

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

CONSTITUTIONAL PROTECTION OF INDIVIDUAL RIGHTS IN THE DIGITAL ERA: EMERGING CHALLENGES TO PRIVACY AND FREEDOM OF EXPRESSION

AUTHORED BY - UMANG KAMBOJ

Table of Contents

Abstract

I. Introduction

II. Literature Review

III. Analysis and Discussion

A. Constitutional Foundations: From Reticence to Recognition

B. Freedom of Expression in the Digital Public Square

C. State Surveillance and the Absence of an Oversight Framework

D. The Digital Personal Data Protection Act, 2023 and the 2025 Rules

E. Artificial Intelligence, Algorithmic Governance and New Frontiers

F. Comparative Perspectives

G. Data Localisation, Cross-Border Transfers and Digital Sovereignty

H. Hate Speech, Misinformation and the Limits of Platform Self-Regulation

I. Towards a Layered Proportionality Framework

IV. Findings

V. Recommendations

VI. Conclusion

References

List of Figures

Figure 1: Growth of Internet Subscribers in India, 2021–2025 (TRAI data)

Figure 2: Timeline of the Evolution of Constitutional Privacy and Digital-Rights Jurisprudence in India (1954–2025)

Figure 3: Phased Implementation Timeline — DPDP Act, 2023 and Rules, 2025

Figure 4: The Puttaswamy Four-Part Proportionality Test, with Proposed Layered Extensions

Abstract

*The transition from an analogue to an algorithmically mediated society has placed unprecedented strain on the constitutional architecture built to protect individual liberty. This paper examines how constitutional courts, legislatures and regulators have attempted to reconcile the right to privacy and the freedom of speech and expression with the imperatives of a data-driven economy, platform governance and artificial intelligence. Taking Indian constitutional law as the primary frame of reference and situating it within comparative jurisprudence from the United States and the European Union, the paper traces the doctrinal journey from *Kharak Singh v. State of Uttar Pradesh* and *M.P. Sharma v. Satish Chandra*, through the watershed recognition of informational privacy as a facet of Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, to the operationalisation of statutory data protection through the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. It further analyses the intermediary liability regime under Section 79 of the Information Technology Act, 2000 as interpreted in *Shreya Singhal v. Union of India*, the 2021 Intermediary Guidelines, and subsequent judicial responses to fact-checking and content-moderation mandates. The paper argues that while Indian courts have constitutionalised privacy as an intrinsic facet of dignity and liberty, the legislative and executive follow-through remains uneven, particularly with respect to surveillance oversight, algorithmic accountability and the proportionality of speech restrictions. Drawing on comparative material — the General Data Protection Regulation, 2016, *Carpenter v. United States* and *Google Spain SL v. AEPD* — the paper develops a framework of layered proportionality for evaluating digital-era restrictions on rights. It concludes with recommendations for an independent data protection authority insulated from executive control, judicially supervised surveillance reform, algorithmic transparency obligations, and a re-calibrated intermediary liability regime that safeguards both dignity and discourse. The analysis is intended to contribute to the emerging jurisprudence on constitutionalism in the algorithmic age and to inform ongoing legislative and regulatory reform.*

Keywords: Right to Privacy; Freedom of Speech and Expression; Article 21; Digital Personal Data Protection Act, 2023; Intermediary Liability; Data Protection; Artificial Intelligence; Surveillance; Proportionality; Constitutionalism.

I. Introduction

Constitutions are written for an imagined future, yet few constitution-makers of the twentieth century could have anticipated a world in which a single hand-held device continuously records location, communication, biometric and behavioural data, and transmits it to servers controlled by private corporations and, occasionally, the State. The digital revolution has not merely added a new medium of communication; it has altered the very conditions under which the constitutional guarantees of privacy and free expression operate. Personal data has become, in the oft-repeated phrase, "*the new oil*" of the information economy, while social media platforms have become the principal public square for the exercise of the freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India.¹

This paper interrogates the adequacy of constitutional doctrine — both judge-made and statutory — in addressing the twin challenges that the digital era poses to individual rights: first, the erosion of informational privacy through mass data collection, algorithmic profiling and State surveillance; and second, the precarious status of free expression in a discourse ecosystem mediated by private intermediaries and, increasingly, by content-recommendation algorithms and generative artificial intelligence. The Supreme Court of India's declaration in *Justice K.S. Puttaswamy (Retd.) v. Union of India* that the right to privacy is intrinsic to Article 21² marked a doctrinal inflection point, yet the six-year interval between that judgment and the enactment of the Digital Personal Data Protection Act, 2023³ — and the further two-year delay before the notification of the Digital Personal Data Protection Rules, 2025 on 13 November 2025⁴ — illustrates a persistent gap between constitutional pronouncement and statutory implementation.

The paper proceeds in six further parts. Part II surveys the existing literature on constitutional privacy, digital free expression and platform governance. Part III undertakes a doctrinal and comparative analysis of the constitutional and statutory framework, organised around privacy jurisprudence, free-expression jurisprudence, intermediary liability, State surveillance, the new data protection regime, and emerging challenges posed by artificial

¹See generally Jack M. Balkin, "Free Speech is a Triangle" 118 Columbia Law Review 2011 (2018) (describing the shift from a dyadic State-speaker model of free expression to a triadic model involving platforms as intermediating gatekeepers).

²*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (nine-judge bench).

³The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), assented to on 11 August 2023.

⁴Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology, Gazette Notification dated 13 November 2025; implementation is staggered, with the Data Protection Board's substantive powers and consent-manager provisions becoming effective in phases through 13 May 2027.

intelligence. Part IV distils the principal findings. Part V offers policy and doctrinal recommendations. Part VI concludes.

II. Literature Review

The conceptual foundations of the right to privacy in Anglo-American jurisprudence trace back to Samuel Warren and Louis Brandeis's canonical essay, which conceived privacy as "*the right to be let alone*."⁵ This formulation, while foundational, proved inadequate for the informational age, prompting Alan Westin's reconceptualisation of privacy as informational self-determination — the claim of individuals to control when, how and to what extent information about them is communicated to others.⁶ Daniel Solove's taxonomic approach further disaggregated privacy harms into distinct categories of information collection, processing, dissemination and invasion, offering courts a more granular analytical vocabulary than the undifferentiated "*right to be let alone*."⁷

Indian scholarship has largely tracked the doctrinal evolution from the restrictive reading of personal liberty in *A.K. Gopalan v. State of Madras*⁸ through the golden triangle established in *Maneka Gandhi v. Union of India*⁹ to the recognition of privacy in *Govind v. State of Madhya Pradesh*¹⁰ and *R. Rajagopal v. State of Tamil Nadu*¹¹. Kurlwal and Shreyansh trace this trajectory to argue that the *Puttaswamy* verdict was less a sudden invention than the culmination of five decades of incremental doctrinal development, and note that the Digital Personal Data Protection Act, 2023 was itself a direct legislative response to the Court's call for a data protection framework.¹² Dhar and Nath similarly document how the judiciary's privacy jurisprudence expanded in tandem with the growth of State surveillance capacity, culminating in *Anuradha Bhasin v. Union of India*, where the Court held that access to the internet is integral to the exercise of speech, expression and trade under Articles 19(1)(a) and 19(1)(g).¹³

⁵Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4(5) Harvard Law Review 193-220 (1890).

