THE RIGHT TO PRIVACY IN INDIA: HISTORICAL EVOLUTION AND CONTEMPORARY CHALLENGES IN THE DIGITAL AGE

By *Animesh Patel*
From *Faculty of Law, University of Lucknow*

Abstract:
The Right to Privacy in India has undergone fundamental changes, evolving from the first Judicial Interpretations to an essential element of Constitutional Jurisprudence amid increasing Digital Challenges. Initially, the Hon'ble Supreme Court of India in the landmark cases like *Kharak Singh v. State of Uttar Pradesh, 1962 SCC OnLine SC 10*, dealt with privacy as an implicit aspect of Personal Liberty under Article 21 of the Indian Constitution, rejecting complete recognition due to that period's focus on procedural safeguards rather than Substantive Autonomy.[1] This limited perspective continued until the landmark *K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1*, where a nine-judge bench affirmed and recognized privacy as a Fundamental Human Right as an essential to Dignity, Life, and Liberty, overruling earlier precedents and emphasizing informational privacy in an age of Data Proliferation.[2] This ruling marked a movement toward dynamic interpretation of constitutionalism, adapting rights to contemporary realities like Surveillance and privacy & Data Breaches, while underscoring proportionality in State Intrusions.[3] Core principles of this right include autonomy over Personal Information, Protection from Arbitrary Surveillance, and a balance between Individual Freedoms and Legitimate Public Interests and concerns, such as security.[4] Values like Human Dignity and Self Determination form the pillars of the right to privacy, as Privacy Shields against undue Judgment and fosters trust in Democratic Institutions.[5] Yet, these ideals confront stark Regulatory Silences in the Digital Realm of technology. The Digital Personal Data Protection Act, 2023 (DPDPA), is a remarkable step toward aligning with Global Norms for privacy and digital autonomy, like GDPR, but it exhibits critical gaps and loopholes: (i) Broad Governmental Exemptions, (ii) Insufficient Safeguards for Sensitive Data, and (iii) Neglect of Emerging Harms from Algorithmic Decision Making and AI driven profiling.[6] Specialists argue that it reinforces State-Centric Control, enabling Unchecked Surveillance through mechanisms like CCTV networks that lack Specific Oversight and exacerbate Privacy Erosion without Empirical Crime Reduction Benefits.[7]

[1] Somesh Jain, 'Originalism v Living Constitutionalism: The Debate Goes On' (*SCC Blog*, 13 September 2022) <https://www.scconline.com/blog/post/2022/09/13/originalism-v-living-constitutionalism-the-debate-goes-on> accessed 18 March 2026.

[2] Kamal Kumar, 'The Dawn of Neurotechnology and Its Legal Challenges' (*SCC Blog*, 16 October 2025) <https://www.scconline.com/blog/post/2025/10/17/the-dawn-of-neurotechnology-and-its-legal-challenges> accessed 18 March 2026.

[3] Siddharth R Gupta and Shivansh Vishwakarma, 'Unconstitutionality of Legislations for Being Obsolete, Outdated and Outlived' (*SCC Blog*, 20 February 2023) <https://www.scconline.com/blog/post/2022/06/03/unconstitutionality-of-legislations-for-being-obsolete-outdated-and-outlived> accessed 18 March 2026.

[4] Shubham Janghu and Kashish Jain, 'EU Data Protection Regulation — Impact on Indian Businesses and Jurisprudence' (*SCC Blog*, 20 July 2020) <https://www.scconline.com/blog/post/2018/07/25/eu-data-protection-regulation-impact-on-indian-businesses-and-jurisprudence> accessed 18 March 2026 (hereinafter 'Data Protection Regulation')

[5] Arjun Harkauli, 'Legal Framework for Privacy of Minors' (*SCC Blog*, 14 July 2020) <https://www.scconline.com/blog/post/2020/05/23/legal-framework-for-privacy-of-minors> accessed 18 March 2026.

[6] Rudraksh Lakra and others, 'Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023' (Working Paper No 5366868, SSRN, 2025) <https://ssrn.com/abstract=5366868> accessed 18 March 2026.

[7] Abhishek Singh and Sarah Imran, 'CCTV Cameras

Governmental failures manifest in Legislative momentum and a lack of Enforcement, as seen in the bypassing of Parliamentary Scrutiny for key Bills, hasty legislation on Privacy Threats.[8] Mass Surveillance via Aadhaar and unregulated tech like Neurotechnology highlight how rapid innovation Outpaces and evolves faster than Law, eroding public trust and individual autonomy.[9] This chapter critiques these silences, advocating for flexible Frameworks that Integrate Privacy by Design to Reconcile Technological Progress and growth with Constitutional Imperatives, Ensuring Privacy's Protection in India's Surveillance Society.[10]

Key Words: 'Right to Privacy', 'Digital Surveillance', 'Regulatory Silence', 'Silence of Laws', 'Unregulated Government Oversight'.

1. Introduction

1.1 Overview of Privacy as a Fundamental Right in Contemporary India

In the landscape of Indian constitutional law, the right to privacy has journeyed from a shadowy implication to a robust pillar of individual liberty. For zdecades after independence, privacy lingered on the fringes of judicial interpretation, often subordinated to broader concerns like state security and procedural justice. Early rulings, such as those in the 1950s and 1960s, treated it as an ancillary aspect of personal liberty under Article 21, without granting it standalone status.[11] This hesitation stemmed from the Constitution's silence on explicit privacy protections, leading courts to prioritize safeguards against arbitrary state actions over a comprehensive privacy doctrine. Yet, as societal norms shifted and technology advanced, the judiciary began to carve out space for privacy, recognizing its ties to human dignity and autonomy.

