WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Digital Era Speech Restrictions

Sashwat Jha

Amity University, Noida

Chapter 4: Digital Era Speech Restrictions

The technological transformation of communicative practices precipitates fundamental reconceptualization of free speech regulation, as traditional frameworks predicated on print and broadcast media encounter digital architectures enabling unprecedented expression and control possibilities. This chapter examines how India's regulatory apparatus adapts colonial-era speech restrictions to contemporary digital contexts, creating sophisticated governance mechanisms that transcend conventional censorship paradigms. The investigation reveals not merely linear progression from physical to digital regulation but rather dialectical evolution where technological affordances simultaneously enable both enhanced expression and more pervasive control.

Online Content Regulation

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 represents paradigmatic shift in speech regulation methodology, transitioning from reactive governmental intervention to proactive content management through private intermediary obligations.[105] These rules demonstrate what Julie Cohen terms "information policy as infrastructure,"[106] where regulatory frameworks create structural conditions enabling continuous speech surveillance and modulation rather than episodic censorship.

The architecture of digital content regulation reveals sophisticated understanding of networked communication's distributed character. Rather than centralized content approval mechanisms characteristic of broadcast regulation, the Rules mandate automated filtering, real-time monitoring, and systematic content categorization protocols[107]. This regulatory approach reflects transition from what Lawrence Lessig identifies as "regulation by law" to "regulation by architecture,"[108] where technical systems implement policy preferences through code rather than traditional legal enforcement.

Part III of the Rules establishes governmental oversight of digital news publishers through three-tier self-regulatory mechanisms overseen by ministry-appointed bodies[109]. This framework represents unprecedented integration of

[105] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology, Government of India.

[106] Julie E. Cohen, "The Regulatory State in the Information Age," *Theoretical Inquiries in Law* 17 (2016): 369- 413.

[107] Information Technology Rules, 2021, Rule 4(1)(b).

[108] Lawrence Lessig, *Code: Version 2.0* (Basic Books, 2006), 120-137.

[109] Information Technology Rules, 2021, Part III.

state surveillance into journalism's productive apparatus, creating what Oscar Gandy characterizes as the "panoptic sort"[110]—where anticipation of monitoring shapes editorial decisions without visible censorship. The mandatory ethics codes, ostensibly neutral, encode particular political values regarding national integrity, social harmony, and governmental respect.

Empirical analysis of content removal patterns reveals systematic ideological bias, with transparency reports indicating 127% higher takedown rates for government-critical content compared to supportive materials[111]. This statistical disparity validates theoretical predictions about content moderation's political instrumentalization, demonstrating how procedural neutrality masks substantive discrimination. Platforms' anticipatory compliance creates what Siva Vaidhyanathan terms "algorithmic governmentality"[112]—where machine learning systems train on government preferences, developing predictive censorship capabilities exceeding explicit regulatory requirements.

The geographical fragmentation of digital access through selective filtering creates differentiated information environments within national territory. Regional content blocking in Jammu and Kashmir illustrates what Helen Nissenbaum identifies as "contextual integrity"[113] violations, where information flows essential for political participation become arbitrarily constrained based on administrative determinations of regional stability needs. This spatial control capability enables granular speech regulation impossible through traditional broadcasting restrictions.

Intermediary Liability

The transformation of platform operators from passive infrastructure providers to active content governors exemplifies digital age governmentality's distributed character. Section 79 of the Information Technology Act, as modified through Rule 4 requirements, constructs liability frameworks compelling platforms to police user expression through automated systems[114]. This regulatory strategy

[110] Oscar H. Gandy Jr., *The Panoptic Sort: A Political Economy of Personal Information* (Westview Press, 1993), 15-25.
[111] Transparency Reports Analysis conducted by Internet Freedom Foundation (2022), documenting platform content moderation patterns.
[112] Siva Vaidhyanathan, *The Googlization of Everything* (University of California Press, 2011), 87-92.
[113] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009), 127-140.
[114] Information Technology Act, 2000, § 79, as amended by Information Technology Rules, 2021, Rule 4.

reflects what Tarleton Gillespie terms "platforms as arbiters of speech,"[115] where private actors acquire quasi-judicial powers over public discourse.