⁶Alan F. Westin, *Privacy and Freedom* (Atheneum, New York, 1967).

⁷Daniel J. Solove, "A Taxonomy of Privacy" 154 University of Pennsylvania Law Review 477 (2006).

⁸*A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.

⁹*Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

¹⁰*Govind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

¹¹*R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (the "Auto Shankar" case, recognising a common-law and constitutional right to privacy against unauthorised publication).

¹²Anupam Kurlwal and Shreyansh, "Evolution of the Right to Privacy in India: Constitutional Perspective and Judicial Approach" 5(4) ShodhKosh: Journal of Visual and Performing Arts 1985 (2024).

¹³Dr Rumi Dhar and Sonia Nath, "Digital Surveillance and Civil Rights: Assessing the Impact on Privacy" 5(1) Chanakya Law Review (Jan-June 2024), citing *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

On the free-expression side, Jack Balkin's account of the shift from a dyadic to a "*triadic*" model of speech governance — in which platforms mediate between speakers and the State, and are themselves increasingly regulated as quasi-public utilities — has shaped comparative scholarship on intermediary liability.¹⁴ Indian commentary on the *Shreya Singhal* judgment has similarly emphasised the Court's adoption of the vagueness and overbreadth doctrines to strike down Section 66A of the Information Technology Act, 2000, while noting that subordinate legislation such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 has continued to generate constitutional friction by resurrecting vague, discretionary content-removal standards through executive rule-making rather than primary legislation.¹⁵

A distinct strand of literature addresses the tension between the right to information and the right to privacy following the 2023 amendment to Section 8(1)(j) of the Right to Information Act, 2005, which converted a qualified exemption for personal information into what commentators describe as an "*absolute*" exemption, thereby narrowing the transparency regime in the name of data protection.¹⁶ Finally, an emerging body of writing addresses algorithmic discrimination and the "*right to be forgotten*" in Indian law, noting the absence of binding Supreme Court authority and the resulting inconsistency between High Court decisions such as *Vysakh K.G. v. Union of India*¹⁷ and subsequent references pending before the Supreme Court on the erasure of personal information from public judicial records.¹⁸ This paper builds on these strands by integrating privacy, free-expression and algorithmic-governance literature into a single proportionality-based analytical framework, and by extending the analysis to the phased implementation of the 2025 Rules and to comparative developments through 2026.

¹⁴Balkin, *supra* note 1.

¹⁵See generally Abhinav Sekhri and Apar Gupta, "Section 66A and Its Afterlife," analysed in Supreme Court Observer, "Section 66A: 4 Must Reads" (2023).

¹⁶See Krishna, "Interface between Right to Information and Right to Privacy in the Backdrop of the Digital Personal Data Protection Act, 2023" ILI Law Review, Summer Issue 261 (2024).

¹⁷*Vysakh K.G. v. Union of India*, 2022 SCC OnLine Ker 7337.

¹⁸See Inder Jain, "Right to Be Forgotten in India: Constitutional Privacy, Judicial Limits, and the Balance with Free Speech," Legal Service India (December 2025).

III. Analysis and Discussion

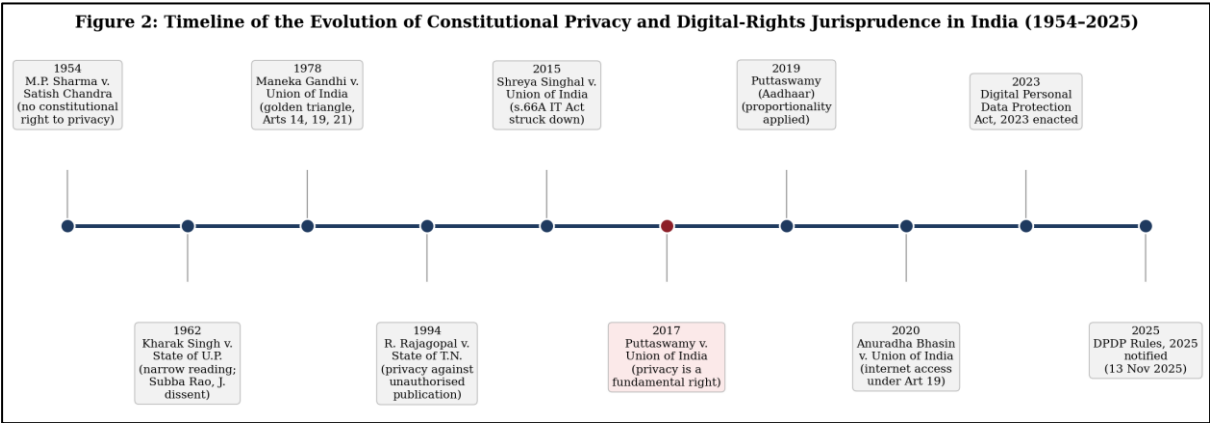


Figure 2: Timeline of the evolution of constitutional privacy and digital-rights jurisprudence in India (1954–2025), showing the doctrinal shift from M.P. Sharma's rejection of a constitutional privacy right to the DPDP Rules, 2025.

A. Constitutional Foundations: From Reticence to Recognition

India's constitutional text contains no express reference to a right to privacy. The framers, mindful of colonial-era surveillance and the felt need for a strong developmental State, left privacy to be inferred — if at all — from the residual guarantees of Part III. Early jurisprudence was hostile: in *M.P. Sharma v. Satish Chandra*, an eight-judge bench held that the Constitution contained no analogue to the American Fourth Amendment and therefore no constitutional limitation on search and seizure.¹⁹ In *Kharak Singh v. State of Uttar Pradesh*, a six-judge bench went further, upholding police surveillance regulations while a lone dissent by Justice Subba Rao presciently observed that the right to personal liberty was "*a compendious term*" that took in a variety of rights, including the right to be free of unauthorised intrusion into the home.²⁰ That dissent, vindicated over five decades later, foreshadowed the transformative approach the Court would eventually adopt.

