Rules, 2021, Automated Censorship*

I. INTRODUCTION

As public discourse increasingly migrates to digital platforms, the governance of speech has shifted from state-centric models to a complex interplay of private algorithmic curation and state-imposed 'due diligence.'

The 'marketplace of ideas' is no longer a physical public square; it is a digitally curated feed. In India, with over 800 million internet users, social media platforms have become the primary

¹ Author is an Assistant Professor (Law) at Maharashtra National Law University Mumbai, Maharashtra, India.

infrastructure for democratic deliberation. However, this infrastructure is not neutral more so in the times when algorithmic governance of free speech is the norm. The governing algorithms are designed to maximize engagement, often prioritizing sensationalism over substance, and by content moderation systems that police speech at a scale impossible for human moderators.

This paper explores the unique challenges of regulating speech in the Indian context, where a diverse, multi-lingual society meets the rigid, often culturally illiterate logic of Silicon Valley algorithms and the increasing assertiveness of the Indian state. India is transitioning from a ‘safe harbour’ regime to a ‘compliance-first’ model. This shift, while ostensibly targeting disinformation and harm, risks creating a ‘chilling effect’ on legitimate expression through automated censorship and the spectre of intermediary liability. This paper examines the regulatory landscape of online speech in India, analysing the tension between the constitutional guarantees of Article 19(1)(a) and the opaque manner of free speech regulation in algorithmic age.

II. CHANGES IN THE ALGORITHMIC AGE

A. Destabilisation of the ‘editorial-control’ requirement of safe harbour

For the first two decades of the commercial internet, the legal architecture of the web rested on a crucial distinction: the difference between a publisher and an intermediary. A publisher, like a newspaper, exercises editorial control and is liable for the content it prints. An intermediary, like a telephone company or an early bulletin board, is a passive conduit and generally lacks liability for the speech of others. This distinction formed the bedrock of ‘safe harbour’ provisions like section 79 of the Information Technology Act, 2000.² These laws shielded platforms from liability for user-generated content (UGC) on the premise that they were neutral hosts.

However, the algorithmic age has fundamentally destabilised this binary. Modern platforms are no longer passive repositories; they are active curators that use sophisticated recommendation engines to rank, boost, and suppress content to maximise user engagement. The algorithmic amplification constitutes a form of automated editorial control that erodes the ‘passive conduit’ rationale of safe harbour. By shifting from merely hosting speech to actively selecting and prioritizing it, platforms have entered a legal grey zone that challenges the sustainability of their

² Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India) (shielding intermediaries, such as social media platforms and internet service providers, from legal liability for third-party information, data, or communication links hosted by them, provided they observe due diligence, act merely as facilitators without modifying the content, and promptly remove unlawful material upon receiving an official government or court order.)

current immunities.

The destabilisation of this framework arises from the distinction between *negative* and *positive* editorial control. Safe harbour laws were designed primarily to protect *negative* control—the removal of illegal or harmful content. However, the business model of the modern web relies on *positive* control—the algorithmic selection of content to show to specific users.³ Algorithms on platforms like TikTok, YouTube, and Facebook do not merely display content chronologically; they make billions of editorial decisions daily. They assess the ‘newsworthiness’ or ‘engagement potential’ of a piece of content and decide whether to amplify it to millions or bury it.⁴ When platforms use algorithms to solicit and purposefully amplify content to keep users glued to the screen, they move beyond the role of a passive host and engage in conduct that resembles a publisher’s discretion.

This shift destroys the neutrality argument. If a newspaper editor places a controversial op-ed on the front page, they own the decision. When an algorithm places a controversial video in the ‘Up Next’ queue, the platform claims it is merely a neutral reflection of user preferences. Is that so? Or is it that the algorithm has become the editor, and its code enforces an editorial policy prioritized for profit over accuracy?

The ‘editorial control’ requirement of safe harbour is currently in a state of collapse. As we move forward, the legal focus is shifting from content liability that is to hold platforms responsible for what users post, to product liability that is to hold platforms responsible for how their algorithms amplify that content. The destabilisation of safe harbour does not necessarily mean the end of a free and open internet, but it signals the end of the era where algorithmic curation is viewed as a neutral, consequence-free technical process.

B. Redundancy of Media classification: Push media and pull media

For decades, media theory and marketing relied on a binary classification to understand content consumption: ‘push’ media and ‘pull’ media. Push media, epitomized by broadcast television and radio, involved a central broadcaster transmitting content to a passive audience. Pull media, on the other hand, required users to actively seek out specific information via search engines or direct navigation. This dichotomy was referred to by the petitioners before the Supreme Court while arguing that higher threshold of tolerance to be attributed to ‘pull’ media.⁵

³ TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET: PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA (2018).