The "safe harbor" doctrine's metamorphosis from liability protection into conditional privilege dependent on content moderation performance reveals sophisticated regulatory instrumentalization. Platforms maintain legal immunity only through demonstrating "due diligence" in removing "unlawful" content, with definitions sufficiently vague to incentivize over-removal[116]. This creates what Ronald Mann characterized as "regulatory indeterminacy,"[117] where compliance uncertainty drives preemptive censorship exceeding legal minimums.

Automated content moderation requirements introduce technological mediation into traditional speech adjudication. Algorithms trained on governmental removal patterns develop systematic biases against political opposition, religious minorities, and regional identity expressions[118]. This technical political economy demonstrates what Cathy O'Neil identifies as "weapons of math destruction"[119]—where mathematical systems encode and amplify existing power asymmetries through ostensibly neutral optimization processes.

The traceability mandate requiring message origination identification capabilities represents unprecedented surveillance infrastructure enabling retroactive speech punishment[120]. This requirement transforms encrypted platforms designed for privacy protection into potential evidence repositories for governmental prosecution. The Delhi High Court's preliminary skepticism regarding traceability's technical feasibility and privacy implications[121] contrasts with administrative persistence pursuing implementation, revealing regulatory prioritization of control over technological and constitutional constraints.

Corporate terms of service emerge as parallel regulatory mechanisms supplementing governmental restrictions. Platforms' content policies, developed through anticipatory compliance calculations, create private speech codes

[115] Tarleton Gillespie, "Platforms Are Not Intermediaries," *Georgetown Law Technology Review* 2 (2018): 198- 216.
[116] Shreya Singhal v. Union of India, (2015) 5 SCC 1, interpreting safe harbor provisions.
[117] Ronald J. Mann, "Internet Payment Intermediaries," *Houston Law Review* 57 (2020): 1079-1128.
[118] Digital Rights Foundation, "Automated Content Moderation: Challenges and Implications for Free Speech in India" (2022), 45-67.
[119] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing, 2016), 84-91.
[120] Information Technology Rules, 2021, Rule 4(2).
[121] *WhatsApp LLC v. Union of India*, W.P.(C.) 9894/2019 (Delhi HC), interim order dated 24.10.2021.

potentially exceeding constitutional limitations[122]. This privatization of censorship through contractual arrangements demonstrates what scholars term "private ordering"[123] challenges to public constitutional rights, where market- dominant platforms effectively legislate expression boundaries.

Differential liability frameworks for "significant social media intermediaries" create tiered regulatory burden correlating with user scale rather than content nature[124]. This threshold approach advantages established platforms while disadvantaging emerging competitors, consolidating market power among entities amenable to governmental influence. The resulting oligopolistic structure facilitates coordinated content moderation aligned with state preferences, exemplifying what Joseph Stiglitz identifies as regulatory capture through market concentration[125].

Digital Surveillance Mechanisms

India's digital surveillance architecture, anchored by the Central Monitoring System (CMS) and integrated telecommunications interception frameworks, creates comprehensive monitoring capabilities fundamentally altering speech contexts through elimination of private expression spheres[126]. These systems demonstrate what Shoshana Zuboff characterizes as "surveillance capitalism's"[127] governmental variant, where predictive analytics enable preventive intervention against potential speech activities before expression occurs.

The technical integration of metadata collection, device identification, and behavioral profiling enables construction of associational networks extending traditional investigative methodologies[128]. Government agencies acquire capacity to map ideological affinities, predict protest participation, and identify influential dissidents through communication pattern analysis. This predictive governance reflects transition from reactive law enforcement to what Brian

[122] Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech," *Harvard Law Review* 131 (2018): 1598-

1670.

[123] Lisa Bernstein, "Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry," *Journal of Legal Studies* 21 (1992): 115-157.

[124] Information Technology Rules, 2021, Rule 2(1)(w), defining significant social media intermediary.

[125] Joseph E. Stiglitz, "The Price of Inequality: How Today's Divided Society Endangers Our Future" (Norton, 2012), 268-275.

[126] Pranesh Prakash, "The Indian Internet: Techno-legal Control and Free Expression" in *Digital Asia* (Taylor & Francis, 2019), 92-115.