The turning point began with *Maneka Gandhi*, which read Articles 14, 19 and 21 as a mutually reinforcing "*golden triangle*" rather than isolated silos, and required that any procedure depriving a person of life or liberty be fair, just and reasonable.²¹ Building on this, *Govind* cautiously recognised a limited right to privacy as an emanation of personal liberty, subject to compelling State interest,²² and *R. Rajagopal* extended protection to prevent

¹⁹M.P. Sharma v. Satish Chandra, 1954 SCR 1077.
²⁰Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.
²¹Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
²²Govind v. State of Madhya Pradesh, (1975) 2 SCC 148.

unauthorised publication of personal facts, while carving out a robust exception for public officials and matters of public record.²³ These decisions, however, lacked the authoritative force of a larger bench and could not definitively displace *M.P. Sharma* and *Kharak Singh*.

The question was forced by litigation challenging the Aadhaar biometric identification scheme. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge bench unanimously held that the right to privacy is a fundamental right, protected as an intrinsic part of the right to life and personal liberty under Article 21 and as part of the freedoms guaranteed by Part III of the Constitution, expressly overruling *M.P. Sharma* and the majority in *Kharak Singh*.²⁴ The Court located privacy in Article 21's guarantee of dignity and identified it as a necessary condition for the meaningful exercise of other fundamental freedoms, including freedom of expression, association and movement. Importantly, the judgment recognised informational privacy — the ability to control the dissemination of personal data — as one of three overlapping zones of privacy, alongside decisional and spatial privacy,²⁵ and articulated a four-part test for permissible restrictions: legality, legitimate State aim, proportionality (a rational nexus between means and ends, with the least restrictive alternative), and procedural safeguards against abuse.²⁶ This proportionality standard, adapted substantially from South African and German constitutional doctrine, has since become the operative test for evaluating both privacy-restricting and speech-restricting State action in India.

A follow-on constitution bench applied this framework in the Aadhaar judgment, upholding the linkage of Aadhaar to welfare subsidies and income tax filings as a proportionate measure serving the legitimate aim of preventing leakage in public distribution, while striking down mandatory Aadhaar-seeding for bank accounts and mobile SIM connections as disproportionate and lacking sufficient legislative backing.²⁷ The bifurcated outcome illustrates both the analytical power and the indeterminacy of proportionality review: reasonable jurists applying the same four-part test reached sharply divergent conclusions on different facets of the same scheme, underscoring the need for legislative concretisation of the standard — a need only partially met by the 2023 Act discussed in Part III(F) below.

²³R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

²⁴Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, paras 3(A)-3(J) (Chandrachud, J., for four judges) and concurring opinions of Khehar, C.J., Chelameswar, Bobde, Nariman, Sapre, Kaul and Nazeer, JJ.

²⁵Ibid., per Chandrachud, J., paras 141-142 (identifying "informational privacy" as distinct from bodily and decisional autonomy, and noting its particular vulnerability to State and non-State digital data processing).

²⁶Ibid., per Chandrachud, J., para 310; see also Sanjay Kishan Kaul, J., para 71 (independently formulating a similar four-fold proportionality standard).

²⁷Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1.

B. Freedom of Expression in the Digital Public Square

Article 19(1)(a) guarantees the freedom of speech and expression, subject to reasonable restrictions under Article 19(2) on grounds including the sovereignty and integrity of India, State security, public order, decency, morality, contempt of court, defamation and incitement to an offence. The migration of public discourse to digital platforms has tested the boundaries of this framework in three principal respects: the criminalisation of online speech, State-directed content removal, and intermediary liability.

The most significant judicial intervention remains *Shreya Singhal v. Union of India*, in which the Supreme Court struck down Section 66A of the Information Technology Act, 2000 — which criminalised sending information that was "*grossly offensive*" or of "*menacing character*" through a computer resource — as unconstitutionally vague and overbroad, holding that it fell outside the eight subject-matter heads enumerated in Article 19(2) and possessed a chilling effect that swept in innocent as well as culpable speech.²⁸ The Court also read down Section 69A (blocking of content) and, critically, Section 79 (intermediary safe harbour), holding that an intermediary's obligation to remove content upon acquiring "*actual knowledge*" could only be triggered by a court order or a notification from an appropriate government agency — not by unilateral private complaint — thereby averting a regime of privatised, extra-judicial censorship.²⁹

Yet *Shreya Singhal*'s protective architecture has been tested by subsequent executive rule-making. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under Section 87 of the Act, impose due-diligence obligations on significant social media intermediaries, including traceability requirements for the "*first originator*" of messages, mandatory grievance-redressal officers, and a three-tier regulatory mechanism for digital news and OTT content.³⁰ Critics have argued that provisions requiring proactive removal of content on vague grounds of "*public order*" or "*decency*" echo the overbreadth that proved fatal to Section 66A, but do so through subordinate legislation that escapes the same level of parliamentary scrutiny.³¹ This tension crystallised in litigation over the 2023 amendment establishing a government "*Fact Check Unit*" empowered to flag online content relating to the Central Government as "*fake, false or misleading*," with non-compliant

²⁸*Shreya Singhal v. Union of India*, (2015) 5 SCC 1, paras 78-83, 94.