⁴ Dorcas Adisa, *Everything You Need to Know About Social Media Algorithms*, Sprout Social (Oct. 30, 2023), <https://sproutsocial.com/insights/social-media-algorithms/>.

⁵ Apoorva Arora & Anr. v. State (Gov’t of NCT of Delhi) & Anr., 2024 INSC 223.

The algorithmic age while bringing the dominance of machine learning recommender systems has discarded this distinction. Platforms like TikTok, Netflix, and Instagram have engineered a hybrid model where content is neither purely broadcast nor purely requested. Instead, users are subjected to ‘predictive push’: a system where algorithms anticipate user desires and ‘push’ content that the user would have theoretically (or hypothetically) ‘pulled’ themselves. The push/pull dichotomy now appears to be redundant. It is replaced by a paradigm of algorithmic curation where user agency and platform control are inextricably blurred. The shift to a ‘hybrid’ media model where the platforms actively push content users didn’t explicitly pull, fundamentally rewires the legal conception of free speech.

C. Due diligence with regulatory oversight

Historically, the Information Technology Act, 2000⁶ provided intermediaries (platforms like X (formerly Twitter), Facebook, YouTube, etc.) with ‘safe harbour’ protection under Section 79.⁷ This meant platforms were immune from liability for user-generated content, provided they acted as ‘mere conduits’ and removed content upon receiving ‘actual knowledge’ of illegality.⁸ However, the enactment of the IT Rules, 2021 fundamentally altered this landscape.⁹ The Rules introduced a tiered compliance structure, designating platforms with over 5 million users as ‘Significant Social Media Intermediaries’ (SSMIs).¹⁰ These entities are no longer passive conduits but are legally obligated to appoint resident grievance officers¹¹ and compliance personnel,¹² deploy automated tools to filter specific types of content (e.g., child sexual abuse material)¹³ and trace the ‘first originator’ of information (primarily affecting encrypted messaging apps like WhatsApp).¹⁴

The IT Rules, 2021, effectively shifted the burden of policing speech from the state to the private sector. Platforms must now exercise ‘due diligence’ to ensure users do not host content that threatens ‘public order,’ ‘decency,’ or the ‘sovereignty and integrity of India.’¹⁵ Presence

⁶ Hereinafter the IT Act.

⁷ Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India) (shielding intermediaries, such as social media platforms and internet service providers, from legal liability for third-party information, data, or communication links hosted by them, provided they observe due diligence, act merely as facilitators without modifying the content, and promptly remove unlawful material upon receiving an official government or court order.)

⁸ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁹ *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, G.S.R. 139(E), Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021) (hereinafter the IT Rules, 2021).

¹⁰ Ministry of Electronics and Information Technology, Notification S.O. 942(E), *Gaz. India*, Extraordinary, Pt. II, Sec. 3(ii) (Feb. 25, 2021).

¹¹ Rule 4(1)(c), the IT Rules, 2021.

¹² Rule 4(1)(b), the IT Rules, 2021.

¹³ Rule 4(4), the IT Rules, 2021.

¹⁴ Rule 4(2), the IT Rules, 2021.

¹⁵ Rule 3(1)(d), the IT Rules, 2021.

of such vague terms, when coupled with the threat of criminal liability for platform executives, encourages ‘preventive censorship’—where platforms err on the side of removal to avoid legal battles.¹⁶

III. THE INVISIBLE EDITOR

While the law focuses on removal of speech, the greater power of platforms lies in the amplification and suppression of speech. These functions are performed by black-box algorithms. The IT Rules, 2021 mandates the Significant SMIs (SSMIs) to do the same however, in the context of “information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled.”¹⁷ These tools may take various forms and accordingly impact the free speech.

A. Shadow banning

Content moderation is a responsibility handed to the Social Media Intermediaries (SMIs). Especially in the context of addressing the menace of misinformation, “various technology based measures including automated tools or other mechanisms”¹⁸ are deployed by the SSMIs. Shadow banning usually refers to visibility remedies such as delisting and downranking.¹⁹ These interventions do not remove content; instead, they limit its reach by suppressing it within discovery mechanisms.²⁰ ‘Shadow banning reduces the visibility of a user’s content without notifying them. It resultantly creates a unique regulatory challenge. Unlike a takedown, which can be legally contested, algorithmic demotion is invisible. In the Indian context, political commentators and activists across the spectrum have alleged that opaque algorithms disproportionately suppress dissenting voices.’²¹

From a constitutional perspective, shadow banning presents a significant challenge to fundamental rights in India. It appears to violate Article 19(1)(a), which protects not only the act of speaking but also the dissemination and receipt of information—a standard reinforced by

¹⁶ Vasudev Devadasan, *Conceptualising India’s Safe Harbour in the Era of Platform Governance*, 19 Indian J. L. & Tech. 1 (2023);

¹⁷ Rule 4(4), IT Rules, 2021.