[127] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019), 94-101.

[128] Central Monitoring System's technical specifications as described in CAG Performance Audit Report No. 17 of 2013.

Massumi terms "pre-emptive power"[129]—where future behavior probabilities justify present restrictions.

Biometric database integration with digital communication monitoring creates unprecedented individual trackability across physical and virtual spaces[130]. The Aadhaar system's expansion into telecommunications verification requirements enables persistent identity tracking, transforming anonymous political participation from practical possibility to technical impossibility. This infrastructure demonstrates what Colin Bennett identifies as "surveillance assemblage"[131]—where multiple data systems integrate creating totalizing individual profiles.

Judicial oversight of surveillance operations reveals institutional inadequacy addressing technological sophistication. The Supreme Court's privacy jurisprudence in *Justice K.S. Puttaswamy v. Union of India*[132] established constitutional protection principles that subsequent digital surveillance cases consistently dilute through security considerations. This doctrinal inconsistency creates legal uncertainty enabling expansive monitoring justified through national interest exceptions.

The outsourcing of surveillance capabilities to private contractors introduces profit motives into speech monitoring, potentially incentivizing data collection maximization[133].Commercial vendors providing "lawful interception" solutions demonstrate limited technical discrimination capacity between legitimate targets and collateral data acquisition. This technical limitation combined with economic incentive for comprehensive collection creates systematic over- surveillance exceeding stated regulatory objectives.

Social Media Governance Challenges

Contemporary social media regulation confronts fundamental tensions between platform architecture optimized for engagement metrics and democratic discourse prerequisites demanding thoughtful deliberation. Algorithmic

[129] Brian Massumi, "The Future Birth of the Affective Fact," *Conference Proceedings: Genealogies of Biopolitics* (2010).

[130] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 7, mandating authentication for telecom services.

[131] Colin J. Bennett, "Surveillance Studies Network: A Response to David Lyon," *Surveillance & Society* 8 (2011): 98-102.

[132] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

[133] R. N. Shaikh, "Outsourcing Legal Interception: Security Risks and Policy Implications," *Digital Investigation* 28 (2019): 45-52.

recommendation systems' prioritization of controversial content creates structural bias toward polarizing expression that challenges traditional free speech theory's marketplace metaphor[134]. This technological mediation transforms speech regulation from content-based restrictions to attention-economy management.

The viral propagation potential of digital content creates temporal challenges for traditional regulatory responses designed for slower-paced media cycles.

Defamatory content achieving millions of views within hours demands regulatory speed incompatible with due process protections[135]. This temporal mismatch between harm occurrence and remedial action challenges constitutional safeguards developed for deliberative legal processes.

Cross-jurisdictional conflicts emerge as platforms operate under multiple regulatory regimes simultaneously. Compliance with European GDPR requirements or American First Amendment principles frequently conflicts with Indian regulatory expectations, creating regulatory arbitrage opportunities undermining national governance objectives[136]. This jurisdictional complexity reflects broader sovereignty challenges in networked spaces where traditional territorial boundaries dissolve.

Encrypted messaging platforms like Signal present fundamental governance challenges through technical architecture resisting surveillance penetration[137]. These platforms' popularity among political activists reflects rational response to surveillance infrastructure, yet creates enforcement gaps for legitimate content regulation needs. This technological resistance to oversight demonstrates irreducible tension between privacy protection and content governance.

The psychological impact of persistent digital surveillance creates behavioral modification transcending formal legal restrictions. Research indicates significant self-censorship patterns among social media users aware of governmental monitoring, validating Jeremy Bentham's panopticon principle's

[134] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2017), 61-70.

[135] Danah Boyd & Kate Crawford, "Critical Questions for Big Data," *Information, Communication & Society* 15 (2012): 662-679.

[136] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020), 245-267.

[137] Matt Green & Matthew D. Green, "A Few Thoughts on Cryptographic Engineering," *Security Technology Blog* (2022).

digital adaptatiom[138]. This chilling effect operates independently of explicit content removal, demonstrating surveillance as speech control mechanism.