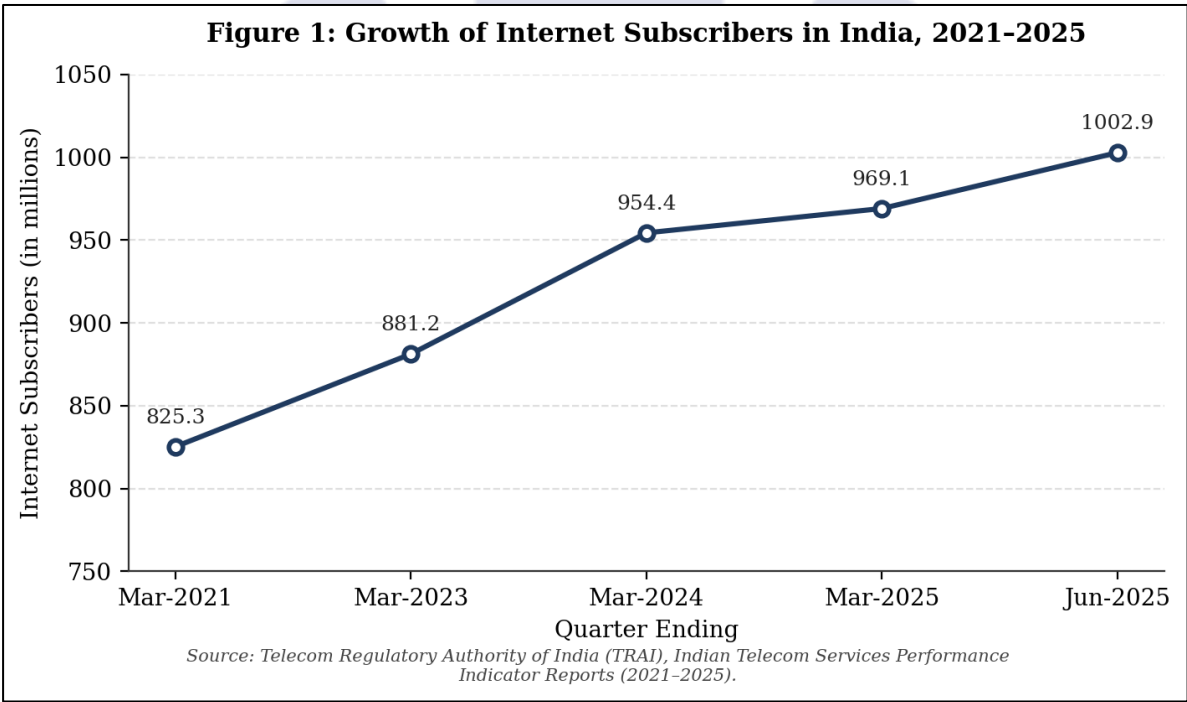
²⁹*Ibid.*, paras 117, 122.

³⁰Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified 25 February 2021.

³¹Pratap Vikram Singh, discussed in Supreme Court Observer, "Section 66A: 4 Must Reads" (2023) (drawing parallels between the vagueness of Section 66A and that of the 2021 Intermediary Guidelines).

intermediaries losing safe-harbour protection. In *Kunal Kamra v. Union of India*, the Bombay High Court struck down the Fact Check Unit rule as unconstitutional, holding that it delegated to the executive an unbridled power to be the sole arbiter of truth regarding its own affairs, in violation of Article 19(1)(a) and Article 14, and that the resulting chilling effect on satire, opinion and commentary was disproportionate.³²

A further dimension is access to the internet itself. In *Anuradha Bhasin v. Union of India*, arising from prolonged internet shutdowns in Jammu and Kashmir, the Supreme Court held that the freedom of speech and expression and the freedom to carry on trade and business over the internet are constitutionally protected under Articles 19(1)(a) and 19(1)(g), that indefinite suspension of internet services is impermissible, and that suspension orders must satisfy the tests of necessity and proportionality and are subject to periodic judicial review.³³ The judgment situates connectivity itself as a precondition for the exercise of digital-age speech rights, extending the proportionality framework of *Puttaswamy* from data privacy to network access.



*Figure 1: Growth of internet subscribers in India, 2021–2025 (TRAI data). The scale of connectivity underscores why the Supreme Court in *Anuradha Bhasin* treated internet access as integral to Articles 19(1)(a) and 19(1)(g), and why platform governance now affects an audience approaching one billion users.*

³²Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023, Bombay High Court; see also Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.
³³Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, paras 105, 137, 145.

C. State Surveillance and the Absence of an Oversight Framework

Notwithstanding *Puttaswamy*'s insistence on legality, necessity and procedural safeguards as preconditions for any privacy-restricting State action, India's surveillance architecture remains largely governed by the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 — both pre-digital or early-digital instruments retrofitted through executive rules rather than a purpose-built legislative framework. Interception of communications under Section 5(2) of the Telegraph Act, and monitoring, decryption and blocking under Sections 69, 69A and 69B of the Information Technology Act, are authorised through executive orders reviewed by an internal Review Committee composed of executive officials, without independent judicial or parliamentary oversight.³⁴ Revelations concerning the deployment of commercial spyware against journalists, activists and opposition politicians renewed calls for judicial oversight; the Supreme Court's response, in the Pegasus matter, was limited to constituting a technical committee to examine specific instances of infection, without addressing the systemic absence of independent authorisation for surveillance.³⁵ The persistence of executive self-authorisation stands in contrast to the *Puttaswamy* requirement of "procedural safeguards against abuse" and represents, in the view of this paper, the most significant unaddressed gap between constitutional doctrine and operative law.

D. The Digital Personal Data Protection Act, 2023 and the 2025 Rules

The Digital Personal Data Protection Act, 2023 is India's first comprehensive statute governing the processing of digital personal data, enacted to give legislative effect to the informational-privacy dimension of *Puttaswamy*.³⁶ It establishes a consent-based processing regime built around the roles of "Data Fiduciary" (the entity determining the purpose and means of processing, a formulation borrowed from the European Union's General Data Protection Regulation) and "Data Principal" (the individual to whom the data relates), grants data principals the rights to access, correction, erasure and grievance redressal, and creates a Data Protection Board of India with adjudicatory and penalty-imposing functions.³⁷ Notably, unlike the GDPR, the Act does not create a heightened category of "sensitive personal data" attracting

³⁴Indian Telegraph Act, 1885, s 5(2); Information Technology Act, 2000, ss 69, 69A, 69B; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

³⁵*Manohar Lal Sharma v. Union of India*, (2022) 8 SCC 1 (Pegasus spyware matter; technical committee appointed to investigate deployment of surveillance software, without adjudicating the constitutionality of the surveillance framework itself).

³⁶The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Preamble and Statement of Objects and Reasons.

³⁷*Ibid.*, ss 2(i), 2(h), 11-14 (data principal rights), 18-19 (Data Protection Board).

stricter obligations, applying a uniform standard to all personal data regardless of its intrinsic sensitivity — a design choice that has drawn scholarly criticism for under-protecting categories such as health, sexual orientation and biometric data.³⁸

The Act's practical effect was long deferred: although assented to in August 2023, its substantive provisions remained largely dormant pending subordinate rules. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025 following a ten-month consultation on draft rules published in January 2025, during which the Ministry of Electronics and Information Technology received 6,915 stakeholder submissions.³⁹ The Rules operationalise consent architecture, breach-notification timelines (requiring detailed notification to the Board within seventy-two hours of a fiduciary becoming aware of a breach), cross-border data transfer conditions, and heightened protections for children's data and persons with disabilities, including verifiable parental consent requirements.⁴⁰ Implementation is staggered: provisions establishing the Data Protection Board and the Government's rule-making powers took immediate effect; provisions on consent-manager registration become effective in November 2026; and the remaining provisions, including the core data-fiduciary obligations, are deferred to 13 May 2027 — nearly a decade after *Puttaswamy*.⁴¹ This phased approach, while administratively pragmatic, leaves citizens without an enforceable statutory remedy for data misuse during the transition period, a lacuna this paper returns to in Part V.