¹⁸ Rule 4(4), IT Rules, 2021.

¹⁹ Kelley Cotter, “*Shadowbanning Is Not a Thing*”: *Black Box Gaslighting and the Power to Independently Know and Credibly Critique Algorithms*, 26 Info. Comm’n & Soc’y 1226 (2023).

²⁰ Paddy Leerssen, *An End to Shadow Banning? Transparency Rights in the Digital Services Act Between Content Moderation and Curation*, 48 Computer L. & Security Rev. 105,790 (2023).

²¹ Rafid Akhter, *Why India Needs to Fill the Legal Vacuum on Social Media Shadow Banning*, \textsc{The Leaflet} (Sept. 19, 2025, 12:04 PM), <https://theleaflet.in/digital-rights/why-india-needs-to-fill-the-legal-vacuum-on-social-media-shadow-banning>; Shamani Joshi, *An Investigation Alleging Facebook India’s Links with the BJP Has Sparked a Political Row*, \textsc{Vice} (Aug. 17, 2020, 1:05 PM), <https://www.vice.com/en/article/wsj-investigation-of-facebook-india-links-with-bjp-sparked-political-row/>.

India's commitment to Article 19 of the ICCPR. The Supreme Court has consistently held, through judgments such as *LIC v. Manubhai D. Shah*²² and *Secretary, Ministry of I&B v. Cricket Association of Bengal*,²³ that access to communication mediums is intrinsic to free speech; shadow banning covertly severs this access without procedural fairness.

Furthermore, the landmark *Anuradha Bhasin v. Union of India*²⁴ ruling established that using the internet for trade or profession is constitutionally protected. Consequently, any restriction must satisfy the tests of legality, necessity, and proportionality under Articles 19(2) and 19(6). Shadow banning fails these metrics as it lacks statutory backing, operates opaquely, and offers no mechanism for redress. Finally, by artificially suppressing visibility without due process, the practice undermines the economic survival of digital creators and journalists, thereby infringing upon the right to practice a profession under Article 19(1)(g). The Supreme Court of India has consistently held that restrictions on free speech must be 'reasonable' and grounded in the specific categories of Article 19(2). In 2015, the Supreme Court struck down Section 66A of the IT Act for being vaguely worded and overbroad.²⁵ However, the current regulatory push for automated filtering risks reintroducing this vagueness through code rather than law.

B. Context collapse and bias

Algorithmic moderation systems are predominantly trained on English-language data. In India, where discourse spans 22 scheduled languages and hundreds of dialects, AI moderators frequently fail to detect hate speech in vernacular languages or, conversely, flag innocuous colloquialisms as offensive. This 'context collapse' results in the over-policing of marginalized linguistic communities and the under-policing of genuine incitement in regional languages. An empirical study concluded "current hate speech detection models demonstrate a distinct dependency on specific lexical markers, resulting in the disproportionate classification of terms like 'Muslim', 'gay', and 'Jew' as offensive. This keyword-based bias, which fluctuates across different languages and architectures, arises primarily from a lack of contextual processing. Although advanced methodologies utilizing pre-trained word embeddings offer partial mitigation, they remain susceptible to the latent biases present within the general-purpose AI

²² *Life Ins. Corp. of India v. Manubhai D. Shah*, (1992) 3 SCC 637.

²³ *Sec'y, Ministry of Info. & Broad. v. Cricket Ass'n of Bengal*, (1995) 2 SCC 161.

²⁴ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

²⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

foundation models they utilize.”²⁶ There exists bias in the way content moderation happens if the task is outsourced to the algorithms.²⁷

Wrapped in a ‘personalised recommendations’ format algorithms also engage with the freedom of speech and allied rights. To curate personalized feeds, AI systems analyse both overt user signals—such as likes and follows—and passive behavioural metrics like viewing duration. While users retain some curatorial agency through the ability to follow hashtags or filter specific keywords from their feeds and direct messages, the primary recommendation engine relies on a continuous feedback loop of user actions and behavioural data to surface thematically relevant content.

