JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 1 (Jan.-Mar.) | 2026 Art. 15

Understanding the Right to Privacy in India: Article 21's Evolution in the Digital Age

Shreya Pandey
Law Student,
B.A.LL.B. (Hons), 5th Year
Amity Law School, Amity University, Lucknow

Dr. Sarita Yadav
Assistant Professor,
Amity Law School, Amity University, Lucknow

Recommended Citation
Shreya Pandey and Dr. Sarita Yadav, *Understanding the Right to Privacy in India: Article 21's Evolution in the Digital Age*, 2 JILPS 250-262 (2026).
Available at www.jilps.in/archives/.

Understanding the Right to Privacy in India: Article 21's Evolution in the Digital Age

Shreya Pandey
Law Student,
B.A.LL.B. (Hons), 5th Year
Amity Law School, Amity University, Lucknow

Dr. Sarita Yadav
Assistant Professor,
Amity Law School, Amity University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
02 Mar. 2026	04 Mar. 2026	05 Mar. 2026

ABSTRACT

The constitutional recognition of the right to privacy represents one of the most transformative developments in Indian fundamental rights jurisprudence under Article 21. Once absent from constitutional text and early judicial interpretation, privacy has evolved through a series of judicial decisions into a core component of life and personal liberty grounded in dignity and individual autonomy. This paper examines the doctrinal evolution of the right to privacy culminating in the landmark judgment of Justice K.S. Puttaswamy v. Union of India, which definitively established privacy as a fundamental right and articulated the proportionality framework governing state intrusion. The paper situates privacy jurisprudence within the realities of India's digital transformation by analyzing contemporary threats arising from biometric identification systems, algorithmic surveillance, state monitoring practices, and large-scale corporate data collection. It critically evaluates the statutory framework introduced by the Digital Personal Data Protection Act, 2023, highlighting structural and institutional limitations that weaken effective enforcement, including broad executive exemptions, limited regulatory autonomy, and the conceptual limitations of consent-based data governance. The paper argues that although constitutional doctrine has established a robust normative foundation for privacy protection, statutory implementation remains incomplete. Effective realization of privacy as a fundamental right requires stronger institutional safeguards, meaningful oversight of surveillance powers, differentiated protection for sensitive data, and improved digital literacy. The study concludes that the future of privacy under Article 21 depends upon bridging the gap between constitutional principle and regulatory practice in India's rapidly expanding digital ecosystem.

KEYWORDS

Right to Privacy, Article 21, Digital Privacy, Constitutional Jurisprudence, Data Protection, Surveillance

I. INTRODUCTION

Personal data has become one of the defining commodities of the twenty-first century. The Cambridge Analytica scandal of 2018 illustrated with stark clarity how the unauthorized harvesting of personal information from millions of users can destabilize democratic institutions. In India, where over a billion citizens have enrolled in the world's largest biometric identification program, the stakes of privacy protection are particularly acute. This paper examines the constitutional foundations of the right to privacy in India, its judicial evolution under Article 21 of the Constitution, and the adequacy of the Digital Personal Data Protection Act, 2023 ("DPDPA") in responding to contemporary digital threats.

The right to privacy in India travelled a remarkable path over seven decades, from a right unacknowledged by the Supreme Court's earliest judgments to one unanimously recognized as intrinsic to human dignity and personal liberty. The landmark nine-judge bench decision in *Justice K.S. Puttaswamy v. Union of India* (2017)[1] constitutes the watershed moment of this evolution, overruling decades of contrary precedent and establishing a three-part proportionality test that continues to govern the permissible scope of governmental intrusion. Yet constitutional recognition is only the beginning. Effective protection requires independent regulatory institutions, transparent oversight of state surveillance, and a citizenry with the digital literacy to exercise its legal rights in practice. This paper argues that while India has made significant progress, the DPDPA's structural deficiencies and broad executive exemptions risk undermining the privacy protections the *Puttaswamy* Court so carefully constructed.

