The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 8 | August 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Protection of Right to Privacy and Freedom of Expression in the Digital Age

Nishu Singh
Research Scholar (Ph.D. In Law), Bundelkhand University, Jhansi
Prof. L. C. Sahu
Bundelkhand University, Jhansi

DOI : https://doi.org/10.5281/zenodo.18734649

ARTICLE DETAILS

Research Paper
Accepted: 21-08-2025
Published: 10-09-2025
Keywords:

ABSTRACT

This paper critically analy zes the emerging interplay between the freedom of expression and the right to privacy in India's digital era, with special reference to legislative evolution, judicial monitoring, and technological demands. It starts by situating India's constitutional jurisprudence, specifically the K.S. Puttaswamy v. Union of India 2017 judgment, which held that privacy is a right under the principles of necessity, proportionality, and legality. The article then assesses India's digital regulations, such as the Digital Personal Data Protection Act, 2023, on its consent frameworks, obligations of data fiduciaries, adjudicatory provisions, and substantial government exemptions that can compromise privacy protections. It also critically analyzes the Information Technology Rules, 2021, their recent regulatory directions seen to be facilitating "digital authoritarianism"—specifically mandating traceability on encrypted apps and sweeping powers of censorship. Technological aspects are discussed through concerns of algorithmic content moderation—pointing to bias, opaqueness, and threat to marginalized voices—and decentralized systems that can potentially provide a counterpoint to centralized control. The research also charts actual-world violations of digital rights, like recurring shutdowns of the internet and emergency content blocking, which heavily abridge both speech and privacy.Through the integration of

legal principles, policy analysis, and technology critiques, the article discovers essential gaps: weak provisions for surveillance, confusion in legislative definitions, and lack of digital skills among citizens. The paper concludes with proposals to enhance judicial review, improve platform transparency, enable decentralized alternatives, and create public awareness to promote democratic values in India's digital environment.

1. Introduction

The digital era—defined by the accelerated pace of technological change, almost universal internet connectivity, and omnipresent smart devices—brings challenging and adaptive obstacles to two cornerstones of democracy: freedom of expression and the right to privacy. In India, the very quick expansion of e-governance, biometric identifiers such as Aadhaar, and the explosion of social media outlets have dramatically transformed how citizens interact, access information, and engage with the state and each other.

The constitutional requirement to uphold such rights has responded accordingly. The Supreme Court's milestone ruling in Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right under Article 21 and established the necessary test of legality, necessity, and proportionality for any state interference. Judicial scrutiny has also played an integral role in protecting online speech: in Shreya Singhal v. Union of India (2015), the Court struck down Section 66A of the IT Act for the overly broad restrictions that muffled legitimate expression. However, digital regulatory frameworks inadvertently undermine these rights. The Digital Personal Data Protection Act, 2023—India's first data privacy omnibus statute—provides necessary protections like requirements for consent and adjudication. Nevertheless, its delayed enactment, sweeping state exemptions, and operational vagueness remain contentious issues.

Concurrently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (and their 2023 amendments), require traceability of end-to-end encrypted messages and authorize government-controlled "fact-checking" organizations. Such steps, although deemed indispensable for accountability, have chilling effects on speech and erode privacy rights.

Against this background, the paper aims to critically analyze the interplay between technological innovations, legislative action, and judicial control in modern India—assessing whether the equilibrium between privacy and expression is truly protected or progressively lost in the guise of regulation online.

2. Constitutional and Judicial Foundations

2.1 Right to Privacy

The path-breaking ruling in Justice K. S. Puttaswamy (Retd.) v. Union of India ingrained the Right to Privacy as a fundamental right of Article 21 of the Constitution. The nine judge bench set the landmark "legality, necessity, proportionality" test for governmental invasion of privacy, reaffirming that any violation would have to meet these strict standards

Justice D. Y. Chandrachud, on behalf of the bench, stressed that "Dignity cannot exist without privacy… Privacy is the ultimate expression of the sanctity of the individual," interconnecting privacy with more general concepts of autonomy, bodily integrity, and self determination

2.2 Freedom of Expression & ICT

In accordance with Article 19 (1) (a), citizens have the right to free speech. Nevertheless, this right has suffered considerably in the digital age:

- Section 66A of the Information Technology Act, 2000 made transmission of "grossly offensive" or "menacing" matter through computer resources an offence. It was invalidated by the Supreme Court in Shreya Singhal v. Union of India (2015) on the grounds that it was arbitrary and disproportionate and violated Article 19(1)(a).
- Section 69 gives authorization for government decryption and interception of digital communications, criticized by opponents as eroding the constitutional right to privacy. Instances of sweeping surveillance under this section have provoked serious constitutional issues.
- Section 69A permits app bans for national security reasons, at times invoked without open procedure—potentially raising conflicts with freedom of expression and equitable governance.