In India free speech is not just the right to shout; it is the right to hear. Accordingly, right to be informed is also a right that emanates from the freedom of speech and information. Personalized algorithms create ‘Filter Bubbles’. It effectively quarantines the user in an informational prison. By hyper-tuning a feed to a user’s existing biases, the algorithm actively suppresses dissenting, novel, or challenging information. Personalization creates a fragmented public sphere where speech is not open to all but open only to those the algorithm selects. This violates the egalitarian conception of free speech.

IV. PARAMOUNT FUNDAMENTAL RIGHT TO SPEECH

In a democracy freedom of speech and expression is not just a right but a structural necessity. The truth is most likely to emerge from the open competition of ideas. Even false speech has value because, in refuting it, the truth is clarified and strengthened.²⁸ In addition to having political utility, free speech is essential for self-realization. A human being cannot fully develop their personality or intellect without the freedom to speak, write, and create.²⁹ Even in the algorithmic age, the value of free speech will continue to hold paramount significance. Normatively the algorithmic age will have to attribute the same value to free speech.

²⁶ EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, BIAS IN ALGORITHMS: ARTIFICIAL INTELLIGENCE AND DISCRIMINATION (2022), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf.

²⁷ Reuben Binns et al., *Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation*, in SOCIAL INFORMATICS 405 (Giovanni Luca Ciampaglia et al. eds., 2017); Emma Llansó et al., *Artificial Intelligence, Content Moderation, and Freedom of Expression* (Transatlantic Working Grp. on Content Moderation Online & Freedom of Expression, Working Paper, Feb. 26, 2020), <https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf>.

²⁸ David Schultz, *Marketplace of Ideas*, THE FIRST AMEND. ENCYC. (July 9, 2024), <https://firstamendment.mtsu.edu/article/marketplace-of-ideas/>; Leonard Williams, *John Stuart Mill*, THE FIRST AMEND. ENCYC. (July 5, 2024), <https://firstamendment.mtsu.edu/article/john-stuart-mill/>.

²⁹ Jeffrey W. Howard, *Freedom of Speech*, in STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta & Uri Nodelman eds., Jan. 19, 2024), <https://plato.stanford.edu/entries/freedom-speech/>.

A. Algorithms influenced by heckler's veto

By pressuring intermediaries to take down content within tight timelines without judicial oversight, the state effectively deputizes private companies to adjudicate constitutional rights. This creates a 'heckler's veto,' where organized mass-reporting campaigns can trick algorithms into silencing opponents.³⁰

Algorithms are designed to maximize engagement, and 'outrage' is a high-engagement emotion. This creates a perverse incentive structure that strengthens the Heckler's Veto. When a mob attacks a post, the algorithm sees high engagement and amplifies the post further, inviting more abuse. This forces the user to delete the post for their own safety. Organized groups can coordinate to mass report a specific account. Automated moderation systems often cannot distinguish between a coordinated attack and genuine policy violations, leading to automatic bans.

In traditional Indian constitutional law, the Supreme Court has firmly rejected the Heckler's Veto. The state cannot cite a mob's violent reaction as a valid excuse to silence a speaker; instead, the state has a duty to protect the speaker. Established in *S. Rangarajan v. P. Jagjivan Ram*,³¹ the Court held that speech can only be restricted if it is like a 'spark in a powder keg' i.e. the danger to public order is imminent and inevitable. While the Courts reject the Heckler's Veto, local law enforcement often invokes law and order concerns to shut down internet access or block content when online outrage spills offline.

B. Widespread takedown powers and chilling effect

In 2025, the Karnataka High Court delivered a judgment on Sahyog portal. Sahyog portal is a centralized platform launched by the Ministry of Home Affairs (MHA) and maintained by the Indian Cyber Crime Coordination Centre (I4C).³² Its purpose is to streamline and automate the process for government agencies (like the police) to send content takedown notices directly to internet intermediaries. An RTI response revealed a specific list of digital platforms that have been onboarded onto the Sahyog portal. There are as many as 94 companies onboarded on the Sahyog portal.³³

The IT Rules, 2021 have undergone modification in Oct. 2025³⁴ after the Karnataka High

³⁰ Charles S. Nary, *The New Heckler's Veto: Shouting Down Speech on College Campuses*, 21 U. PA. J. CONST. L. 305 (2018).

³¹ *S. Rangarajan v. P. Jagjivan Ram*, (1989) 2 SCC 574.

³² Ministry of Home Affairs, *Sahyog Portal*, <https://sahyog.mha.gov.in/> (last visited Dec. 11, 2025).

