INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 3 | 2026 Art. 23

Reimagining Regulatory Frameworks for Platform Power Algorithmic Opacity and Democratic Accountability in India's Digital Public Sphere

Anbunila P
Law Student,
4th Year, BBA.LL.B.(Hons.)
Bharath Institute of Law, BIHER, Tamil Nadu

Recommended Citation
Anbunila P, *Reimagining Regulatory Frameworks for Platform Power Algorithmic Opacity and Democratic Accountability in India's Digital Public Sphere*, 5 IJHRLR 354-365 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Reimagining Regulatory Frameworks for Platform Power Algorithmic Opacity and Democratic Accountability in India's Digital Public Sphere

ABSTRACT

Digital media platforms have grown into powerful entities which have taken control of essential functions needed to operate democratic systems from government bodies. The research paper examines platform power which is studied through the concept of algorithmic opacity to show how hidden content curation systems control political discussions and election outcomes and determine what people can find in India's online public spaces. The study demonstrates that secretive systems which determine algorithmic outcomes create a situation where democratic processes break down because they allow false information and extreme views and hidden digital campaigns to grow without control.[1] The research examines how the privacy protection and surveillance systems interact with the data protection practices and also by the analysis while displaying the dangers which both governmental surveillance methods and companies, which collect data, pose to people.[2] The research paper uncovers ongoing deficiencies which prevent organizations from maintaining accountability and protecting constitutional rights by analysing Indias new regulatory framework for data protection and intermediary liability standards. The research paper supports a transition to rights-based digital governance which requires algorithmic transparency and public involvement in monitoring and creating standards for responsibility.[3] The approach establishes a framework which enables people to maintain their core democratic rights while technology develops through their daily lives.[4]

KEYWORDS

Platform Power, Algorithmic Opacity, Democratic Accountability, Data Protection, Digital Public Sphere

[1] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.
[2] Tarleton Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (2018)
[3] Shoshana Zuboff, The Age of Surveillance Capitalism (2019)
[4] U.N. Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/RES/34/7 (Mar. 23, 2017).

INTRODUCTION

The digital media platforms from Meta Platforms and Google to X Corp have experienced rapid growth which has resulted in new structures that modern democratic societies use to operate their governments. The platforms have developed into major organizations which now manage all communication channels while they determine what people discuss and how they participate in politics. The platforms have developed into the new "digital public sphere" which operates in India through its increasing digital access while it replaces existing public spaces like print media and public assemblies and public debates.[5] The shift from physical locations to digital spaces operated through algorithms has resulted in private companies gaining unprecedented control over essential organizational functions. These platforms function as public entities while they lack direct democratic control because they manage public activities which include speech regulation and content moderation and information visibility decisions. The system operates because private companies perform as unofficial government officials who control public discussion but this raises major issues about how they operate and whether they maintain fairness and openness.[6] The central problem of this situation is Instagram's algorithmic opacity because its automated decision-making processes operate without user understanding. Algorithms control everything from content display to trend selection and voice amplification while they also choose which content will be hidden from users. The public cannot access these processes because the companies involved use proprietary technology and trade secrets to maintain their operations. The "black-box" system of algorithms prevents users and regulators and governments from learning about the decision-making processes.[7]

Democratic governance in the current situation faces deep challenges because of political leaders who intentionally keep important information secret. The electoral process suffers from multiple threats which include unregulated spread of false information, efforts to manipulate political outcomes through targeted attacks, bias present in algorithms, and the establishment of echo chambers. The diverse and intricate nature of Indian society amplifies these dangers, which can endanger the fundamental constitutional rights that protect free speech and public access to knowledge.

Current Indian rules about platform power and algorithmic control of a

[5] Meta Platforms, Community Standards.
[6] Tarleton Gillespie, *Custodians of the Internet* (2018)
[7] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015)

require new approaches because they do not provide proper solutions for these modern problems. Regulators must develop new methods that use the rights-based systems to achieve better results through enhanced transparency and accountability and active citizen involvement. The required reforms will enable India to achieve many technological progress and democratic values protection in its developing digital public space.

PLATFORM POWER IN DIGITAL ECONOMIES

Digital platforms have developed into digital systems which control both economic and informational power throughout contemporary societies. Meta Platforms, Google, and X Corp now operate as information gatekeepers who determine all digital content which can be shown to people through public online spaces. These platforms which differ from conventional media organizations use algorithmic systems for content creation which enables them to control how users experience their content.