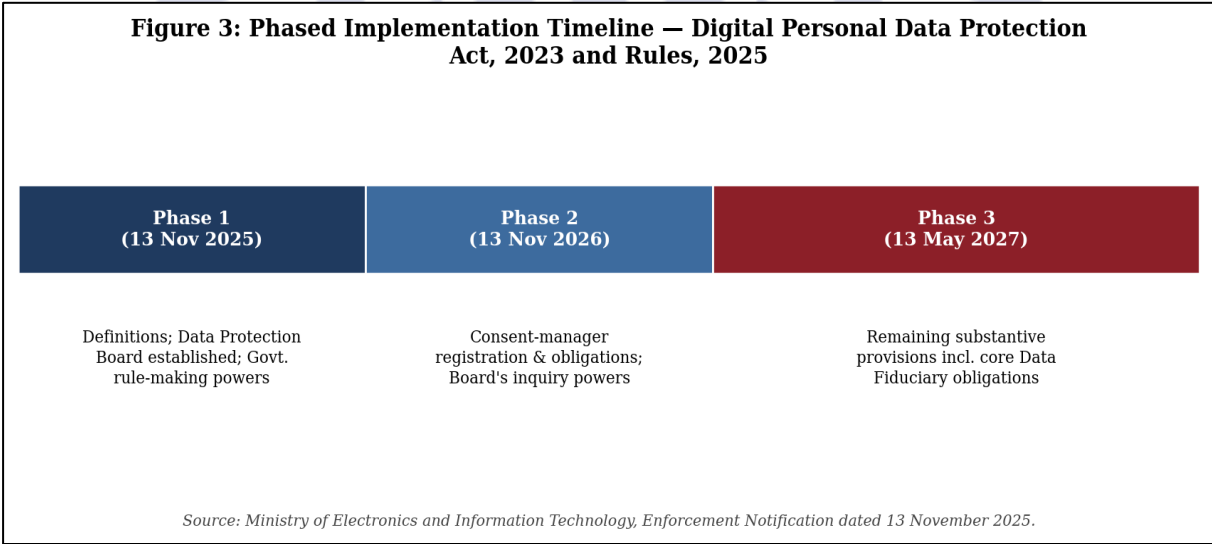


Figure 3: Phased implementation timeline of the Digital Personal Data Protection Act, 2023

³⁸See Kurlwal and Shreyansh, *supra* note 8 at 1991-1992.
³⁹Ministry of Electronics and Information Technology, Government of India, Press Information Bureau release, "DPDP Rules, 2025 Notified" (17 November 2025).
⁴⁰Digital Personal Data Protection Rules, 2025, rr 6-7 (breach notification), 10-11 (children's data and persons with disabilities).
⁴¹See DPDP Rules, 2025 Enforcement Notification dated 13 November 2025; timeline summarised in Lexology, "Digital Personal Data Protection Rules 2025 – Highlights" (17 November 2025).

and Rules, 2025, as notified by the Ministry of Electronics and Information Technology on 13 November 2025.

Two further features merit critical attention. First, Section 17 of the Act grants the Central Government broad power to exempt itself and its instrumentalities from the Act's obligations in the interests of sovereignty, security, public order and prevention of offences, without the judicially supervised authorisation contemplated by *Puttaswamy*'s legality and procedural-safeguard prongs.⁴² Second, the 2023 Act amended Section 8(1)(j) of the Right to Information Act, 2005 to remove the qualifying language that had earlier permitted disclosure of personal information where the larger public interest justified it, replacing it with a blanket exemption for all personal information. Commentators have observed that this recalibration, while data-protective, sacrifices the transparency function of the RTI regime and may itself require proportionality scrutiny as a restriction on the constitutionally recognised right to information under Article 19(1)(a).⁴³

E. Artificial Intelligence, Algorithmic Governance and New Frontiers

The most recent phase of the digital-rights debate concerns generative artificial intelligence and algorithmic decision-making. Automated content-recommendation, credit-scoring, predictive-policing and facial-recognition systems raise privacy and expression concerns that exceed the categories contemplated by either *Puttaswamy* or the 2023 Act: algorithmic opacity frustrates the data principal's right to meaningful access and correction; automated content curation shapes the "*marketplace of ideas*" in ways not easily attributable to identifiable State action, complicating Article 19 analysis premised on State-speaker confrontation; and large-scale facial-recognition deployment by law-enforcement agencies operates largely outside statutory authorisation, raising the same legality concerns identified in the surveillance context above.⁴⁴ India's approach to AI governance remains predominantly advisory rather than binding: the draft National Strategy for Artificial Intelligence and subsequent policy instruments emphasise "*responsible AI*" principles without imposing enforceable transparency or audit obligations comparable to the European Union's Artificial Intelligence Act, which entered into force in 2024 and imposes risk-tiered obligations, including a prohibition on certain forms of biometric categorisation and real-time remote

⁴²The Digital Personal Data Protection Act, 2023, s 17(2).

⁴³See Krishna, *supra* note 12 at 265-268.

⁴⁴See generally discussion of "algorithmic discrimination" as an emerging right in Indian scholarship, e.g., the proposed "right to freedom from algorithmic discrimination" discussed in TIJER, "Emerging Rights in the Digital Age" 12(6) (June 2025).

biometric identification in public spaces.⁴⁵ The absence of a comparable binding instrument in India means that algorithmic accountability currently depends on the general, and untested, application of the 2023 Act's fairness and purpose-limitation principles to automated processing — an application the statute does not expressly address.

