International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 17-02-2026; Accepted: 19-03-2026; Published: 03-04-2026
Volume 12, Issue 2, 2026, Page No. 474-478

The evolution of the right to privacy in India: A constitutional analysis

Tanushree Khichi
Research Scholar, Jai Narain Vyas University, Jodhpur, Rajasthan, India
DOI: https://doi.org/10.66856/ijl.2026.12.2.12209

Abstract
Background: The right to privacy occupies a central position in India's constitutional edifice. Though not expressly enumerated in the Constitution, it has been progressively recognized as an essential component of the fundamental rights framework, particularly under Article 21, which guarantees the right to life and personal liberty.
Objective: This paper analyses the constitutional and judicial evolution of the right to privacy in India, tracing its development from early judicial scepticism to its landmark recognition as a fundamental right by the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India (2017).
Methodology: The study adopts a doctrinal-analytical methodology, relying on primary sources including constitutional provisions, judicial decisions, and legislative enactments, supplemented by secondary sources comprising academic commentary and comparative legal scholarship.
Key Findings: The paper finds that the right to privacy has evolved through distinct judicial phases: initial denial, qualified recognition, and finally unanimous affirmation as a fundamental right. The Puttaswamy judgment is a watershed moment in Indian constitutional law. However, significant challenges persist in the digital era, particularly concerning data protection, state surveillance, and artificial intelligence.
Conclusion: While Indian privacy jurisprudence has made transformative strides, the Digital Personal Data Protection Act, 2023 and the absence of an independent data protection authority reveal continuing structural gaps. Stronger safeguards, robust institutional oversight, and a rights-based approach to data governance are urgently required.

Keywords: Right to privacy, Article 21, fundamental rights, constitutional law, puttaswamy, data protection

Introduction

Privacy is a foundational value of human existence. It creates a sphere of individual autonomy that shields persons from arbitrary intrusions by the State, corporations, and other individuals. The capacity to control one's personal information, bodily integrity, domestic affairs, and intimate relationships is not merely a legal entitlement but a precondition for a dignified human life. Privacy enables individuals to develop their personalities, exercise freedom of expression, form associations, and participate meaningfully in democratic governance.

In the Indian constitutional context, privacy derives its significance from the deeper commitments of the Constitution to liberty, dignity, and individual autonomy. The Preamble promises to secure to every citizen "liberty of thought, expression, belief, faith and worship" and to promote "fraternity, assuring the dignity of the individual." These foundational commitments create a constitutional ethos within which privacy necessarily operates as a core value, even in the absence of an express provision.

For several decades, however, the constitutional status of privacy remained contested. Early decisions of the Supreme Court, particularly M.P. Sharma v. Satish Chandra (1954) [1] and Kharak Singh v. State of Uttar Pradesh (1962), either denied or qualified the existence of a fundamental right to privacy. It was only through a long and evolving line of judicial decisions, culminating in the historic nine-judge bench ruling in Justice K.S. Puttaswamy v. Union of India (2017) [7], that privacy was unanimously recognised as an intrinsic component of the right to life and personal liberty under Article 21 of the Constitution.

Against this backdrop, this paper pursues the following research objectives: (i) to trace the constitutional foundations of the right to privacy in India; (ii) to analyse the judicial evolution of privacy rights from 1954 to 2017 [24]; (iii) to identify contemporary challenges to privacy in the digital era; and (iv) to critically evaluate the existing legal framework and propose future directions for strengthening privacy protection in India.

The study employs a doctrinal-analytical methodology. Primary sources, comprising constitutional provisions, judgments of the Supreme Court and High Courts, and statutory enactments, form the backbone of the analysis. Secondary sources, including academic articles, comparative constitutional scholarship, and reports of law commissions, are used to contextualise and interrogate the primary materials. The scope of the study is confined to the constitutional dimension of privacy rights in India, with comparative references to international standards where appropriate.

Constitutional Foundations of the Right to Privacy

1. Privacy and Fundamental Rights

The Indian Constitution does not expressly enumerate a right to privacy among the fundamental rights guaranteed under Part III. Nevertheless, privacy finds implicit support in a cluster of fundamental rights provisions. Article 14 guarantees equality before the law and the equal protection of the laws, prohibiting arbitrary state action that may invade individual privacy without reasonable justification. Article 19, which guarantees a range of freedoms including freedom of speech and expression, freedom of association, and the right to move freely throughout the territory of India, necessarily implies a private sphere of individual activity that is shielded from state interference.