Platform power exists because of network effects which create a situation where more platform users increase platform value. The market develops a self-sustaining loop which creates market concentration and results in operators who dominate the market to behave like monopolists, who then restrict available options for their customers while driving their smaller rivals out of existence. Platforms within the data economy collect enormous amounts of consumer data, which they use to enhance their algorithms and create targeted advertising that determines how users interact with their content. Through its data-driven approach to digital capitalism platforms achieve both economic success and maintain their power over social and political matters.[8]

Market power enables companies to control democratic systems because their influence reaches beyond economic competition. Digital platforms function as essential tools which create public views that affect election results and help political movements get support. Political parties in India use social media platforms as essential tools for their electoral strategies because they can use targeted advertisements and influencer networks and data analytics to identify particular voter groups.[9] Platforms use behavioural data to create user profiles which enable them to target specific users, which raises issues about their capacity to hide information and shape how voters decide.

[8] Organisation for Economic Co-operation and Development (OECD), *Data-Driven Innovation: Big Data for Growth and Well-Being* 45–50 (2015).
[9] David Carroll, The Cambridge Analytica Scandal and the Global Implications of Data-Driven Political Campaigns, 20 *J. Cyber Pol'y* 1, 3–6 (2018).

The Cambridge Analytica scandal demonstrates how platform power creates risks which lead to multiple data breaches that occurred when the company illegally obtained user data from millions of people without their permission to manipulate election results which included the 2016 U.S. Presidential Election and the Brexit referendum. The incident demonstrated how data-driven profiling and algorithmic targeting functions as a tool to control democratic processes between political groups. India has not experienced an exact duplicate of this major scandal but also the people have raised similar worries about how political groups misuse user data and distribute false information during specific electoral periods.

Platforms play a major role in determining how people will participate in collective actions through their power to control which stories people can access and which tales they will suppress. Online activists use social media platforms to create hashtag movements which operate through digital campaigns and online mobilization efforts that face algorithmic prioritization which frequently deviates from basic standards of the fairness and neutrality, justice.[10]

Digital economies experience platform dominance because of combined economic power which intersects with technological progress and political authority. The absence of proper regulatory control over these organizations increases worries about their ability to be held accountable because it hampers fair competition while violating basic human rights.[11] The critical assessment of platform functions in governance systems becomes essential because their power has grown throughout time.

ALGORITHMIC OPACITY AND ITS RISKS

The governance of digital platforms has made algorithmic opacity into a major problem because these platforms now hold increasing power to shape public discussions. The term algorithmic opacity describes the situation where automated decision-making systems do not disclose their methods for ranking and recommending content or removing content on platforms like Meta Platforms Google and X Corp. The algorithms function as black boxes because users can see their inputs and outputs yet they cannot access the hidden operational processes which keep their internal functions secret from users and regulators and platform operators.

[10] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* 55–63 (2018).
[11] United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/32/L.20 (June 27, 2016).

The systems maintain their hidden operations because the two main reasons provide acceptable reasons for their continued use. The platforms protect their trade secrets by claiming that disclosing their algorithmic processes will harm their ability to compete in the digital market. The growing use of artificial intelligence and machine learning technologies creates additional technical difficulties which make it challenging to explain how particular results are achieved. Users do not receive useful information about the methods used to create their online experiences which results in their online content.

Algorithms do not merely reflect reality; they actively construct it. The world faces a major danger because false information spreads at a fast pace together with intentional falsehoods. Content which people find exciting or which generates strong feelings or which contains contentious topics gets promoted more by engagement-focused algorithms than by its factual correctness.[12] The propagation of fake news becomes a major issue because it leads users astray while creating wrong public perceptions and impacting how people vote.

Algorithmic systems enable users to enter echo chambers which show them only information that matches their established views. The systems create ideological rifts by blocking access to opposing viewpoints which prevents people from engaging in genuine democratic discussions. The result of this situation leads to societal divisions which destroy the basic elements that support diverse viewpoints and educated discussions.[13]

Political groups use algorithmic systems because they allow them to control information flow through targeted audience segmentation and customized advertising methods. The systems enable political groups to create specific messages which reach different demographic segments but they operate without any need for public understanding or official responsibility. The system creates an unfair situation which blocks people from accessing essential information and results in uneven playing fields during democratic activities.[14]

Digital platforms today control user behavior through digital sanctions which include account suspension and permanent bans and content removal and shadow banning because these platforms restrict user content visibility without informing users. Meta Platforms and Google and X Corp established internal policies which provide community

[12] Soroush Vosoughi, Deb Roy & Sinan Aral, The Spread of True and False News Online, 359 *Science* 1146, 1146–51 (2018).
[13] Cass R. Sunstein, #*Republic: Divided Democracy in the Age of Social Media* 9–15 (2017).
[14] Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 *U.C. Davis L. Rev.* 1149, 1155–60 (2018).

standards that determine acceptable speaking and behavioral standards for their platforms. The platforms position themselves as private organizations which manage speech through their harmful content restrictions because they operate like judges without following the standard legal procedures that government agencies use.