A turning point came with the Supreme Court's evolving stance in key cases. In one early instance, the Court grappled with surveillance practices, affirming that personal liberty encompassed elements of privacy, even if not expressly named in the Constitution.[12] This laid groundwork for later expansions, where privacy was seen as essential to the pursuit of happiness and self-determination. The real breakthrough, however, arrived in 2017, when a nine-judge bench unanimously declared privacy a fundamental right intrinsic to life and liberty under Article 21.[13] This judgment overturned prior limitations, emphasizing that privacy shields

---

and Making of Surveillance Societies' (*Live Law*, 26 June 2024) <https://www.livelaw.in/articles/cctv-cameras-and-surveillance-societies-261531> accessed 18 March 2026.

[8] Saumya Tripathi, 'The Quiet Death of Deliberation in Parliament' (*Live Law*, 19 July 2025) <https://www.livelaw.in/articles/the-quiet-death-of-deliberation-in-parliament-298090> accessed 18 March 2026.

[9] Manik Mahey, 'Evolution of Data Privacy Law in India: Understanding Digital Personal Data Protection Rules, 2025' (*Live Law*, 22 November 2025) <https://www.livelaw.in/articles/data-privacy-law-in-india-and-digital-personal-data-protection-rules-analysis-310865> accessed 18 March 2026.

[10] Aastha Abhya, 'A Practical Guide for Compliance with India's Digital Personal Data Protection Act & Rules' (*Live Law*, 23 April 2025) <https://www.livelaw.in/law-firms/law-firm-articles-/atreus-law-firm-digital-personal-data-protection-act-data-principal-data-fiduciaries-kyc-290050> accessed 18 March 2026.

[11] 'Right to Privacy: Landmark Supreme Court Rulings & Why a 9-Judge Bench Decision is Crucial' (*SCC Blog*, 18 July 2017) <https://www.scconline.com/blog/post/2017/07/18/right-to-privacy-supreme-courts-earlier-rulings-on-the-issue-why-a-9-judge-bench-decision-might-change-everything> accessed 18 March 2026.

[12] Shubhanshi Phogat, 'The Curious Case of Right to Privacy in India' (Working Paper No 3951726, SSRN, 2021) < https://ssrn.com/abstract=3951726> accessed 18 March 2026.

[13] '9-Judge Bench Declares Privacy as a Fundamental Right; Information, Family Life, Sexual Orientation Are All Part of Privacy' (*SCC Blog*, 24 August 2017) <https://www.scconline.com/blog/post/2017/08/24/9-judge-bench-declares-privacy-as-a-fundamental-right-information-family-life-sexual-orientation-are-all-part-of-privacy-judgment> accessed 18 March 2026.

informational autonomy, family life, and even sexual orientation from unwarranted intrusion. It marked a shift toward a living constitutionalism, adapting rights to modern contexts like data proliferation and digital surveillance.

Today, privacy stands as a cornerstone in contemporary India, interwoven with other fundamental rights like equality and free speech. It protects against both state overreach and private encroachments, fostering a society where individuals can navigate their lives without constant fear of exposure. This recognition has influenced legislative efforts, such as the Digital Personal Data Protection Act, 2023, which aims to govern data handling while aligning with global norms.[14] Nonetheless, the right remains dynamic, responding to emerging threats in a nation balancing rapid digitization with democratic values.

1.2 Significance of Privacy in the Digital Era: Autonomy, Dignity, and Vulnerabilities

As India hurtles into the digital age, privacy's significance amplifies, serving as a bulwark for personal autonomy and dignity amid unprecedented vulnerabilities. In an interconnected world, where daily interactions leave digital footprints (from social media shares to online transactions), privacy empowers individuals to control what they reveal and to whom.[15] It nurtures self-esteem, intimate relationships, and the freedom to hold beliefs without judgment, ensuring that one's inner world remains shielded from external scrutiny. Without it, the risk of constant oversight stifles behaviour, eroding the essence of free living.

The digital era, however, exposes profound vulnerabilities. Data, often likened to the "new oil," is collected, stored, and monetized on scales that dwarf traditional threats.[16] Technologies like artificial intelligence, biometrics, and the Internet of Things permeate every facet of life, enabling corporate surveillance and state monitoring that can undermine individual freedoms. For instance, unchecked data breaches and algorithmic profiling not only compromise personal security but also threaten democracy by manipulating public trust and autonomy.[17] In India, with its vast population and booming digital economy, these issues are acute; the proliferation of apps and platforms often extracts data under opaque consent mechanisms, leaving users exposed to misuse.

At its core, privacy upholds human dignity by preventing dehumanizing exploitation. Philosophers and jurists alike stress that autonomy depends on personal boundaries, a view echoed in Indian jurisprudence where privacy is tied to ethical underpinnings of freedom.[18] Yet, the era's challenges (deepfakes, neurotechnology, and mass surveillance) highlight how innovation can outpace protections, turning vulnerabilities into systemic risks. Balancing these with technological progress requires frameworks that prioritize informed consent and

[14] Abdullah Zubair Motiwala, 'A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India' (Working Paper No 5335388, SSRN, 2025) <https://ssrn.com/abstract=5335388> accessed 18 March 2026.

[15] 'Interplay between Right to Information and Right to Privacy' (*SCC Blog*, 20 November 2020) <https://www.scconline.com/blog/post/2020/11/20/interplay-between-right-to-information-and-right-to-privacy> accessed 18 March 2026.