II. CONSTITUTIONAL FOUNDATION: ARTICLE 21 AND THE RIGHT TO PERSONAL LIBERTY

A. The Text and Original Understanding of Article 21

Article 21 of the Indian Constitution provides: "No person shall be deprived of his life or personal liberty except according to procedure established by law."[2] This deceptively simple guarantee encompasses two distinct rights — the right to life and the right to personal liberty — whose scope the Supreme Court has dramatically expanded through decades of interpretive evolution. The framers drew inspiration from international instruments, including Article 12 of the Universal Declaration of Human Rights (1948), which prohibits arbitrary interference with an individual's privacy, family, and

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

[2] INDIA CONST. art. 21.

correspondence.[3]

During the Constituent Assembly debates of December 1948, members disputed whether to adopt the phrase "procedure established by law" — drawn from the Japanese Constitution — or the American "due process of law." Proponents of "due process" argued that the judiciary should be empowered to strike down legislation that, while formally enacted, violated other fundamental rights. Opponents contended that unelected judges ought not to sit in judgment of the legislature's policy choices. The Assembly ultimately retained "procedure established by law," a choice whose implications were to occupy the Court for decades.

B. From Literal to Liberal Interpretation: Gopalan to Maneka Gandhi

The Supreme Court's initial interpretation of Article 21 was conspicuously narrow. In *A.K. Gopalan v. State of Madras* (1950),[4] a five-judge majority held that "procedure established by law" referred to state-enacted procedure that need not conform to principles of natural justice. The Court treated Articles 19, 21, and 22 as independent silos, declining to read them harmoniously. Under this regime, the executive could deprive an individual of personal liberty through any procedure, however arbitrary, so long as it had statutory backing.

The interpretive landscape shifted profoundly with *Maneka Gandhi v. Union of India* (1978).[5] Overruling *Gopalan*, the Court held that the procedure contemplated by Article 21 must be fair, just, and reasonable — not arbitrary, fanciful, or oppressive.[6] The judgment introduced a triple test: any law limiting personal liberty must satisfy legality (the existence of a valid law), legitimate state aim, and proportionality between the object and the means employed. Crucially, the Court read Articles 14, 19, and 21 as a "golden triangle" of interlocking guarantees, such that a procedure satisfying one might still fail another.

The expansive reading of Article 21 was further cemented by *Francis Coralie Mullin v. Union Territory of Delhi* (1981),[7] where Justice Bhagwati, writing for the Court, held that the right to life encompasses more than mere animal existence — it includes the right to live with basic human dignity, including access to adequate nutrition, clothing, shelter, and the means of reading and writing. This reasoning would later serve as the intellectual foundation for the right to privacy: if life encompasses dignity, and dignity encompasses the freedom to control one's intimate sphere, then privacy too must be sheltered within Article 21.

---

[3] INDIA CONST. art. 21; see also Universal Declaration of Human Rights art. 12, Dec. 10, 1948, G.A. Res. 217A (III).

[4] A.K. Gopalan v. State of Madras, AIR 1950 SC 27.

[5] Maneka Gandhi v. Union of India, AIR 1978 SC 597.

[6] Id.

[7] Francis Coralie Mullin v. Union Territory of Delhi, AIR 1981 SC 746.

C. The Pre-2017 Privacy Jurisprudence: Uncertainty and Incremental Recognition

The Constitution's text makes no mention of privacy, and the framers did not expressly contemplate it as a fundamental right. The Court's early encounters with privacy claims were largely dismissive. In *M.P. Sharma v. Satish Chandra* (1954),[8] an eight-judge bench, while considering search and seizure operations, made only a passing reference to privacy and rejected arguments that such operations violated fundamental rights. Eight years later, in *Kharak Singh v. State of Uttar Pradesh* (1962),[9] a six-judge majority similarly refused to recognize privacy as a fundamental right, though it struck down regulations permitting nocturnal domiciliary visits as an infringement of the right to life under Article 21. Justice Subba Rao's prescient dissent observed that the concept of liberty in Article 21 was comprehensive enough to include the right to privacy — "nothing," he wrote, "is more deleterious to a man's physical happiness and health than a calculated interference with his privacy."[10]

The Court took a more nuanced approach in *Govind v. State of Madhya Pradesh* (1975).[11] While dismissing a challenge to police surveillance regulations, the Court acknowledged that privacy-dignity claims deserved careful scrutiny and could be overridden only when a compelling countervailing state interest was demonstrated.[12] This borrowed the "compelling state interest" standard from American constitutional law, laying the groundwork for a proportionality framework that the Court would fully articulate in *Puttaswamy* over four decades later.