F. Comparative Perspectives

The European Union's General Data Protection Regulation remains the most influential comparative template, establishing an omnibus regime built on data-minimisation, purpose-limitation, and accountability principles, enforced by independent supervisory authorities in each member State with the power to impose fines of up to four per cent of global annual turnover.⁴⁶ The Court of Justice of the European Union's recognition of a qualified "*right to be forgotten*" in *Google Spain SL v. Agencia Espanola de Proteccion de Datos* — requiring search engines to de-list links to lawfully published information where it is inadequate, irrelevant or excessive in relation to processing purposes, subject to a public-interest balancing test — offers a template that Indian High Courts have invoked, inconsistently, in the absence of Supreme Court guidance or express statutory recognition.⁴⁷

United States Fourth Amendment jurisprudence offers a contrasting model built on the reasonable-expectation-of-privacy doctrine rather than an omnibus data-protection statute. In *Carpenter v. United States*, the Supreme Court of the United States held that the government's acquisition of historical cell-site location information from a wireless carrier constitutes a search under the Fourth Amendment, requiring a warrant supported by probable cause, and declined to extend the third-party doctrine — under which information voluntarily shared with a third party loses Fourth Amendment protection — to the pervasive, involuntarily generated location data produced by mobile-phone use.⁴⁸ The decision's recognition that the sheer comprehensiveness of digitally generated data can itself trigger constitutional protection, irrespective of formal ownership or third-party custody, resonates closely with the Indian Supreme Court's recognition of informational privacy in *Puttaswamy*, and offers a useful doctrinal bridge for evaluating India's own third-party surveillance practices, including law-

⁴⁵Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Arts 5, 6 and Annex III.

⁴⁶Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Arts 5, 51, 83.

⁴⁷*Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD)*, Case C-131/12, [2014] ECR (CJEU); see *Vysakh K.G. v. Union of India*, 2022 SCC OnLine Ker 7337 (restrictive approach); contrast more permissive approaches of other High Courts, discussed in Inder Jain, *supra* note 14.

⁴⁸*Carpenter v. United States*, 585 U.S. 296 (2018).

enforcement access to platform and telecom data under Section 91 of the Code of Criminal Procedure and its successor, Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023.⁴⁹

G. Data Localisation, Cross-Border Transfers and Digital Sovereignty

A further constitutional dimension, distinct from but related to individual privacy, concerns the territorial governance of data — the question of where personal data may be stored and processed, and under whose legal jurisdiction. The Reserve Bank of India's 2018 directive requiring payment system operators to store the entirety of payment-system data exclusively in India was an early instance of sector-specific data localisation, justified on grounds of regulatory access and national security rather than individual privacy as such.⁵⁰ The Digital Personal Data Protection Act, 2023 adopts a comparatively liberal, negative-list approach to cross-border transfer, permitting transfer of personal data to any country or territory outside India except those specifically restricted by the Central Government by notification — a marked departure from the more restrictive, whitelist-based localisation proposals contained in earlier draft data protection bills.⁵¹ While this approach eases compliance burdens for the digital economy and aligns India more closely with the GDPR's adequacy-based transfer model, it also means that the ultimate scope of cross-border restriction is left to executive notification rather than legislative standard-setting, raising the same institutional-design concern — delegation of rights-affecting decisions to unreviewed executive discretion — identified elsewhere in this paper with respect to Section 17 exemptions and the Intermediary Guidelines. The interaction between data localisation, national-security justifications and the proportionality standard of Puttaswamy remains, as yet, untested before the higher judiciary.

H. Hate Speech, Misinformation and the Limits of Platform Self-Regulation

The digital public square has also amplified categories of speech harm that pre-date the internet but acquire distinct characteristics online: hate speech capable of rapid, algorithmically amplified dissemination, and misinformation capable of influencing electoral and public-health outcomes at scale. Indian law addresses these harms through a patchwork of provisions — Sections 153A, 295A and 505 of the erstwhile Indian Penal Code (now substantially reproduced in the Bharatiya Nyaya Sanhita, 2023), the defamation provisions of the same code, and the due-diligence obligations under the Intermediary Guidelines, 2021 requiring platforms

⁴⁹Bharatiya Nagarik Suraksha Sanhita, 2023, s 94 (power to summon production of documents, including electronic records).

⁵⁰Reserve Bank of India, Notification RBI/2017-18/153, "Storage of Payment System Data" (6 April 2018).

⁵¹The Digital Personal Data Protection Act, 2023, s 16.

to act on user complaints regarding specified categories of unlawful content.⁵² The doctrinal challenge is that content-moderation decisions taken by platforms in response to these obligations are rarely subject to the same constitutional scrutiny as direct State action, because the proximate decision-maker is a private entity. Balkin's triadic model is instructive here: platforms occupy an intermediary position in which government pressure — whether through binding rules, informal requests, or the threat of safe-harbour withdrawal — can achieve speech-restrictive outcomes that would be constitutionally impermissible if enacted directly, a phenomenon commentators term "*jawboning*" or indirect censorship.⁵³ The Bombay High Court's invalidation of the Fact Check Unit rule in *Kunal Kamra* is significant precisely because it recognised this dynamic, holding that a government-controlled arbiter of "*truth*" backed by the coercive threat of safe-harbour withdrawal was constitutionally indistinguishable from direct censorship, notwithstanding the formally private status of the intermediaries actually removing the content.

I. Towards a Layered Proportionality Framework

Synthesising the preceding analysis, this paper argues that Indian courts and legislators require a more granular, "*layered*" application of the *Puttaswamy* proportionality standard specific to the digital context. The four established prongs — legality, legitimate aim, necessity/proportionality (least restrictive means), and procedural safeguards⁵⁴ — must be supplemented, in the digital setting, by two further inquiries: (i) an assessment of *aggregation risk*, recognising that discrete data points, individually innocuous, generate disproportionate privacy harm when algorithmically combined (the insight underlying *Carpenter*); and (ii) an assessment of *chilling effect on collective discourse*, recognising that content-moderation and surveillance measures affecting digital platforms restrict not only the individual target but the wider ecosystem of public deliberation (the insight underlying *Shreya Singhal* and *Anuradha Bhasin*). Applied together, these six inquiries would provide a more predictable and rigorous standard than the current ad hoc application of proportionality, and would better equip courts to evaluate novel digital-era measures — algorithmic profiling, biometric surveillance, platform content moderation — that do not map neatly onto pre-digital categories of search,

⁵²Bharatiya Nyaya Sanhita, 2023, ss 196, 299, 356 (successor provisions to IPC ss 153A, 295A, 499-500); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r 3(1)(d).

⁵³Balkin, *supra* note 1 at 2020-2027 (describing government leverage over private infrastructure providers as a distinct free-speech concern requiring "new-school" doctrinal responses beyond classical First Amendment/Article 19 State-action analysis).

⁵⁴K.S. Puttaswamy, *supra* note 3, para 310 (Chandrachud, J.).

seizure or censorship.