Most significantly, Article 21 provides that "no person shall be deprived of his life or personal liberty except according to procedure established by law." This provision has served as the principal constitutional anchor for the right to privacy. The Supreme Court's expansive interpretation of "life" under Article 21, beginning with the landmark decision in Maneka Gandhi v. Union of India (1978) [4], transformed this provision from a narrow procedural guarantee into a substantive charter of individual rights encompassing dignity, liberty, and all facets of a life worth living.

The concept of human dignity, while not a separately enumerated right, pervades the entire constitutional scheme. It finds expression in the Preamble, in the Directive Principles of State Policy, and in the fundamental duties. Privacy and dignity are inseparably linked: an invasion of privacy is, in its very essence, a violation of the dignity of the person. This constitutional commitment to dignity provides a powerful normative basis for the recognition and protection of privacy as a fundamental constitutional value.

2. Privacy as an Implied Constitutional Right

The doctrine of implied constitutional rights holds that fundamental rights are not exhausted by the express text of the Constitution but may be derived by necessary implication from the constitutional structure and the rights expressly guaranteed. This interpretive methodology has been extensively employed by the Supreme Court of India to read a rich set of rights into the broad language of Part III.

The expansion of Article 21 jurisprudence following Maneka Gandhi created fertile ground for the judicial recognition of implied rights. The Court recognised that the "right to life" must be interpreted expansively to include not merely the right to exist but the right to live with dignity, which presupposes a zone of personal privacy. Over successive decades, the Court implied rights to livelihood, health, education, a clean environment, and ultimately, privacy, from the foundational guarantee of life and personal liberty.

This interpretive approach aligns with the purposive method of constitutional interpretation, which holds that constitutional provisions must be construed in accordance with the objectives they seek to achieve. Since the overarching purpose of Part III is to protect individuals from arbitrary state power and to secure conditions for a dignified human life, an interpretation that includes privacy within the ambit of fundamental rights is not only defensible but constitutionally mandated.

Judicial Evolution of the Right to Privacy in India

1. Early Judicial Approach

1.1 M.P. Sharma v. Satish Chandra (1954) [1]

The Supreme Court's earliest significant engagement with the right to privacy arose in M.P. Sharma v. Satish Chandra, AIR 1954[1] SC 300. The case concerned the validity of search and seizure operations conducted under the Code of Criminal Procedure. The petitioners challenged the searches as unconstitutional, arguing that they violated an implied right to privacy.

An eight-judge Constitution Bench of the Supreme Court rejected this contention. The Court held that the framers of the Constitution did not intend to subject the power of search and seizure to the restrictions applicable to fundamental rights, and that no fundamental right akin to the Fourth Amendment of the United States Constitution could be read into Part III of the Indian Constitution. This decision effectively foreclosed, at least for a time, the development of a constitutional right to privacy. The Court's restrictive approach was rooted in an originalist interpretive methodology that declined to read rights not expressly stated in the constitutional text.

1.2 Kharak Singh v. State of Uttar Pradesh (1962)

Eight years later, the Supreme Court revisited the issue in Kharak Singh v. State of Uttar Pradesh, AIR 1963[2] SC 1295. The petitioner challenged the validity of police surveillance under the Uttar Pradesh Police Regulations, which authorised domiciliary visits, secret surveillance, and restrictions on the movement of persons classified as "history-sheeters."

The majority judgment struck down the provision permitting domiciliary night visits as a violation of the right to personal liberty under Article 21 but declined to recognise a general fundamental right to privacy. Justice Subba Rao, in a notable dissent, advanced a broader vision, holding that the right to privacy is an essential ingredient of personal liberty and that surveillance by the State, even without physical restraint, constitutes a violation of Article 21. While the majority's position prevailed for some years, Justice Subba Rao's dissent sowed the seeds for the subsequent expansion of privacy rights.

2. Recognition of Privacy Rights

2.1 Govind v. State of Madhya Pradesh (1975) [3]

A decisive shift occurred in Govind v. State of Madhya Pradesh, AIR 1975[3] SC 1378, where a three-judge bench of the Supreme Court explicitly recognised that the right to privacy is a fundamental right implicit in the rights guaranteed under Articles 19 and 21. The Court, while upholding the validity of police surveillance regulations subject to a test of compelling state interest, acknowledged that individual privacy is a constitutionally protected value.

The Govind judgment introduced the concept of a "penumbral right" to privacy, drawing inspiration from American constitutional jurisprudence. The Court held that fundamental rights have peripheral values, and privacy constitutes one such value that resides in the penumbra of Articles 19 and 21. Importantly, the Court also formulated an early balancing test, holding that privacy could be overridden only when there exists a compelling state interest and the means adopted are narrowly tailored to achieve that interest. This proportionality framework became foundational to subsequent privacy jurisprudence.