DIGITAL SANCTIONS & PLATFORM GOVERNANCE

Platform-based sanctions operate through hidden systems which lack the transparency and judicial review and due process requirements that traditional legal systems need to make judgments about rights. Content moderation decisions depend on automated systems and internal algorithms which provide limited information to users who are affected by those decisions. Users face procedural unfairness because they receive penalties before they are informed about the charges against them and their chance to defend themselves and their ability to use proper procedures.[15] Private organizations which possess such judicial authority operate outside established legal standards to create an alternative governing system which functions independently from democratic processes.[16] The regulation of digital platforms in India is controlled by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 which derive their authority from the Information Technology Act of 2000. The rules require intermediaries to perform due diligence which includes removing illegal content within defined time limits and creating systems that let users file complaints.[17] The government maintains extensive power from Section 69A of the Information Technology Act which allows them to shut down public access to knowledge because of security needs and public safety requirements and state protection needs. The provisions demonstrate how governments increasingly control the digital environments through their regulatory authorities. The platforms establish their own operational requirements which they enforce but these standards do not always match the requirements established by the government or the Constitution. The system of dual control creates a situation which leads to inconsistent enforcement practices and excessive authority use and legal conflicts because government orders threaten to violate essential rights which include freedom of speech protected under Article 19(1)(a) of the Constitution of India.[18] The relationship between government

[15] Nicolas Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* 27–35 (2019).
[16] Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 *Harv. L. Rev.* 1598, 1625–32 (2018).
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), issued under the Information Technology Act, No. 21 of 2000, India Code.
[18] Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* 102–08 (2016).

power and platform management creates problems which lead to excessive censorship and wrongful power use. Platforms have the ability to delete content for legal reasons but their actions create hazards which disproportionately impact genuine speech especially in situations with political sensitivity. Government authorities who intervene excessively in state matters create obstacles which prevent digital platforms from achieving their full potential while they disrupt progress throughout the digital market.[19]

The regulatory framework of digital sanctions together with platform governance creates a complicated system which combines private control with governmental authority. The current situation requires content moderation and enforcement standards to be established through clear and consistent guidelines that need to be made available to the public and maintained throughout the process.

LEGAL FRAMEWORK IN INDIA

The law governing digital platforms in India exists through a combination of statutory laws and subordinate legislation and constitutional protections. The new judiciary system creates a framework to evaluate platform responsibility and state requirements and essential human rights because of rising worries about the platform control and algorithm management. The Information Technology Act of 2000 serves as the main legal framework which controls all online activities.[20] The Central Government uses Section 69A which represents one of its most important provisions to restrict public information access when necessary to protect state sovereignty and national integrity and state defense and public safety. The state uses this provision to remove dangerous and illegal material, but the system creates issues about content blocking because it keeps blocking orders secret and fails to share detailed explanations with the public. The Act creates an intermediary liability system which protects platforms from third-party content, but this protection only exists when platforms meet their due diligence obligations. The Information Technology Intermediary Guidelines and Digital Media Ethics Code Rules 2021 build upon existing regulation standards by creating specific new requirements and norms for intermediaries. The rules establish specific requirements for platforms to follow, which mandate them to eliminate illegal content within designated times when they gain actual knowledge or receive government instructions. Social media platforms that qualify as significant intermediaries must establish compliance officers who will create message traceability systems and deliver regular compliance

[19] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[20] Information Technology Act, No. 21 of 2000, India Code.

reports.[21] The rules create a complaint resolution system which requires platforms to establish mechanisms that enable users to file complaints and receive their solutions.

The Act requires data fiduciaries to obtain explicit user consent before collecting and processing personal data according to its rules about data processing based on user consent. The Act requires data fiduciaries to implement security measures which protect data from unauthorized access and maintain user rights for data access and correction and data deletion. The legislation establishes data protection as a core principle of digital governance Yet there are ongoing issues with the implementation of enforcement systems and the state receives special treatment through its ability to obtain exemptions from the law. The regulation of digital platforms needs to follow constitutional requirements which stem from Article 19(1)(a) of the Constitution of India that protects freedom of speech and expression rights. Digital platforms have become primary spaces for exercising this right, which makes online content restrictions to face constitutional evaluation.[22] The law permits authority to impose reasonable restrictions according to Article 19(2) which protects sovereignty and security and public order and decency and moral standards.[23]

Judicial interpretation has played a crucial role in shaping this legislation. The Supreme Court declared Section 66A of the IT Act unconstitutional because it contained vague language which protected online speech. [24]The Court held that internet access as a required element of freedom of expression rights in Anuradha Bhasin v. Union of India because content restrictions need to follow proportionality principles.[25]

INTERNATIONAL PERSPECTIVE

International regulatory frameworks display comparative strengths and weaknesses when they assess India's methods for governing platforms and protecting user data. The European Union has become the worldwide leader in this area through its extensive legal framework which includes the General Data Protection Regulation (GDPR). The GDPR establishes a robust framework which protects user rights and safeguards personal data through access rights and rectification rights and deletion rights and processing restriction rights. The law requires data controllers and processors to obtain informed consent while

[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3, 4, G.S.R. 139(E) (India).
[22] India Const. art. 19, cl. 1(a).
[23] India Const. art. 19, cl. 2.
[24] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[25] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

practicing data minimization and fulfilling their accountability requirements. The GDPR establishes severe penalties which protect user rights and enhance compliance monitoring and violation deterrence systems.