[16] Bhavani Balaji and Vaagish B V, 'Orwellian Dilemma: Evaluating India's Progress on Privacy Rights Post Puttaswamy' (Working Paper No 5013084, SSRN, 2024) <https://ssrn.com/abstract=5013084> accessed 18 March 2026.

[17] Harshali Chowdhary, 'The Mole That AI Revealed: Hallucinations and Biometric Privacy Risks' (*Live Law*, 2 October 2025) <https://www.livelaw.in/articles/use-of-artificial-intelligence-and-privacy-risk-analysis-305718> accessed 18 March 2026.

[18] Ananya Agarwal, 'Right to Privacy in Digital Age: Challenges and Solutions' (Working Paper No 4955726, SSRN, 2024) < https://ssrn.com/abstract=4955726> accessed 18 March 2026.

ethical governance, ensuring privacy remains a lived reality rather than a theoretical ideal.

1.3 The Concept of "Silence of Law": Technology, Surveillance, and Regulatory Gaps

The "silence of law" emerges as a critical concept in India's privacy discourse, denoting regulatory voids where technology and surveillance flourish unchecked, amplifying threats to individual rights. This silence manifests in legislative inertia and enforcement lapses, allowing pervasive monitoring tools like CCTV networks and phone tapping to operate with minimal oversight.[19] While courts have affirmed privacy's fundamental status, the absence of comprehensive statutes has created gaps, enabling state and corporate entities to exploit data without robust safeguards. For example, surveillance practices often bypass proportionality tests, echoing concerns over arbitrary intrusions that echo Orwellian fears.

In the realm of technology, this silence is particularly deafening. Rapid advancements in AI and data-driven ecosystems outstrip legal adaptations, leading to ethical dilemmas around profiling and backdoor access.[20] India's Data Protection Act, while a step forward, reveals shortcomings: broad governmental exemptions and weak compliance mechanisms dilute its impact, permitting unchecked interception that contradicts privacy jurisprudence.[21] Critics point to how such gaps erode public trust, as seen in cases involving Pegasus spyware and centralized data projects, where innovation masks regression toward surveillance states.

Regulatory failures compound these issues, with parliamentary deliberation often bypassed, stifling nuanced responses to digital harms.[22] The result is a fragmented landscape where privacy threats (ransomware to algorithmic biases) proliferate, demanding agile laws that integrate privacy-by-design principles. Bridging this silence requires not just statutes but vigilant enforcement, public awareness, and a commitment to harmonizing progress with constitutional imperatives.

1.4 Scope and Structure of the Chapter

This chapter delves into the evolution of privacy rights in India, examining key principles, core values, and governmental shortcomings in safeguarding them amid technological surges. It critiques the "silence of law" through historical, judicial, and contemporary lenses, drawing on landmark cases and recent legislation to highlight persistent gaps. The analysis underscores the need for proactive reforms to balance individual autonomy with societal advancement.

Following this introduction, Section 2 traces the historical evolution from early interpretations to modern affirmations. Section 3 outlines privacy's principles and values, emphasizing dignity and non-arbitrariness. Section 4 explores governmental failures, focusing on regulatory silences in surveillance and data protection. Section 5 discusses implications for technology and democracy, with comparative insights. The conclusion offers recommendations for an adaptive legal framework.

2. Historical Evolution of Privacy Rights in India

2.1 Early Constitutional and Judicial Interpretations (1950s–1960s)

(Absence of Explicit Recognition Post-Independence)

When India gained independence in 1947 and adopted its Constitution in 1950, the framers laid out a robust

[19] Surveillance Societies (n 7).

[20] Garv Laroia, 'Telephone Tapping, Interception and Surveillance: Thin Line of Privacy' (*Live Law*, 8 September 2025) <https://www.livelaw.in/articles/phone-tapping-and-right-to-privacy-analysis-303171> accessed 18 March 2026.

[21] Rohit Jolly and others, 'The Confluence of AI and Data Privacy: Aligning Data Privacy Regime in India for the Age of AI' (*Bar and Bench*, 9 May 2025) <https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-regime-in-india-for-the-age-of-ai> accessed 18 March 2026.

[22] Deliberation in Parliament (n 8).

framework for fundamental rights, but privacy was not mentioned as a standalone entitlement. This omission reflected the priorities of the time, where the focus was on establishing democratic institutions, protecting against arbitrary state power, and ensuring basic liberties like speech and equality. The Constitution's architects drew from global models, including the Universal Declaration of Human Rights, yet they did not incorporate an explicit privacy clause, perhaps viewing it as subsumed under broader guarantees. As a result, privacy lingered in the shadows, not emerging as a distinct legal concept until judicial scrutiny forced its consideration.[23]

Scholars have noted that this gap stemmed from the era's emphasis on collective nation-building over individual intimacies. In the immediate post-colonial context, the judiciary interpreted rights through a lens of procedural fairness rather than substantive personal autonomy. Privacy, often tied to Western notions of individualism, seemed secondary to India's communal ethos and the urgent need to curb state excesses inherited from colonial rule. Without textual anchoring, courts initially treated privacy claims as peripheral, relying instead on Articles 19 and 21 to address related grievances.[24]

This absence created a vacuum where state actions, such as searches or surveillance, faced limited constitutional checks. Early legal discourse highlighted how the lack of explicit recognition allowed for interpretations that prioritized public order over personal spheres, setting the stage for future conflicts as society modernized and technology advanced.[25]

Initial Focus on Life, Liberty, and Due Process under Article 21. In the 1950s and 1960s, judicial attention centered on Article 21's promise of life and personal liberty, emphasizing due process to prevent arbitrary deprivations. Courts viewed liberty as protection from unlawful detention or state overreach, not as encompassing private domains like home or information. This narrow lens meant privacy issues were often reframed as violations of procedural justice rather than inherent rights.[26]