A significant advance came with *R. Rajagopal v. State of Tamil Nadu* (1994),[13] arising from a dispute over publication of a condemned prisoner's autobiography. The Court held, for the first time, that the right to privacy is a fundamental right inferred from Article 21 — that every individual possesses a right to be left alone and to protect personal matters from unauthorized publication.[14] Borrowing from the American defamation doctrine of *New York Times Co. v. Sullivan*,[15] the Court held that state actors who publish false information about private individuals with reckless disregard for the truth could be held liable. *Rajagopal* thus set the doctrinal stage for the definitive recognition that would arrive in 2017.

III. THE PUTTASWAMY JUDGMENT AND THE ESTABLISHMENT OF A CONSTITUTIONAL RIGHT TO PRIVACY

A. Background and Reference to the Nine-Judge Bench

[8] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[9] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

[10] Id. (Subba Rao, J., dissenting).

[11] Govind v. State of Madhya Pradesh, AIR 1975 SC 1378.

[12] Id.

[13] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

[14] Id.

[15] New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

In 2012, Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition challenging the constitutional validity of the Aadhaar scheme, contending that mandatory biometric enrollment violated the right to privacy. A three-judge bench recognized the gravity of the question and, on August 11, 2015, ordered that a bench of appropriate strength must determine whether privacy is a fundamental right under the Constitution. On July 18, 2017, the matter was referred to a nine-judge constitution bench — one of the largest the Court had ever assembled.

B. The Unanimous Verdict and Its Doctrinal Architecture

On August 24, 2017, the nine-judge bench delivered a unanimous verdict recognizing privacy as a fundamental right guaranteed by the Constitution — principally under Article 21, and supplemented by the values enshrined in Part III as a whole.[16] The Court overruled *M.P. Sharma* and *Kharak Singh* to the extent they declined to recognize a fundamental right to privacy.[17]

The Court characterized privacy as an attribute of human dignity, protecting an individual's freedom to make choices about personal matters and to control the significant aspects of one's own life. Personal intimacies, including sexual orientation, relationships, and bodily autonomy, were held to lie at the core of this protected sphere. The judgment articulated a three-part test — identical in structure to that employed in *Maneka Gandhi* — holding that any state action limiting privacy must satisfy: (1) legality (the existence of a law sanctioning the restriction); (2) a legitimate state aim; and (3) proportionality between the aim pursued and the means employed.[18]

Although the nine judges produced six separate opinions, each employing distinct philosophical frameworks ranging from natural rights theory to transformative constitutionalism, they converged on the fundamental proposition: privacy is not a gift from the state but an inherent attribute of human personhood that the Constitution protects against both state and, in some circumstances, private violation.

C. Sexual Privacy: Navtej Singh Johar v. Union of India (2018)

The transformative implications of *Puttaswamy* were swiftly realized in *Navtej Singh Johar v. Union of India* (2018),[19] where a five-judge bench unanimously declared Section 377 of the Indian Penal Code unconstitutional insofar as it criminalized consensual same-sex conduct between adults. Relying centrally on *Puttaswamy*, the Court held that sexual orientation is an essential attribute of privacy and that the choice of one's intimate partner lies at the core

[16] Puttaswamy, supra note 15.

[17] Id.

[18] Id. The three-part test requires that any restriction on privacy satisfy (1) legality — the existence of a law; (2) legitimate state aim; and (3) proportionality between the object and the means adopted.

[19] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.

of constitutionally protected personal liberty.[20]

Justice Malhotra's concurrence offered a candid acknowledgment of historical wrongs: the law owed an apology to members of the LGBT+ community for the centuries of legal ignominy they had endured.[21] The judgment, read alongside *Puttaswamy*, stands for the principle that the state's legitimate interest in regulating conduct ceases at the bedroom door — that intimacy between consenting adults falls outside the proper domain of criminal law. The progression from Justice Subba Rao's lonely dissent in *Kharak Singh* to the unanimous verdict in *Navtej* represents the most significant evolution in Indian civil liberties jurisprudence since Independence.[22]