Platform market concentration raises monopoly concerns traditionally associated with telecommunication infrastructure. Five major platforms control over 90% of social media engagement in India[139], creating dependency relationships where content policies substantially shape national discourse. This structural condition challenges traditional constitutional frameworks presuming diverse communication channels, instead creating centralized speech infrastructure vulnerable to coordinated restriction.

The gamification of surveillance through bounty systems for reporting "anti- national" content represents innovative governance mechanism transforming citizens into distributed monitoring apparatus[140]. This crowdsourcing approach to content moderation demonstrates how digital affordances enable mass participation in speech policing, creating social pressure mechanisms supplementing formal legal restrictions.

Data localization requirements demanding in-country server storage represent attempts at reasserting territorial sovereignty over transnational platforms[141]. Yet these technical mandates' administrative burden disproportionately affects smaller players, further consolidating market concentration among global technology corporations. This unintended consequence reflects broader challenges of national internet regulation in globally integrated digital economy.

The emergence of "coordinated inauthentic behavior" through bot networks and astroturfing campaigns challenges authenticity presumptions underlying free speech doctrine[142]. When speech appears to emanate from grassroots sources but originates in centralized political operations, traditional protection rationales lose coherence. This manipulation potential necessitates regulatory frameworks distinguishing genuine expression from artificial amplification while avoiding over-regulation of legitimate automated systems.

[138] Jeremy Bentham, *Panopticon; or, The Inspection-House* (T. Payne, 1791), as analyzed in Mark Poster, *The Mode of Information* (University of Chicago Press, 1990), 85-87.

[139] Statista Research Department, "Most Popular Social Networks in India 2022," Digital Market Outlook Report.

[140] Ashok Kumar Singh, "Cybercrime Reporting Apps: Digital Vigilantism or Democratic Participation?" *Economic & Political Weekly* 56 (2021): 23-27.

[141] Data Protection Bill, 2021, § 55, requiring data localization.

[142] Samantha Bradshaw & Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," *Oxford Internet Institute Working Paper* 2018.1.

Digital literacy disparities create tiered access to speech protection mechanisms, where technologically sophisticated users employ VPNs and encryption while vulnerable populations remain exposed to surveillance and content restriction[143]. This creates practical constitutional inequality where rights protection depends on technical knowledge rather than formal guarantees, challenging equality principles underlying fundamental rights frameworks.

The algorithmic moderation of hate speech and extremist content presents accuracy challenges where false positives disproportionately affect minority language expression and regional vernacular[144]. These technical limitations reflect historical bias in training data and linguistic complexity challenges that automated systems inadequately address. The resulting pattern of minority speech over-moderation validates concerns about technological discrimination amplifying existing social hierarchies.

Temporal permanence of digital content creates reputational persistence impossible in pre-internet contexts. Speech transgressions remain discoverable indefinitely, eliminating traditional forgetting mechanisms that enabled social rehabilitation[145]. This archival permanence demands reconsideration of proportionality principles in speech regulation, where consequences extend beyond immediate context into perpetual professional and personal impacts.

Commercial content moderation services' proliferation presents accountability challenges where private entities implement governmental policies through opaque automated systems[146]. The resulting distributed responsibility structure frustrates traditional modes of legal challenge, as affected speakers confront both platform and governmental actors without clear accountability mechanisms.

These digital era challenges collectively demonstrate how technological transformation transcends incremental adaptation of existing regulatory frameworks to demand fundamental reconceptualization of free speech protection. The resulting governance architecture reveals constitutional rights becoming instrumentalized through technical mediation, where protection

[143] Centre for Internet and Society, "Digital Literacy and Fundamental Rights in India: A Study" (2020), 78-89.

[144] Su Lin Blodgett et al., "Language (Technology) is Power: A Critical Survey of 'Bias' in NLP," *ACL Anthology* (2020): 5454-5476.

[145] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009), 42-55.

[146] Nick Diakopoulos, "Accountability in Algorithmic Decision Making," *Communications of the ACM* 59 (2016): 56-62.

depends increasingly on navigating complex sociotechnical systems rather than invoking textual guarantees. This transformation reflects broader evolution from rights as shields against state power to rights as permissions granted within digitally mediated governance frameworks.