For instance, early rulings stressed that any restriction on liberty must follow established law, aligning with a formalistic approach. This era's jurisprudence, influenced by British common law, prioritized state interests in security and order, sidelining evolving ideas of personal dignity. As cases involving searches and police powers arose, the judiciary began probing whether such actions infringed on liberty, but without invoking privacy explicitly. This foundational focus on due process under Article 21 would later evolve, providing the bedrock for privacy's emergence as technology and societal changes demanded broader protections.[27]

2.2 Landmark Judicial Milestones

2.2.1 M.P. Sharma v. Satish Chandra (1954): Limited Engagement with Privacy

The Supreme Court's first major encounter with privacy-like concerns came in M.P. Sharma v. Satish Chandra, an eight-judge bench decision addressing search and seizure powers under the Criminal Procedure Code. The case involved allegations of embezzlement, leading to widespread searches of company premises. Petitioners argued that these actions violated fundamental rights, drawing parallels

[23] Gautam Bhatia, 'State Surveillance and the Right to Privacy in India: A Constitutional Biography' (Working Paper No 2605317, SSRN, 2014) <https://ssrn.com/abstract=2605317> accessed 18 March 2026. (hereinafter 'Bhatia')

[24] Privacy in India (n 12).

[25] Bhumesh Verma, 'Evolution of Data Privacy' (*SCC Blog*, 6 February 2020) <https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-privacy> accessed 18 March 2026.

[26] Living Constitutionalism (n 1).

[27] Privacy (n 11).

to the U.S. Fourth Amendment's protection against unreasonable searches.[28]

The Court rejected this, holding that no fundamental right to privacy existed analogous to the American model. It reasoned that the Constitution's framers had deliberately omitted such a provision, and importing it would strain interpretation. Privacy was not seen as inherent to Article 21's liberty or Article 20(3)'s self-incrimination clause. Instead, the judgment focused on procedural validity, upholding the searches as authorized by law.[29]

This ruling set a precedent of reluctance, viewing privacy as non-essential to India's constitutional scheme. Critics later argued it reflected a post-independence caution against expansive rights that might hinder governance. For over six decades, M.P. Sharma influenced a conservative stance, until its overruling in 2017 highlighted its limitations in addressing modern privacy threats.[30]

2.2.2 Kharak Singh v. State of Uttar Pradesh (1963): Implicit Recognition and Domiciliary Surveillance

A decade later, Kharak Singh v. State of Uttar Pradesh challenged Uttar Pradesh Police Regulations allowing surveillance of "history-sheeters," including secret picketing, movement tracking, and domiciliary visits. Kharak Singh, acquitted in a prior case but labeled suspicious, contended these measures violated his freedoms under Articles 19(1)(d) and 21.[31] The six-judge bench, in a majority opinion, struck down domiciliary visits as infringing personal liberty under Article 21, likening them to unauthorized intrusions into one's home. However, it upheld other surveillance forms, asserting no fundamental right to privacy existed. The Court interpreted Article 21 as protecting against physical restraints, not psychological ones from oversight.[32] Justice Subba Rao's dissent marked a turning point, arguing privacy was an essential ingredient of personal liberty. He viewed constant surveillance as stifling freedom, invalidating the entire regulation. This minority view foreshadowed future expansions, emphasizing privacy's role in dignity and autonomy.[33] Kharak Singh thus introduced implicit privacy elements while denying explicit status, creating doctrinal tension. Its partial affirmation of liberty protections against arbitrary intrusion laid groundwork for later cases, though the majority's denial of privacy endured as a hurdle until explicitly overruled.[34]

2.2.3 Gobind v. State of M.P. (1975): Nuanced Expansion and Dignity-Based Approach

Building on Kharak Singh, Gobind v. State of M.P. addressed similar Madhya Pradesh Police Regulations permitting surveillance. Gobind, under watch as a habitual offender, challenged them as violative of Articles 19 and 21.[35] The three-judge bench, led by Justice Mathew, adopted a more expansive view, deriving privacy from personal liberty and dignity under Article 21. It acknowledged privacy as encompassing home intimacies, family, and

[28] Ibid.
[29] 'Right to Digital Privacy: A Critical and Comparative Analysis' (*SCC Blog*, 1 October 2021) <https://www.scconline.com/blog/post/2021/10/01/right-to-digital-privacy> accessed 18 March 2026.
[30] Living Constitutionalism (n 1).
[31] Gautam Bhatia, 'The Supreme Court's Right to Privacy Judgment — I: Foundations' (*Live Law*, 24 August 2017) <https://www.livelaw.in/supreme-courts-right-privacy-judgment-foundations> accessed 18 March 2026.
[32] ibid.
[33] Devansh Malhotra, 'Where Privacy Takes a Detour: Navigating the Controversy of Live Location Sharing' (*Live Law*, 11 November 2023) <https://www.livelaw.in/articles/where-privacy-takes-a-detour-navigating-the-controversy-of-live-location-sharing-244315> accessed 18 March 2026.
[34] Justice Jayasankaran Nambiar, '"Does the Ghost of Gopalan Still Haunt Our Jurisprudence?": A Search for the Contemporary Relevance of AK Gopalan v State of Madras' (*Live Law*, 22 June 2020) <https://www.livelaw.in/columns/does-the-ghost-of-gopalan-still-haunt-our-jurisprudence-159026> accessed 18 March 2026.
[35] Bhatia (n 23).