IV. DIGITAL PRIVACY CHALLENGES IN CONTEMPORARY INDIA

A. The Aadhaar Program and Biometric Data Vulnerabilities

India's Aadhaar scheme constitutes one of the world's most ambitious experiments in digital identity governance. Each enrolled resident receives a unique twelve-digit number linked to biometric identifiers — fingerprints and iris scans — as well as demographic information. As of 2023, over 1.38 billion enrollments cover approximately ninety percent of India's population.[23] The scheme's scale creates correspondingly large risks: unlike passwords, biometric data is permanent and cannot be reset if compromised. A security researcher from the Centre for Internet and Society documented that approximately 130 million Aadhaar numbers, together with associated sensitive data, were publicly accessible on the internet at various points,[24] and approximately 200 government websites inadvertently exposed personal Aadhaar data in 2018.[25] These incidents underscore a structural vulnerability: the aggregation of irreplaceable biometric identifiers in a centralized database creates a singularly attractive target for malicious actors and an enduring threat to the privacy of every enrolled individual.

B. State Surveillance: The Pegasus Spyware Controversy

The deployment of Pegasus spyware against Indian citizens represents perhaps the most disturbing documented instance of privacy violation at the hands of a state actor. Pegasus, developed by the Israeli NSO Group, is capable of harvesting any data stored on a target device, activating cameras and microphones remotely, extracting message histories, and monitoring keystrokes in real time. Investigations by Forbidden Stories and Amnesty

[20] Id.

[21] Id.

[22] Kharak Singh, supra note 8, at 1295 (Subba Rao, J., dissenting); Puttaswamy, supra note 15.

[23] Unique Identification Authority of India, UIDAI Annual Report 2022–23 (2023), https://uidai.gov.in.

[24] Amber Sinha & Srinivas Kodali, Ctr. for Internet & Soc'y, A Legislated Identity: The Aadhaar Project and the Right to Privacy (2017).

[25] Apar Gupta, Aadhaar Data Leaks and the Limits of Biometric Governance, 4 INDIAN J. L. & TECH. 45, 52 (2018).

International revealed a leaked list of over 50,000 phone numbers of individuals allegedly selected for surveillance across multiple countries;[26] over 300 verified Indian mobile numbers appeared on this list, including those of journalists, opposition politicians, judges, and activists.[27] The Indian government neither confirmed nor denied the use of Pegasus, and no independent judicial inquiry has been established. The incident illustrates the inadequacy of existing legal frameworks: Section 5 of the Indian Telegraph Act and Section 69 of the Information Technology Act authorize interception orders on grounds including national security, but neither statute requires prior judicial authorization nor provides for ex post notification to surveilled individuals, leaving citizens without meaningful remedies.

C. Facial Recognition Technology and Algorithmic Surveillance

India's law enforcement and public safety agencies have increasingly deployed facial recognition technology (FRT) for purposes including crowd monitoring, criminal identification, and attendance tracking. By 2019, at least 75 countries had deployed AI-powered surveillance systems.[28] Facial recognition poses qualitatively distinct privacy risks compared with conventional surveillance: it enables covert, mass, real-time identification of individuals in public spaces without any individualized suspicion.[29] Studies have consistently demonstrated that commercial FRT systems exhibit materially higher error rates for individuals of darker skin tones and for women, raising serious concerns about discriminatory misidentification. At present, no legislation specifically governs the deployment of FRT by Indian government agencies, and there is no requirement for algorithmic impact assessments prior to deployment — a gap that the DPDPA only partially addresses for private actors designated as Significant Data Fiduciaries.

D. Corporate Data Collection and Informed Consent

The private sector presents an equally significant threat to informational privacy. Major technology platforms collect vast quantities of data — browsing histories, location information, behavioural patterns, and inferred preferences — often through consent mechanisms that are structurally incapable of generating genuine informed consent. Research in the American context has found that the average privacy policy runs to nearly 7,000 words, requiring approximately thirty minutes to read; reading the privacy policies of the twenty most popular American websites would consume over nine hours.[30] Indian

[26] Council of Europe Parliamentary Assembly, Pegasus Spyware and Surveillance of Politicians, Journalists and Civil Society, Doc. No. 15521 (2022), https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8.

[27] Id.

[28] Ravi Shankara Prasad, AI Surveillance and the Right to Privacy, 12 NUJS L. REV. 1, 8 (2019).