³³ *Zoom and Quora Among 94 Platforms Onboarded on Sahyog*, MEDIANAMA (Dec. 5, 2025), <https://www.medianama.com/2025/12/223-zoom-quora-list-companies-sahyog-portal-rti/>.

³⁴ *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (updated Oct.

Court's decision on Sept. 24, 2025.³⁵ The amended rules have come into effect from November 15, 2025. The amendment introduced significant safeguards to Rule 3(1)(d) of the existing 2021 Rules. It aims to enhance transparency, accountability, and proportionality in the removal of unlawful online content by replacing broad notification powers with a structured 'reasoned intimation' process. This process mandates that removal requests must now clearly specify the legal basis, the nature of the unlawful act, and the specific URL or electronic identifier of the content in question, thereby aligning with the 'actual knowledge' requirement of Section 79(3)(b) of the IT Act.³⁶ Furthermore, the amendment enforces stricter authorization protocols, stipulating that only senior officers specifically those not below the rank of Joint Secretary (or equivalent/Director in certain cases) or, for police authorities, a Deputy Inspector General (DIG) can issue such intimations.³⁷ To prevent arbitrary enforcement, a new periodic review mechanism has been established, requiring all removal intimations to be reviewed monthly by an officer not below the rank of Secretary of the Appropriate Government.³⁸ Now, it remains to be seen as to how effective the amended rules will be in safeguarding the freedom of speech and expression.

C. Difference in the nature of SMIs as subjects of law and end users as subjects of law

Even if the control over SMIs violates end users rights to free speech indirectly, there exists chilling effect and this does result in violating the constitutional protection of freedom of speech and expression. The information asymmetry between the SMIs and the end users weakens the position of the end users to take an action against the unreasonable and arbitrary actions of the government. The indirect effect then remains indirect only because there is no access to the rationale for the executive actions done in secrecy. In a legal system, one has the right to a fair hearing and an appeal. In algorithmic systems, decisions are often instantaneous and opaque (the 'Black Box' problem). Users rarely know why they were banned, and appeal mechanisms are often automated and unresponsive. Such approach significantly curtails the scope of available freedom of speech and expression and associated rights.

An alternative approach is available in the European Union. The European Union's implementation of the Digital Services Act (DSA) presents a compelling alternative to the current Indian framework.³⁹ While the DSA preserves the foundational principle of safe harbour

22, 2025), Ministry of Electronics & Info. Tech., <https://www.meity.gov.in/static/uploads/2025/10/708f6a344c74249c2e1bbb6890342f80.pdf>.

³⁵ *X Corp. v. Union of India*, W.P. No. 7405 of 2025 (Karnataka H.C. Sept. 24, 2025).

³⁶ Rule 3(1)(d)(ii), IT Rules, 2021

³⁷ Rule 3(1)(d)(ii)(I), IT Rules, 2021

³⁸ *Id.*

³⁹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single

it fundamentally alters the conditions required to maintain that immunity. Unlike the traditional model where liability is waived simply by complying with takedown notices, the EU has introduced a tiered system of accountability. Under the DSA, Very Large Online Platforms (VLOPs) face significantly higher scrutiny. They are mandated to perform systemic risk assessments, engage in rigorous transparency reporting, and provide robust mechanisms for users to challenge moderation decisions. Consequently, the EU model suggests that immunity is not an inherent right but a privilege earned through responsible governance and transparency. In stark contrast, the Indian regime remains largely reactive, pivoting almost exclusively on government-mandated takedown orders. The Indian approach is characterized by a ‘command-and-control’. The focus is squarely on the swift removal of specific content upon government notification. While India has tightened the timelines and enforcement of these ‘notice-and-takedown’ protocols, it lacks the DSA’s broader architecture of external oversight and proactive systemic reporting. Thus, in India, there is currently no parallel statutory requirement in India for platforms to publicly disclose their moderation logic or systemic risks. Thus, while India has strengthened the hook of enforcement (by mandating the takedowns), the EU has widened the net of accountability (by focusing on the oversight and transparency).

V. CONCLUSION

India stands at a critical juncture. The digitization of the public sphere offers unprecedented opportunities for democratization but also poses severe risks of manipulation. The current trajectory where heavy-handed executive control combined with opaque private algorithmic curation threatens to squeeze the space for free expression. A truly ‘Indian perspective’ on speech regulation must reject both Silicon Valley’s data colonialism and digital authoritarianism, striving instead for a ‘digital constitutionalism’ that protects the citizen’s right to speak, to be heard, to be informed and to dissent in the algorithmic age.

Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 6, 2022 O.J. (L 277) 1.