procreation, essential for happiness and self-development. However, privacy was not absolute; it could be restricted for compelling public interests like security, subject to reasonable procedures.[36]

The Court upheld the regulations narrowly, finding them justified for crime prevention, but warned of potential unconstitutionality if arbitrarily applied. Gobind's dignity-based approach shifted from Kharak Singh's formalism, recognizing privacy's relational and decisional aspects. It cited U.S. precedents like Griswold, integrating global ideas while adapting to Indian contexts.[37] This nuanced expansion marked a watershed, affirming privacy's constitutional roots without full declaration, paving the way for its fundamental status amid growing surveillance concerns.[38]

2.2.4 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017): Affirmation as a Fundamental Right

The culmination came in Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench unanimously declared privacy a fundamental right under Article 21. Triggered by Aadhaar challenges, the case revisited M.P. Sharma and Kharak Singh, overruling their denial of privacy.[39]

The polyvocal judgment emphasized privacy's ties to dignity, autonomy, and liberty, encompassing informational, decisional, and spatial facets. Justice Chandrachud's plurality opinion traced privacy's evolution, rejecting absolute status but requiring proportionality for restrictions. It addressed digital age vulnerabilities, like data proliferation, affirming privacy's role in democratic freedoms.[40] Puttaswamy integrated zonal, relational, and decisional paradigms, drawing from Gobind while expanding to modern contexts. It vindicated Subba Rao's Kharak Singh dissent, establishing privacy as intrinsic to Part III rights, subject to legitimate state aims.[41]

This affirmation transformed jurisprudence, influencing data protection and surveillance laws, though implementation challenges persist.[42]

2.3 Legislative Developments: From Absence to the Digital Personal Data Protection Act, 2023

Post-Puttaswamy, legislative inertia gave way to the Digital Personal Data Protection Act, 2023 (DPDPA), evolving from earlier bills like the 2019 Personal Data Protection Bill. Initially absent dedicated laws, privacy relied on judicial safeguards and sector-specific rules.[43] The 2019 Bill aimed at comprehensive

[36] Anubhav Khamroi and Anujay Shrivastava, 'The Curious Case of Right to Privacy in India' (Working Paper No 4318889, SSRN, 2017) < https://ssrn.com/abstract=4318889> accessed 18 March 2026.

[37] Shivnath Tripathi, 'Right to Privacy as a Fundamental Right: Extent and Limitations' (Working Paper No 2273074, SSRN, 2017) < https://ssrn.com/abstract=2273074> accessed 18 March 2026.

[38] Dr G V Mahesh Nath, 'A Conceptual Journey of Privacy Rights in India' (Working Paper No 3464353, SSRN, 2019) < https://ssrn.com/abstract=3464353> accessed 18 March 2026.

[39] Murali Krishnan, 'Puttaswamy: Right to Privacy is a Fundamental Right under Article 21, Supreme Court' (*Bar and Bench*, 24 August 2017) <https://www.barandbench.com/news/right-privacy-fundamental-right-supreme-court> accessed 18 March 2026.

[40] Rishika Taneja & Sidhant Kumar, *Setting the Record Straight: Clarifying the Right to Privacy*, BAR & BENCH (Sept. 15, 2017), https://www.barandbench.com/columns/setting-record-straight-clarifying-right-privacy.

[41] Ranjana Adhikari and others, 'A Case to Keep Aadhaar as a Voluntary KYC Document' (*Bar and Bench*, 27 March 2019) <https://www.barandbench.com/view-point/a-case-to-keep-aadhaar-as-a-voluntary-kyc-document> accessed 18 March 2026.

[42] Aditya AK, 'Proportionality Test for Aadhaar: The Supreme Court's Two Approaches' (*Bar and Bench*, 1 October 2018) <https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches> accessed 18 March 2026.

[43] Gauri Goyal, 'Privacy and Data Protection in India: A Critical Analysis of the Legal Framework' (Working Paper No 5821002, SSRN, 2025)

regulation but faced criticism for state exemptions. The 2023 Act, assented on August 11, 2023, mandates consent-based data processing, rights for data principals, and fiduciary duties, aligning with global norms like GDPR.[44] However, gaps remain: broad government exemptions, weak consent mechanisms, and neglect of neural data. DPDPA represents progress in addressing digital vulnerabilities but highlights ongoing tensions between privacy and state interests.[45] This evolution from judicial crafting to statutory frameworks underscores privacy's maturation, yet calls for agile amendments to match technological pace.[46]

3. Silence of Law: Governmental and Regulatory Failures in Ensuring Privacy

The phrase "silence of law" captures the persistent gaps where legal frameworks have lagged behind technological realities, leaving privacy vulnerable to both state and private actors. Despite the Supreme Court's emphatic recognition of privacy as a fundamental right in 2017, governmental and regulatory responses have often fallen short, creating structural voids that persist even after the passage of the Digital Personal Data Protection Act, 2023. These failures are not merely administrative oversights; they reflect a deeper reluctance to translate judicial pronouncements into robust, enforceable protections.[47]

3.1 Historical and Structural Regulatory Gaps

Prolonged Judicial Reluctance to Recognize Privacy Independently

For nearly seven decades after the Constitution came into force, the judiciary hesitated to treat privacy as an independent constitutional entitlement. Early decisions viewed it only as an incidental aspect of personal liberty under Article 21, never as a standalone guarantee. This reluctance stemmed from a formalistic reading that refused to import foreign doctrines without express textual support, leaving citizens without clear constitutional armour against intrusive practices.[48] Even when surveillance challenges reached the Supreme Court, the majority opinions stopped short of declaring privacy fundamental, preferring to uphold state regulatory powers over individual spheres. The dissenting voices that argued for a broader reading remained just that until a nine-judge bench finally overruled the earlier narrow positions in 2017. This prolonged judicial caution created a doctrinal vacuum in which state agencies and private entities operated with minimal constitutional restraint for generations.[49]