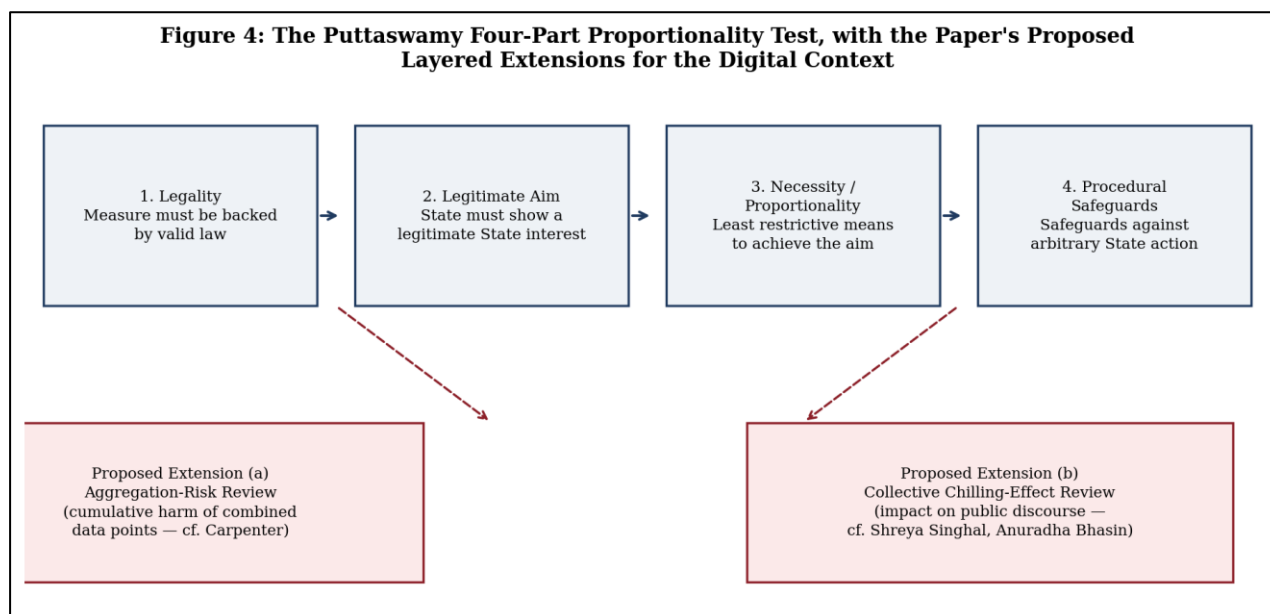


Figure 4: The Puttaswamy four-part proportionality test (legality, legitimate aim, necessity/proportionality, procedural safeguards), together with the two extensions — aggregation-risk review and collective chilling-effect review — proposed in this paper for digital-era rights adjudication.

IV. Findings

1. The Indian judiciary has firmly constitutionalised both informational privacy and digital free expression, but through a proportionality standard that remains analytically underdeveloped for algorithmic-era harms such as data aggregation and automated profiling.
2. A significant implementation gap persists between constitutional pronouncement and statutory operationalisation: nearly a decade separates Puttaswamy (2017) from the full, phased enforcement of the Digital Personal Data Protection Act, 2023, scheduled to conclude only in May 2027.
3. State surveillance remains governed by pre-constitutional and early-digital statutes (the Telegraph Act, 1885 and the Information Technology Act, 2000) that rely on internal executive review rather than independent judicial or parliamentary authorisation, in tension with Puttaswamy's procedural-safeguards requirement.
4. Executive rule-making — particularly the Intermediary Guidelines, 2021 and the since-invalidated Fact Check Unit rule — has repeatedly reintroduced the vagueness and overbreadth infirmities that the Supreme Court excised from primary legislation in

Shreya Singhal, suggesting that subordinate legislation has become a workaround for constitutional constraints on speech regulation.

5. The Digital Personal Data Protection Act, 2023 grants the Central Government broad self-exempting power under Section 17 and treats all personal data uniformly without a heightened category for sensitive personal data, diverging from comparative models such as the GDPR and diluting the protective force of the statute.
6. India lacks a binding, rights-specific regulatory framework for artificial intelligence and algorithmic decision-making, relying instead on advisory principles, in contrast to the European Union's risk-tiered Artificial Intelligence Act, 2024.
7. Right-to-be-forgotten jurisprudence remains fragmented across High Courts in the absence of Supreme Court authority or express statutory recognition, producing inconsistent outcomes for similarly situated litigants.
8. The Digital Personal Data Protection Act, 2023 addresses cross-border data transfer through a liberal negative-list model that delegates the ultimate scope of restriction to unreviewed executive notification, replicating the institutional-design concerns identified with respect to Section 17 exemptions and the Intermediary Guidelines.
9. Content-moderation obligations imposed on private platforms function as an indirect mechanism for speech restriction that frequently escapes the constitutional scrutiny applicable to direct State action, a dynamic starkly illustrated by the judicial invalidation of the government Fact Check Unit rule in Kunal Kamra.

V. Recommendations

Independent Data Protection Board. The composition and appointment process of the Data Protection Board of India should be insulated from executive control through a broad-based selection committee including judicial and civil-society representation, on the model of other independent regulators, to secure the institutional independence contemplated but not guaranteed by the 2023 Act.

Judicially Supervised Surveillance Reform. Parliament should enact a dedicated surveillance-authorisation statute requiring prior judicial (rather than purely executive) sanction for interception, monitoring and decryption orders, consistent with the legality and procedural-safeguards prongs of Puttaswamy and the reasoning in Carpenter, replacing the current Review Committee mechanism under the Telegraph Act and Information Technology Act.

Narrowing Section 17 Exemptions. The blanket government self-exemption under

Section 17(2) of the Digital Personal Data Protection Act, 2023 should be narrowed and made subject to specific, proportionate, and time-bound notification requirements, with periodic legislative review, to prevent the exemption from swallowing the rule.

Sensitive Personal Data Category. The Act should be amended to introduce a heightened category of sensitive personal data (health, sexual orientation, caste, religious belief, biometric and genetic data) attracting stricter consent and security obligations, aligning Indian law with comparative best practice under the GDPR.

Codifying the Right to Be Forgotten. Parliament or the Data Protection Board should issue binding rules operationalising a right to erasure/de-listing modelled on Google Spain, with a structured public-interest balancing test, to resolve the current inconsistency across High Courts.

Algorithmic Transparency Obligations. India should adopt binding, risk-tiered obligations for high-impact automated decision-making systems (credit scoring, predictive policing, facial recognition, content recommendation), including mandatory impact assessments and a meaningful right to explanation, rather than relying solely on advisory AI governance principles.

Legislating Intermediary Standards. Content-moderation obligations currently imposed through the Intermediary Guidelines should be elevated to primary legislation, incorporating the vagueness and overbreadth safeguards articulated in *Shreya Singhal*, with any fact-checking or content-classification function vested in a body independent of the government whose own conduct is subject to scrutiny.