[29] Australian Info. Comm'r, Facial Recognition Technology: A Guide to Assessing the Privacy Risks (2023), https://www.oaic.gov.au.

[30] Lorrie Faith Cranor & Aleecia M. McDonald, The Cost of Reading Privacy Policies, 4 J. L. & POL'Y FOR INFO. SOC'Y 540, 543 (2008).

users face analogous challenges, compounded by lower rates of digital literacy and by the widespread use of "dark patterns" — interface designs that nudge users toward more permissive data sharing than they would otherwise authorize. The DPDPA's consent framework, however well-intentioned, does not adequately address these structural impediments to meaningful consent.

V. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: FRAMEWORK AND CRITIQUE

A. Core Architecture: Consent, Data Principals, and Data Fiduciaries

India enacted the DPDPA on August 11, 2023, establishing the country's first comprehensive statutory framework for data protection. The Act positions consent as the primary lawful basis for processing personal data. Under Section 6, valid consent must be free, specific, informed, unconditional, and expressed through clear affirmative action.[31] The Act creates two central actors: the "data fiduciary," which determines the purpose and means of processing, and the "data principal," the individual whose data is processed.[32] Data principals are granted rights to access information about their data, to seek correction or erasure, to obtain grievance redressal, and to nominate a representative for the exercise of these rights after death.

B. Significant Data Fiduciaries and Enhanced Obligations

The Central Government may designate certain entities as "Significant Data Fiduciaries" (SDFs) based on criteria including the volume and sensitivity of data processed, potential risk to national sovereignty or democratic processes, and the entity's impact on personal rights.[33] SDFs bear heightened obligations: they must appoint an India-resident Data Protection Officer, conduct periodic Data Protection Impact Assessments, engage independent data auditors, and ensure that their algorithms do not adversely affect the rights of data principals.[34] Upon discovering a personal data breach, all data fiduciaries must notify the Data Protection Board and affected individuals without undue delay, and submit a detailed report — including the nature, extent, and timing of the breach, the remedial measures taken, and the notifications dispatched — within 72 hours.[35]

C. Cross-Border Data Transfers

The DPDPA adopts a "blacklisting" approach to cross-border transfers: personal data may flow to any country unless the Central Government has explicitly restricted transfers to that jurisdiction.[36] This stands in sharp contrast to the GDPR's "whitelist" approach, which requires an adequacy determination

[31] Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India) [hereinafter DPDPA].
[32] Id. § 2(j), (k).
[33] Id. § 10.
[34] Id. §§ 8–9.
[35] Id. § 8(6); Digital Personal Data Protection Rules, 2025 (Draft), Rule 7.
[36] DPDPA, supra note 30, § 16.

or appropriate safeguards — such as standard contractual clauses — before personal data may be transferred outside the European Economic Area.[37] In consequence, Indian personal data flows to the overwhelming majority of jurisdictions without any adequacy assessment, potentially exposing citizens to privacy regimes with lower standards of protection.

D. Comparison with the GDPR

A comparison of the DPDPA with the European Union's General Data Protection Regulation illuminates both the progress made and the gaps that remain. The GDPR provides heightened protection for "special categories" of sensitive data — including health information, biometric data, and data concerning racial or ethnic origin — imposing more stringent conditions for their processing.[38] The DPDPA, by contrast, treats all personal data under a single framework without special-category distinctions, a significant omission given the biometric vulnerabilities discussed above. The GDPR's financial penalties — up to four percent of a company's global annual revenue — are generally more powerful deterrents than the DPDPA's fixed monetary caps, which reach a maximum of INR 250 crore for inadequate security safeguards.[39]

VI. STRUCTURAL WEAKNESSES AND ENFORCEMENT GAPS

A. Compromised Regulatory Independence

The DPDPA establishes a Data Protection Board as its primary enforcement body. However, all Board members are appointed by the Central Government,[40] creating structural dependency on the very executive whose data practices the Board is charged with overseeing. Section 27(3) further empowers the government to modify or suspend the Board's orders, enabling the executive to override adverse decisions in cases involving government entities. This arrangement creates a systemic blind spot for public-sector data practices and undermines the institutional autonomy that is a precondition for credible enforcement. Effective data protection law requires a regulator with the independence, resources, and legal authority to investigate and sanction both private and public actors — a standard the current Board structure does not meet.