Absence of Dedicated Data Protection Legislation Until 2023

Compounding the judicial hesitation was the complete absence of a comprehensive data protection statute until August 2023. For years, privacy protection relied on scattered provisions in the Information Technology Act, 2000 and its 2011 Rules (provisions that were never designed to handle the scale of digital data flows). Without a dedicated law, there was no statutory mechanism for consent, data minimization, or breach notification, leaving individuals exposed in an increasingly data-driven economy. Successive governments drafted bills that were repeatedly delayed or diluted, reflecting a systemic inertia that allowed corporate and governmental data practices to flourish

<https://ssrn.com/abstract=5821002> accessed 18 March 2026. (hereinafter 'Goyal')

[44] Soumya Banerjee, '"Digital Personal Data Protection Act" — A Strudel Served Raw!' (Working Paper No 4956275, SSRN, 2024) < https://ssrn.com/abstract=4956275> accessed 18 March 2026.

[45] Gaurav Thote, 'Unravelling "Consent" under the Digital Personal Data Protection Act, 2023 — A Barrier to Data Principal Rights' (*SCC Blog*, 13 November 2024) <https://www.scconline.com/blog/post/2024/11/13/unravelling-consent-under-the-digital-personal-data-protection-act-2023-a-barrier-to-data-principal-rights> accessed 18 March 2026.

[46] Unconstitutionality of Legislations (n 3).

[47] DPDP Rules 2025 (n 14).

[48] Goyal (n 43).

[49] Rohin Dubey, 'The Great Data Protection Debate: India's New Data Protection Bill' (*Bar and Bench*, 29 December 2020) <https://www.barandbench.com/columns/the-great-data-protection-debate-indias-new-data-protection-bill> accessed 18 March 2026.

unchecked. The eventual enactment of the Digital Personal Data Protection Act came only after years of public pressure and judicial nudging, yet even this legislation arrived late and with significant carve-outs that critics describe as preserving state control rather than empowering citizens.[50]

3.2 Major Failures in Enforcement and Oversight

Inadequate Responses to Data Breaches and Insecure Digital Ecosystems

India has witnessed repeated high-profile data breaches, yet regulatory responses have remained reactive and under-powered. Major incidents involving healthcare insurers and fintech platforms exposed millions of records, including sensitive health and financial information, yet enforcement actions were limited to notices or modest penalties that failed to deter systemic negligence. The absence of mandatory real-time breach reporting standards and independent audits meant organisations could delay disclosure or downplay risks, eroding public confidence. Even after the DPDP Act, draft rules have been criticised for lacking differentiated severity levels for breaches and for placing the burden of proof on victims rather than fiduciaries.[51] These enforcement gaps have turned data security into a paper exercise rather than a lived safeguard.

Permissive or Unchecked State Surveillance Practices

State surveillance continues with minimal oversight. Widespread deployment of CCTV networks, Aadhaar-linked databases, and interception powers under the Telegraph Act operate without comprehensive proportionality checks or independent review boards. Courts have repeatedly noted that such practices risk becoming tools of mass monitoring rather than targeted crime prevention, yet legislative amendments have been slow and narrow. The Pegasus controversy and reports of unauthorised data access highlighted how surveillance tools can bypass existing safeguards, yet accountability mechanisms remain fragmented across ministries and agencies.[52] This permissiveness creates an environment where privacy is treated as secondary to security imperatives, often without empirical justification.

Weak Compliance Mechanisms for Emerging Technologies (Biometrics, AI, IoT, Facial Recognition)

Emerging technologies have outpaced regulatory imagination. Biometric systems, facial recognition software, and AI-driven profiling are deployed across welfare schemes, policing, and private platforms without tailored risk assessments or ethical guidelines. The DPDP Act contains no specific provisions for automated decision-making or neurotechnology risks, while IoT devices collect intimate behavioural data without consent frameworks. Enforcement bodies lack technical capacity to audit algorithmic bias or data flows in real time, leaving citizens exposed to opaque "black box" systems that affect livelihoods and reputations.[53] Regulatory silence here is particularly dangerous because these technologies are irreversible once embedded in public infrastructure.

3.3 Contemporary Manifestations of Regulatory Silence

Challenges in Data Localization, Corporate Surveillance, and Governmental Oversight

The DPDP Act's data localization requirements and broad governmental exemptions have invited criticism for creating compliance nightmares for global businesses while simultaneously granting the state sweeping access. Critics argue that localization, intended to enhance security, concentrates data in

[50] Ishwar Ahuja and Sakina Kapadia, 'Digital Personal Data Protection Act, 2023 — A Brief Analysis' (*Bar and Bench*, 22 August 2023) <https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis> accessed 18 March 2026.

[51] 'Legal Ramifications of a Data Breach Discussed in Light of Star Health and Allied Insurance Breach' (*SCC Blog*, 28 January 2025) <https://www.scconline.com/blog/post/2025/01/28/legal-ramifications-data-breach-discussed-in-light-of-star-health-and-allied-insurance-breach/> accessed 18 March 2026.

[52] Data Privacy (n 9).

[53] Jolly and others (n 21).

vulnerable central repositories without corresponding cybersecurity upgrades. Corporate surveillance through consent-based models has also thrived because the law permits "legitimate uses" that are vaguely defined, allowing platforms to monetise personal data with minimal pushback.[54] Governmental oversight remains centralised in the Data Protection Board, whose independence and capacity are still untested, raising fears of regulatory capture.