The European Union implemented the Digital Services Act (DSA) which works together with the GDPR to establish regulations that enhance platform accountability and transparency. Online platforms must present their content moderation methods while they conduct risk evaluations and their algorithms must operate with better transparency according to DSA requirements. The law requires large platforms to reduce systemic dangers which include disinformation spread and dangers that affect democratic institutions. Digital platforms require data protection laws because their operations impact society beyond their technological boundaries. India has an evolving regulatory framework that lacks proper enforcement mechanisms and transparent processes according to its current state of development. The Digital Personal Data Protection Act 2023 establishes data governance through consent procedures but it does not provide the complete rights-based framework together with enforcement methods that exist in the GDPR. The Information Technology Rules 2021 establish limited obligations for intermediaries yet they fail to resolve the complete range of problems which include algorithmic transparency and systemic platform risks.

CHALLENGES IN THE CURRENT SYSTEM

- ***Lack of Transparency***

  Digital platforms operate through opaque algorithms and undisclosed moderation policies which prevent users from understanding the decision-making process. The absence of clarity results in unaccountable situations which make it impossible for regulators to perform their duties.[26] The system prevents users from understanding how the platform manages their content which results in invisible content management.

- ***Weak Enforcement Mechanisms***

  The IT Act and Data Protection framework exist as legal frameworks which suffer from inconsistent enforcement and limited enforcement capacity.[27] The regulatory authorities need technical capacity and institutional strength to handle compliance monitoring. The legal safeguards which exist to protect users will fail to provide effective

[26] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–10 (2015).
[27] World Bank, *World Development Report 2021: Data for Better Lives* 271–75 (2021).

protection.

- ***Overlapping Regulations***

The IT Act and IT Rules and Data Protection laws create a regulatory system which exists as a disorganized network of legal requirements. The system creates compliance difficulties for platforms which results in legal uncertainties and inconsistent enforcement practices. The system creates legal confusion which has an impact on both enforcement actions and the development of new ideas.[28]

- ***Risk of Government Overreach***

The government can use Section 69A to implement content restrictions because it gives them broad powers which require minimal transparency. The process creates opportunities for government organizations to perform censorship in an arbitrary manner which raises great public concern.[29] The government actions create negative impacts which restrict both democratic expression and free speech rights.

- ***Absence of an Independent Regulator***

India needs an independent organization which will handle digital platform supervision while maintaining fair regulatory controls. Executive-led oversight currently dominates the system which creates a risk of partiality during monitoring. The establishment of an independent regulator needs to happen because it protects fundamental rights while ensuring impartial governance and monitoring responsibilities.

SUGGESTIONS / WAY FORWARD

To address the challenges posed by platform power and algorithmic opacity, India must adopt a rights-based and transparent regulatory framework. First, the introduction of algorithmic transparency audits is essential to ensure that platform decision-making processes are fair, unbiased, and accountable. Second, establishing an independent regulatory authority can provide neutral oversight and prevent excessive executive control. Third, a comprehensive user rights protection framework must be developed to guarantee informed consent, data privacy, and effective grievance redressal. Additionally, public

[28] Anupam Chander & Uyen P. Le, Data Nationalism, 64 *Emory L.J.* 677, 718–22 (2015).
[29] Apar Gupta & Elonnai Hickok, Blocking and Filtering of Online Content in India: A Legal Analysis of Section 69A of the Information Technology Act, 2015 *Indian J.L. & Tech.* 1, 18–25 (2015).

participation in digital governance should be encouraged to enhance legitimacy and inclusiveness. Platforms must also be subjected to stronger accountability mechanisms, including disclosure obligations and periodic compliance reporting. Finally, the adoption of explainable AI systems is necessary to make algorithmic decisions understandable and contestable. Digital platforms must evolve from opaque controllers to accountable public institutions.

CONCLUSION

Digital platforms today wield unprecedented influence, transforming platform power into real political power that shapes public discourse and democratic outcomes. While technological innovation has created new opportunities, it has also introduced serious risks to fundamental rights and democratic values. India must therefore strike a careful balance between innovation and rights protection by strengthening its regulatory framework with transparency, accountability, and constitutional safeguards. The future of democracy in India will depend not only on laws enacted by Parliament, but also on the invisible codes written by algorithms.

"In the digital age, the rule of law must extend beyond legislation to the algorithms that silently govern society."