B. Broad Executive Exemptions and Surveillance Oversight

Section 17 of the DPDPA empowers the Central Government to exempt any government agency from the Act's requirements on grounds including national security, public order, and the prevention of cognizable offences.[41] These exemptions are drafted in sweeping terms, without requiring necessity

[37] Commission Regulation 2016/679, art. 49, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[38] GDPR, supra note 36, art. 9; DPDPA, supra note 30, §§ 1–40.
[39] DPDPA, supra note 30, § 33(2).
[40] DPDPA, supra note 30, § 27(3).
[41] DPDPA, supra note 30, § 17.

assessments, proportionality analyses, or prior judicial authorization. This is constitutionally significant. In *Puttaswamy*, the Supreme Court held that any restriction on the fundamental right to privacy must satisfy a tripartite test of legality, legitimate aim, and proportionality.[42] Blanket executive exemptions that permit surveillance without judicial oversight do not, on their face, satisfy this test. The gap between constitutional doctrine and statutory practice is particularly acute in light of the Pegasus controversy, where the absence of an independent oversight mechanism prevented any meaningful accountability for alleged state-sponsored surveillance.

C. Digital Literacy and the Fiction of Informed Consent

The consent-based architecture of the DPDPA presupposes a data principal who is capable of reading, understanding, and acting upon privacy notices. In India, this presupposition is frequently unrealistic. Millions of citizens engage with digital services through interfaces designed by sophisticated actors who deploy "dark patterns" to maximize data collection. The structural inequality between data principals and large data fiduciaries — in terms of technical knowledge, legal resources, and bargaining power — renders the formal consent framework aspirational rather than protective in many real-world contexts. Effective realization of the DPDPA's consent provisions requires a parallel investment in digital literacy, plain-language disclosure standards, and regulatory action against manipulative interface design.

VII. RECOMMENDATIONS

This paper advances five recommendations to strengthen the right to privacy in India's digital environment. First, the Data Protection Board's independence should be secured by requiring that appointments be made by a statutory selection committee with participation from the judiciary and civil society, and by eliminating the executive's power to modify or suspend the Board's orders. Second, Section 17's exemptions should be narrowed and conditioned: surveillance conducted under national security or public order grounds should require prior judicial authorization except in genuine emergencies, with mandatory ex post notification and periodic reporting to a parliamentary oversight committee. Third, the DPDPA should introduce special-category protection for biometric, health, genetic, and children's data, consistent with international best practice. Fourth, the government should mandate algorithmic impact assessments before deploying facial recognition or other AI-based surveillance systems in public spaces, and should establish a moratorium on live FRT pending the introduction of a governing legal framework. Fifth, the government and the UGC should integrate digital literacy — including practical instruction on data rights, privacy settings, and the recognition of dark patterns — into school and university curricula, recognizing that legal rights without the knowledge to exercise them are effectively illusory.

[42] See generally Puttaswamy, supra note 15 (establishing legality, legitimate aim, and proportionality as the three conditions for permissible restrictions on privacy).

VIII. CONCLUSION

The right to privacy in India has traversed a remarkable arc: from the Supreme Court's early refusals to recognize it as a fundamental right, through the incremental doctrinal advances of *Govind* and *Rajagopal*, to the unanimous and philosophically rich verdict in *Puttaswamy*. That judgment established privacy as intrinsic to human dignity and personal liberty — a hard-won recognition that reversed decades of constitutional uncertainty. The subsequent application of *Puttaswamy* in *Navtej Singh Johar* demonstrated that this constitutional foundation can be deployed to dismantle laws that entrench discrimination in the most intimate domains of human life.

Yet the promise of *Puttaswamy* remains incompletely realized. The threats to privacy posed by biometric databases, state spyware, AI surveillance, and corporate data harvesting are qualitatively novel — and the DPDPA, while a meaningful legislative step forward, contains structural deficiencies that limit its protective reach. A genuinely autonomous Data Protection Board, tightly drawn surveillance exemptions with judicial oversight, special-category protections for sensitive data, and sustained investment in digital literacy are not merely desirable additions to the existing framework — they are the conditions under which a constitutional right to privacy can function as a living protection rather than an aspirational norm.