Erosion of Public Trust and Individual Autonomy Due to Enforcement Deficiencies

Repeated breaches and visible surveillance have chipped away at public trust. Citizens increasingly feel that their data is neither secure nor truly theirs, leading to self-censorship on digital platforms and reluctance to engage with government services. This erosion directly undermines the autonomy the Supreme Court sought to protect in 2017. When enforcement is weak and remedies are bureaucratic, individuals lose faith in the system's ability to vindicate their rights, turning privacy from a lived freedom into an aspirational ideal.[55]

Failure to Integrate Privacy-by-Design and Ethical Governance in Technological Development

Perhaps the most telling silence is the failure to embed privacy-by-design in technological development. Developers and deployers of AI, IoT, and biometric systems are not statutorily required to conduct privacy impact assessments or adopt ethical governance frameworks at the design stage. This omission means privacy is treated as an afterthought rather than a core engineering principle, perpetuating insecure ecosystems and ethical blind spots. Until regulators mandate privacy-by-design across public and private sectors, technological advancement will continue to outrun constitutional protections.[56]

The cumulative effect of these failures is a regulatory landscape that speaks loudly on paper but remains largely silent in practice. Bridging this gap demands more than new rules; it requires sustained political will, technical capacity, and judicial vigilance to ensure that privacy is not merely declared fundamental but genuinely secured in daily life.

4. Implications of Regulatory Silence in the Context of Technology and Surveillance (Mass Surveillance, Corporate Data Exploitation, and Ethical Concerns)

The regulatory silence surrounding privacy has allowed mass surveillance to become embedded in everyday Indian life. CCTV networks, Aadhaar linked databases and interception tools now operate across cities and welfare schemes without consistent independent oversight. These systems collect vast amounts of biometric and behavioural data under the guise of security or service delivery, yet the absence of real time audit mechanisms leaves room for function creep. Corporate platforms compound the problem by harvesting user information through opaque consent flows and targeted advertising models. Social media giants and fintech apps routinely profile individuals based on browsing habits, location and even emotional cues, turning personal data into a commercial asset without meaningful accountability.[57]

Ethical concerns multiply when artificial intelligence enters the picture. Algorithmic decision making in lending, hiring or policing often relies on biased datasets, yet Indian law lacks mandatory impact assessments for such tools. Facial recognition deployed by police forces and private entities raises questions of accuracy and discrimination, particularly against marginalised communities, while IoT devices in homes silently transmit intimate routines to distant servers. The silence of law here is not passive; it actively permits these practices to scale without ethical

[54] Abhya (n 10).
[55] 'Digital Distress, Legal Blindness: Gaps in Consent Mechanisms under India's Data Protection Regime' (Working Paper No 5468066, SSRN, 2025) <https://ssrn.com/abstract=5468066> accessed 18 March 2026.
[56] Jolly and others (n 21).
[57] Surveillance Societies (n 7).

guardrails, creating a digital environment where privacy is traded for convenience or control.[58]

Impact on Democracy, Freedoms, and Societal Trust
These threats extend far beyond individual inconvenience. When citizens know their every move can be tracked, self censorship becomes routine. Journalists, activists and ordinary users hesitate to express dissenting views online, directly chilling the freedom of speech guaranteed under Article 19. During elections, unchecked data exploitation has already enabled micro targeting that distorts public discourse, raising fears about the integrity of democratic choice. Societal trust erodes when data breaches repeatedly expose millions of records and state agencies respond with little more than advisory notices. People begin to view both government services and private platforms with suspicion, withdrawing from digital ecosystems that were meant to empower them. The cumulative effect is a quiet contraction of personal freedoms and a weakening of the democratic fabric that the Supreme Court sought to protect in 2017.[59]

4.2 Comparative Insights and Global Norms
Lessons from International Frameworks (e.g., GDPR) and Their Relevance to India
Europe's General Data Protection Regulation offers a stark contrast. Under GDPR, data controllers face fines up to four percent of global turnover for violations, individuals enjoy a robust right to be forgotten and automated decision making requires explicit safeguards. Consent must be granular, withdrawal must be easy and data protection officers are mandatory for large processors. These features have forced companies to redesign products with privacy at the core rather than as an afterthought.[60]

India's Digital Personal Data Protection Act, by comparison, contains significant carve outs for government agencies and softer penalty structures. While the Indian law borrows concepts like data fiduciary duties and breach notification, it stops short of GDPR's stringent cross border transfer rules and independent supervisory authority with real enforcement teeth. The contrast highlights what regulatory silence has cost India: the opportunity to build a mature data protection regime that commands global respect. Yet the relevance of GDPR is not about blind copying. India's federal structure, digital public infrastructure and developmental priorities demand an adapted model that balances innovation with rights. Learning from GDPR's emphasis on accountability and user empowerment could help close the gaps that currently expose Indian citizens to disproportionate risks.[61]

4.3 The Need for Proactive Legal Adaptation
The persistence of regulatory silence demands a fundamental shift from reactive legislation to proactive legal design. Future reforms must embed privacy impact assessments at the earliest stage of any technological project, whether public welfare schemes or private apps. Regular parliamentary review of the DPDP Rules, coupled with an independent Data Protection Board possessing technical expertise and financial autonomy, would prevent the law from becoming outdated within months of notification. Multi stakeholder consultations involving civil society, technologists and industry can ensure rules reflect ground realities rather than bureaucratic convenience.[62]