3. Digital Legislation and the Privacy–Expression Nexus

3.1 Digital Personal Data Protection Act, 2023

After the Puttaswamy judgment, the Indian government drafted privacy bills leading to the Digital Personal Data Protection Act, 2023. This act marks a major milestone in codifying data rights; however, its ambit and efficacy in preventing abuse and state excess are still matters of continuing assessment.

3.2 Personal Data Protection Bill, 2019

Earlier versions, particularly the Personal Data Protection Bill, 2019, were severely criticized. Even its lead author, Justice B. N. Srikrishna, warned it might usher in an "Orwellian State," which gives too much power of surveillance to the government in the name of sovereignty or public order. Issues are open access rights, vague accountability mechanisms, and threats to democratic liberties.

4. Emerging Digital Threats to Rights

4.1 Surveillance Capitalism & Data Harvesting

Surveillance capitalism—so named by Harvard professor Shoshana Zuboff—refers to the process in which digital platforms commodity people's personal data to make predictions about and shape behavior for profit. In this model, human experience is converted into behavioral data ("behavioral surplus") and marketed through markets of behavioral futures.

Recent empirical work supports these suspicions.

One study (August 2025) examined tech giants' web-monitoring habits in Google, Facebook, Amazon, Microsoft, and Apple, and demonstrated that data gathering persists in being pervasive and on the rise in sophistication. It demonstrated stratified tracking methods unfolding to avoid detection and connected surveillance capitalism to firm financial performance in a direct manner. Another report (December 2024) mapped the covert dynamics of web data collection, highlighting how network traffic analysis lays bare ubiquitous tracking practices and the necessity for more robust transparency and safeguards.

Implications for privacy and freedom:

- Behavioral surveillance undermines individuals' autonomy—not only through overt data collection, but via subtle feedback loops that shape choices and limit self-determination.
- When private entities accumulate such power, democratic oversight, user consent, and privacy erode.

4.2 Algorithmic Moderation and Hate Speech

Automated moderation tools—including GPT 4, Google’s Perspective API, and OpenAI’s Moderation API—are increasingly deployed to detect and curb hate speech. For instance, a 2025 study tested these systems on German online newspaper comments and found GPT 4 (in its GPT 4o variant) outperformed both Perspective API and the Moderation API, exceeding baseline performance by about 5 percentage points in combined metrics.

Although these technologies assist in toxic content management at scale, they come with risks intrinsic to them:

- Censorship of true speech: Under autonomous systems can err on the side of flagging or censoring satire, subtle criticism, or context-dependent speech.
- For instance, "algospeak"—a phenomenon where users intentionally distort language to avoid moderation—arises as a linguistic workaround to maintain expression online.
- Politically satirical content appears to be disproportionately blocked, independent of ideological alignment. One commenter saw that "satirical memes are systematically blocked," which indicated a potential overextension in moderation reasoning.

Bias and lack of transparency: Moderation tools are subject to biases and tend to be unclear as to how they determine what hates or what is harmful content. As one commenter on Reddit pointed out about the moderation toolkit:

"Some heavy biases in the moderation toolkit."

And others stress:

"The lack of transparency" behind how flagging operates continues to be a fundamental problem.

These issues lead to important questions about free expression, equity, and responsibility in algorithmic rule.

5. Legal and Technological Tensions—A Critical Perspective

5.1 Encryption vs. Government Surveillance

In countries such as the UK, legislation like the Online Safety Act 2023 contains controversial provisions like "client side scanning" of end-to-end encrypted messages. Critics fear this erodes encryption, allowing bulk surveillance without adequate controls.

While this anecdote is UK focused, it points to risks for any government looking for backdoor access—risks relevant to India as digital rule-making shifts.

5.2 Platform Liability and Speech Regulation

Law tends to make platforms responsible for user-created content, pushing them towards proactive monitoring or removals. This dynamic has the potential to chill speech and highlight the need for judicial involvement and openness in takedown processes.