Accelerating Phased Implementation. The Central Government should compress the current implementation timeline for the Digital Personal Data Protection Rules, 2025, or in the interim provide an enforceable transitional remedy for data-principal grievances, so that citizens are not left without recourse during the multi-year phased rollout.

Legislative Standard for Cross-Border Transfer Restrictions. The power to restrict cross-border data transfer under Section 16 of the 2023 Act should be exercised against express, published legislative criteria (such as adequacy of the recipient jurisdiction's data protection standards) rather than unguided executive notification, to ensure that digital-sovereignty measures remain subject to the legality prong of the *Puttaswamy* proportionality test.

Independent Review of Platform-Directed Government Pressure. Any government mechanism that classifies online content or threatens intermediary safe harbour should be vested in a body institutionally independent of the entity whose conduct is most often the subject of the content in question, with a statutory right of appeal to an independent tribunal,

to prevent the indirect censorship risk illustrated in Kunal Kamra.

VI. Conclusion

The constitutional protection of individual rights in the digital era stands at an inflection point in India. *Puttaswamy* and *Shreya Singhal* together constitute a robust doctrinal foundation, recognising privacy and free expression as mutually reinforcing facets of dignity and democratic self-governance, and articulating a proportionality standard capable, in principle, of adapting to technological change. Yet doctrine alone cannot discharge the constitutional promise. The persistent gap between judicial pronouncement and legislative or executive implementation — visible in the decade-long journey from *Puttaswamy* to the full operationalisation of the Digital Personal Data Protection Rules, 2025, in the continued absence of independent surveillance oversight, and in the recurring resort to subordinate legislation to regulate speech — suggests that the burden of rights protection has fallen disproportionately on courts, in a piecemeal and reactive fashion, rather than on a coherent legislative architecture designed prospectively for the digital environment. As artificial intelligence and algorithmic governance introduce a further layer of complexity that neither existing privacy doctrine nor the 2023 Act fully anticipates, the task for constitutional law in the coming years is not merely to defend the gains of *Puttaswamy* and *Shreya Singhal*, but to extend their underlying logic — legality, necessity, proportionality and accountability — to forms of State and private power that did not exist, or existed only in nascent form, when those judgments were rendered. The layered proportionality framework proposed in this paper, integrating aggregation-risk and collective chilling-effect analysis into the existing four-part test, offers one doctrinal pathway toward that end; its translation into binding legislative and regulatory form remains the central unfinished task of Indian digital constitutionalism as of 2026.

References

A. Constitution and Statutes

- B. *The Constitution of India, 1950, arts 14, 19, 21.*
- C. *The Indian Telegraph Act, 1885.*
- D. *The Information Technology Act, 2000, ss 66A (repealed), 69, 69A, 69B, 79.*
- E. *The Right to Information Act, 2005, s 8(1)(j) (as amended by the Digital Personal Data Protection Act, 2023).*
- F. *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).*

- G. *The Bharatiya Nagarik Suraksha Sanhita, 2023, s 94.*
- H. *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.*
- I. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.*
- J. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.*
- K. *Digital Personal Data Protection Rules, 2025 (notified 13 November 2025).*
- L. *Regulation (EU) 2016/679 (General Data Protection Regulation).*
- M. *Regulation (EU) 2024/1689 (Artificial Intelligence Act).*
- N. *U.S. Constitution, amend. IV.*

O. Cases

- P. *A.K. Gopalan v. State of Madras, AIR 1950 SC 27.*
- Q. *M.P. Sharma v. Satish Chandra, 1954 SCR 1077.*
- R. *Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.*
- S. *Maneka Gandhi v. Union of India, (1978) 1 SCC 248.*
- T. *Govind v. State of Madhya Pradesh, (1975) 2 SCC 148.*
- U. *R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.*
- V. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
- W. *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1.*
- X. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*
- Y. *Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.*
- Z. *Manohar Lal Sharma v. Union of India, (2022) 8 SCC 1.*
- AA. *Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023 (Bombay High Court).*
- BB. *Vysakh K.G. v. Union of India, 2022 SCC OnLine Ker 7337.*
- CC. *Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD), Case C-131/12, [2014] ECR (CJEU).*
- DD. *Carpenter v. United States, 585 U.S. 296 (2018).*

EE. Books and Articles

- FF. *Jack M. Balkin, "Free Speech is a Triangle" 118 Columbia Law Review 2011 (2018).*

- GG. Rumi Dhar and Sonia Nath, *"Digital Surveillance and Civil Rights: Assessing the Impact on Privacy"* 5(1) *Chanakya Law Review* 1 (Jan-June 2024).
- HH. Inder Jain, *"Right to Be Forgotten in India: Constitutional Privacy, Judicial Limits, and the Balance with Free Speech,"* *Legal Service India* (December 2025).
- II. Krishna, *"Interface between Right to Information and Right to Privacy in the Backdrop of the Digital Personal Data Protection Act, 2023"* *ILI Law Review*, Summer Issue 261 (2024).
- JJ. Anupam Kurlwal and Shreyansh, *"Evolution of the Right to Privacy in India: Constitutional Perspective and Judicial Approach"* 5(4) *ShodhKosh: Journal of Visual and Performing Arts* 1985 (2024).
- KK. Daniel J. Solove, *"A Taxonomy of Privacy"* 154 *University of Pennsylvania Law Review* 477 (2006).
- LL. Aditya Thakur, *"The Right to Privacy in the Digital Age: Challenges and Legal Framework in India,"* *International Journal for Legal Research and Analysis* (2025).
- MM. Samuel D. Warren and Louis D. Brandeis, *"The Right to Privacy"* 4(5) *Harvard Law Review* 193 (1890).
- NN. Alan F. Westin, *Privacy and Freedom* (Atheneum, New York, 1967).

OO. Reports, Official Notifications and Other Sources

- PP. Ministry of Electronics and Information Technology, Government of India, Press Information Bureau release, *"DPDP Rules, 2025 Notified"* (17 November 2025).
- QQ. Lexology, *"India's Digital Personal Data Protection Act 2023 Brought into Force"* (17 November 2025).
- RR. Lexology, *"India's Digital Personal Data Protection Regime Takes Effect"* (24 November 2025).
- SS. Lexology, *"Digital Personal Data Protection Rules 2025 – Highlights"* (17 November 2025).
- TT. Supreme Court Observer, *"Section 66A: 4 Must Reads"* (2023).
- UU. Software Freedom Law Centre, India, *"Case Summary: Shreya Singhal v. Union of India."*