Courts too have a continuing role. They must insist on strict proportionality tests whenever surveillance or data processing is challenged, refusing to accept blanket national security exemptions without evidence. At the same time, the legislature needs to address emerging frontiers such as neurotechnology and generative AI before they entrench new forms of intrusion. Privacy by design must move from aspirational language to enforceable obligation, backed by incentives for compliance and swift penalties for default. Only such proactive adaptation

[58] Chowdhary (n 17).
[59] Orwellian Dilemma (n 16).
[60] Data Protection Regulation (n 4).
[61] DPDP Rules 2025 (n 14).
[62] Digital Distress Legal Blindness (n 55).

can transform the current silence of law into a living constitutional safeguard that keeps pace with technological change while preserving the dignity and autonomy the Supreme Court recognised as fundamental.[63]

In essence, the implications of regulatory silence are not abstract. They manifest as chilled speech, eroded trust and unequal digital citizenship. Comparative lessons from GDPR show that stronger frameworks are possible, but India must tailor them to its context. The path forward lies in deliberate, forward looking legal engineering that treats privacy not as a constraint on progress but as its essential foundation.

5. Conclusion and Way Forward

5.1 Summary of Key Findings

The journey of privacy rights in India reveals a clear arc from constitutional ambiguity to judicial affirmation, yet one marked by persistent regulatory shortfalls. Early post-independence interpretations under Article 21 treated privacy as a mere byproduct of personal liberty rather than a distinct guarantee, allowing surveillance and data practices to operate with little restraint. Landmark rulings gradually shifted this position, culminating in the 2017 Puttaswamy judgment that elevated privacy to fundamental status, encompassing informational, decisional and spatial dimensions tied to dignity and autonomy. Despite this breakthrough, legislative response remained delayed until the Digital Personal Data Protection Act of 2023, and even then the statute carried broad exemptions and enforcement gaps that left citizens exposed.[64]

Core principles such as protection from arbitrary intrusion, autonomy over personal data and procedural safeguards against surveillance were clearly articulated by the courts. These rest on values of human dignity, individual self-determination and a workable balance with public interests like security. In practice, however, governmental and regulatory silence has undermined these ideals. Prolonged judicial reluctance, absence of dedicated legislation for decades and weak oversight mechanisms have permitted mass surveillance, corporate data exploitation and unchecked deployment of biometrics, artificial intelligence and facial recognition tools.[65] The result is heightened threats to democracy, chilled freedoms and declining public trust, as citizens increasingly self-censor and withdraw from digital services. Comparative analysis with the European GDPR underscores what India has missed: stronger penalties, independent supervision and genuine user empowerment. The cumulative findings paint a picture of a right that is constitutionally robust on paper but fragile in daily application.[66]

5.2 Recommendations for Bridging the Silence of Law

Strengthening Enforcement, Public Awareness, and Cybersecurity

Effective bridging of regulatory gaps begins with robust enforcement machinery. The Data Protection Board must be granted genuine independence, adequate funding and technical expertise to conduct proactive audits rather than reactive inquiries. Penalties under the Digital Personal Data Protection Act should be calibrated by severity and repeated violations, with clear timelines for breach notifications and mandatory victim compensation. Public awareness campaigns, integrated into school curricula and digital literacy programmes, can equip citizens to exercise rights such as consent withdrawal and data erasure. At the same time, mandatory cybersecurity standards for government databases and large private platforms, including regular third-party audits, would reduce the frequency of breaches that currently erode confidence.[67]

Adopting Privacy-by-Design and Agile Legislative Approaches

[63] Jolly and others (n 21).
[64] DPDP Rules 2025 (n 14).
[65] Orwellian Dilemma (n 16).
[66] Data Protection Regulation (n 4).
[67] Data Privacy (n 9).

Privacy cannot remain an afterthought. Every new technological deployment, whether public welfare platforms or private apps, should be required to undergo privacy impact assessments at the design stage. Developers must demonstrate how data minimisation, encryption and user controls are baked into architecture rather than added later. The legislature needs an agile mechanism to review and amend rules every two years through parliamentary standing committees that include technologists and civil society voices. Sunset clauses on broad governmental exemptions would prevent permanent carve-outs that dilute the Act's protective intent. Such approaches would align Indian law more closely with global best practices while respecting local developmental needs.[68]

5.3 Future Prospects: Balancing Privacy Rights with Technological Advancement

Looking ahead, the tension between privacy and technological progress need not be zero-sum. India's digital public infrastructure, including Aadhaar and UPI, offers immense potential for inclusion, yet only if privacy safeguards scale alongside innovation. Future prospects hinge on courts continuing to apply strict proportionality tests in surveillance and data cases, refusing blanket national-security justifications without evidence. Legislative foresight must extend to emerging frontiers such as neurotechnology and generative artificial intelligence before they become entrenched. A multi-stakeholder model involving regulators, industry, academia and rights groups can co-create guidelines that promote responsible innovation without sacrificing constitutional values.[69]

If these steps are taken, privacy can evolve from a declared right into a lived reality that supports rather than hinders India's digital ambitions. Citizens would engage more freely with technology, confident that their autonomy and dignity remain protected. The silence of law that has characterised the past can give way to a responsive, forward-looking framework that honours the Supreme Court's vision while meeting the demands of a rapidly digitising society. Ultimately, the measure of success will lie not in the number of statutes enacted but in the everyday experience of ordinary Indians who can navigate the digital age with security, dignity and trust.[70]

*****

[68] Ahuja and Kapadia (n 50).
[69] Jolly and others (n 21).
[70] Digital Distress, Legal Blindness (n 55).