6. Key Challenges and Gaps

Challenge / Gap	Description	Implications & Risks
1. State Surveillance: Section 69/69A & DPDP Exemptions	**Section 69/69A**: Legal provisions for blocking content or intercepting communications lack clear procedural safeguards, raising serious due process concerns—though *Shreya Singhal* upheld Section 69A as "narrowly drawn" and justified under Article 19(2). - **DPDP Act Sections 17/18**: Grant sweeping exemptions to government agencies (e.g., for national security or public order) without independent review, transparency, or sunset clauses.	- Risk of unchecked surveillance and intrusion into privacy. - Potential arbitrary or indefinite data access by the state. - Weakening of judicial oversight and erosion of the rule of law.
2. Weak Enforcement & Structural Ambiguity in DPDP	- The DPDP Act's implementation remains stalled due to undisclosed rules and an unclear enforcement timeline. - The Data Protection Board is government-appointed, potentially compromising its independence and effectiveness.	- Citizens remain uninformed about their rights and protections. - Enforcement may be selective or influenced by political agendas. - Smaller entities (e.g., MSMEs) may struggle to comply or be unaware of obligations.
3. Automated Moderation, Bias, and Lack of Appeal Mechanisms	- Government-mandated Fact-Check Units (FCUs) introduced under IT Rules faced judicial pushback for being vague and overbroad. The Bombay High Court struck them down as unconstitutional under Article 14 and 19 due to chilling effects on speech. - Algorithmic moderation systems are prone to inaccuracies, especially in low-resource languages, and often offer weak or no appeal options.	- High risk of suppression of dissent and satirical expression. - Marginalized communities may be unfairly censored. - Due process and transparency are undermined by automated takedowns.
4. Opacity in	- India currently lacks regulatory standards or	- Users lack clarity on how

Algorithmic Processes	guidelines for transparency and accountability in AI-driven decision-making (such as moderation or content ranking). - The DPDP Act does not specify algorithmic parameters, audit mandates, or responsible authorities.	decisions affecting them are made. - Difficulty in challenging or understanding automated content decisions. - Algorithmic biases may unintentionally reinforce societal inequalities.
5. Marginalized Voices & Digital Exclusion	- Surveillance frameworks and algorithmic biases disproportionately affect marginalized communities (e.g., in vernacular or low-connectivity areas). - Lack of independent safeguards, appeals, or accessibility reinforces exclusion and silencing.	- Democratic discourse narrows, as dissenting or minority voices are muted. - Digital divide widens, undermining equitable civic participation.

Key Insights

- **Balancing Act Under Strain**: While legislation like *Shreya Singhal* and the *Puttaswamy* judgment uphold legal standards for privacy and free speech, evolving tech and law (e.g., surveillance norms, algorithmic tools) pose new threats that existing frameworks aren't fully equipped to handle.
- **Critical Need for Oversight and Accountability**: Each identified gap—from unchecked surveillance powers to opaque automated decisions—demands both legal and institutional reforms to safeguard democratic rights.
- **Digital Literacy as a Foundation**: Without widespread awareness and education about digital rights (e.g., under DPDP), legal protections remain symbolic.

7. Recommendations

1. Strengthen legal protections: Precisely establish triggers for surveillance and have judicial approval and oversight.

2. Improve transparency and accountability: Require disclosure by platforms regarding content moderation and appeals.

3. Adopt privacy by design: Promote encryption and decentralized data practices.

4. Increase digital literacy: Equip citizens with knowledge to make them know their rights and digital risks.

5. Encourage multi stakeholder governance: Engage civil society, technologists, and marginalized communities in policymaking.

8. Conclusion

The digital age has reshaped the public-private divide. India's constitutional tradition—grounded in the Puttaswamy judgment and expressive freedoms—is a strong foundation. But contemporary threats—from surveillance to content control—require watchful, rights-safeguarding frameworks. A rethink that balances privacy, expression, and democratic values is essential.

References

- **Supreme Court Judgment: *K.S. Puttaswamy v. Union of India* (2017)** Wikipedia contributors. (2025, August 10). *K.S. Puttaswamy v. Union of India*. *Wikipedia*. Retrieved August 16, 2025, from Wikipedia Wikipedia
- Burman, A. (2023, October 3). *Understanding India's new data protection law*. *Carnegie Endowment for International Peace*. Retrieved August 16, 2025, from Carnegie Endowment Carnegie Endowment.
- Ministry of Electronics and Information Technology, Government of India. (2023, August 12). *Digital Personal Data Protection Act 2023* [PDF]. Retrieved August 16, 2025, from MEITY MeitY.
- *(Ministry of Electronics and Information Technology, 2023)* **Narrative citation:** According to the Ministry of Electronics and Information Technology (2023), the *Digital Personal Data Protection Act, 2023* was published as a Gazette notification on August 11, 2023, though it remains unenforced until separate commencement notifications are issued MeitYIndian Kanoon.
- *India's long wait for data protection law*. (2025, August 11). *The Economic Times*. Retrieved August 16, 2025, from Economic Times The Economic Times.
- *Data privacy law: Digital payment companies, NPCI seek pause on consent clause*. (2025, August 5). *The Economic Times*. Retrieved August 16, 2025, from Economic Times The Economic Times.

- *Exempt data fiduciaries from data law's provisions for training AI models: IAMAI to govt*. (2025, August 7). *The Economic Times*. Retrieved August 16, 2025, from Economic Times
- Wikipedia contributors. (2025, August 10). *Puttaswamy v. Union of India*. *Wikipedia*. Retrieved August 16, 2025, from https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India Wikipedia
- Wikipedia contributors. (2025). Dhananjaya Y. Chandrachud. *Wikipedia*. Retrieved August 16, 2025, from https://en.wikipedia.org/wiki/Dhananjaya_Y._Chandrachud Wikipedia
- Wikipedia contributors. (2025). *Shreya Singhal v. Union of India*. *Wikipedia*. Retrieved August 16, 2025, from https://en.wikipedia.org/wiki/Shreya_Singhal_v._Union_of_India Wikipedia
- The Hindu. (2015, March 25). *The judgment that silenced Section 66A*. *The Hindu*. Retrieved August 16, 2025, from https://www.thehindu.com/opinion/lead/The-judgment-that-silenced-Section-66A/article59870557.ece The Hindu
- Internet Freedom Foundation. (2022, October 12). *SC's direction: Stop prosecuting people under the unconstitutional S.66A*. Retrieved August 16, 2025, from https://internetfreedom.in/sc-direction-stop-prosecuting-people-under-the-unconstitutional-s-66a/ Internet Freedom Foundation
- Wikipedia contributors. (2025). *Digital Personal Data Protection Act, 2023*. *Wikipedia*. Retrieved August 16, 2025, from https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act%2C_2023 Wikipedia
- **Research Article** (on TikTok and algospeak practices): Steen, E., Yurechko, K., & Klug, D. (2023). *You can (not) say what you want: Using algospeak to contest and evade algorithmic content moderation on TikTok*. *Social Media + Society, 9*(3). https://doi.org/10.1177/20563051231194586 SAGE Journals
- **Narrative citation**: According to Steen, Yurechko, and Klug (2023), TikTok creators employ "algospeak" to evade content moderation—changing or inventing words like "le$bean" for "lesbian" to prevent takedown while still communicating meaningfully to their audience. SAGE Journals
- **Wikipedia Overview (for general definition)**: Wikipedia contributors. (2025, August 15). *Algospeak*. *Wikipedia*. Retrieved August 16, 2025, from https://en.wikipedia.org/wiki/Algospeak Wikipedia
- **News Coverage (emergent trend)**: Aleksic, A. (2025, July 24). Adam Aleksic on how algorithms are transforming the way we communicate. *Reuters*. Reuters

- **Narrative citation**: Aleksic (2025) highlights how users substitute terms like “unalive” for “suicide” and “seggs” for “sex” to bypass moderation filters, calling this phenomenon "algospeak." Reuters
- **News Article (Tech/privacy threat)**: The Online Safety Act isn’t just about age verification—end-to-end encryption is also at risk. (2025, August 14). *TechRadar*. TechRadar
- **News Article (status of encryption clause)**: Britain admits defeat in controversial fight to break encryption. (2023, February). *Wired*. WIRED
- **Narrative citation**: *Wired* (2023) notes that the UK government has suspended the clause threatening encryption due to lack of technically feasible solutions that preserve privacy. WIRED
- Sur, A. (2025, January 4). *DPDP rules: Big Tech must verify algorithms and keep specific personal data within India*. *Moneycontrol*. Retrieved August 16, 2025, from Moneycontrol (moneycontrol.com)
- Mondaq. (2025). *Enhancing privacy and security: Suggestions for the draft Digital Personal Data Protection Rules, 2025*. *Mondaq*. Retrieved August 16, 2025, from Mondaq (mondaq.com)
- Swati, A. (2024, May 23). *A leak of biometric police data is a sign of things to come*. *Wired*. Retrieved August 16, 2025, from WIRED (wired.com)
- Wikipedia contributors. (2025, August 1). *Aadhaar*. *Wikipedia*. Retrieved August 16, 2025, from Wikipedia (en.wikipedia.org)