2.2 R. Rajagopal v. State of Tamil Nadu (1994) [5]

In R. Rajagopal v. State of Tamil Nadu, (1994) [5] 6 SCC 632, also known as the "Auto Shankar" case, the Supreme Court extended the right to privacy to the domain of reputational and informational autonomy. The case arose from a challenge by the State of Tamil Nadu to prevent the publication of the auto-biography of a convicted murderer, which allegedly contained information about high-ranking officials.

The Court held that every citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing, and education. The Court further distinguished between matters relating to the individual's public persona and those pertaining to his private sphere, holding that the state cannot interfere with private matters

unless they concern a matter of legitimate public interest. This decision marked the emergence of informational privacy as a distinct dimension of the constitutional right to privacy and foreshadowed the subsequent developments in data protection law.

2.3 PUCL v. Union of India (1997) [6]

In People's Union for Civil Liberties v. Union of India, (1997) [6] 1 SCC 301, the Supreme Court addressed the constitutional implications of telephone tapping. The Court held that telephone tapping constitutes a serious invasion of an individual's right to privacy, which falls within the ambit of Article 21, and that such interception must be authorised by a procedure that is fair, just, and reasonable.

The Court laid down a series of procedural safeguards that must be observed before telephone tapping can be authorised by the State. These included the requirements of a competent authority, recorded reasons, minimal intrusion, and periodic review. The PUCL judgment thus established the principle that the right to privacy, even when subject to reasonable restrictions in the interest of national security or public order, must be protected by procedural guarantees that prevent its arbitrary curtailment. This principle of procedural due process in matters affecting privacy became an important strand of Indian privacy jurisprudence.

3. The Landmark Justice K.S. Puttaswamy v. Union of India (2017) [7]

3.1 Facts and Issues

The case of Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) [7] 10 SCC 1, arose from a challenge to the constitutional validity of the Aadhaar scheme, a biometric-based unique identification programme administered by the Unique Identification Authority of India. Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition before the Supreme Court contending that the collection and centralised storage of biometric and demographic data by the Government violated the right to privacy.

During the pendency of the Aadhaar matter, a three-judge bench noted a conflict between two prior Constitution Bench decisions, namely M.P. Sharma (1954) [1] and Kharak Singh (1962), on the one hand, and a series of later decisions recognising a qualified right to privacy, on the other. The matter was accordingly referred to a nine-judge Constitution Bench to definitively resolve the question: "Is the right to privacy a fundamental right under the Indian Constitution?"

3.2 Judgment

On 24 August 2017, the nine-judge Constitution Bench of the Supreme Court unanimously answered in the affirmative. All nine judges held that the right to privacy is a fundamental right under the Indian Constitution, constituting an intrinsic component of the right to life and personal liberty under Article 21 and the freedoms guaranteed under Part III. The majority opinion, authored by Justice D.Y. Chandrachud and joined by three other judges, provided the most comprehensive analysis. Four separate concurring opinions were also delivered.

The majority judgment identified three aspects of privacy: (i) privacy of the person or bodily integrity, which protects individuals against violations of their physical body; (ii) informational privacy, which protects the right to control information about oneself; and (iii) privacy of choice, which protects the autonomy of individuals to make decisions about their lives. The Court held that these dimensions of privacy are protected both against state action and, to a degree, against private intrusion.

The Court overruled the decisions in M.P. Sharma and Kharak Singh insofar as they held that the right to privacy is not a fundamental right. It affirmed the correctness of the line of decisions from Govind to PUCL that had recognised a qualified right to privacy. The Court further held that any law curtailing the right to privacy must satisfy the three-part test of: (i) legality, meaning the limitation must be prescribed by law; (ii) legitimate aim, meaning it must serve a legitimate state objective; and (iii) proportionality, meaning the means adopted must be proportionate to the aim pursued.

3.3 Constitutional Significance

The Puttaswamy judgment is a constitutional landmark of the highest magnitude. It settles, with finality, the long-contested question of privacy's constitutional status and provides a comprehensive doctrinal framework for the analysis of privacy claims. By grounding the right to privacy in the fundamental values of dignity, liberty, and autonomy that animate the entire constitutional scheme, the Court elevated privacy from a peripheral penumbral value to a foundational constitutional right.

The judgment has significant implications for a wide range of legal and policy matters. It provides constitutional backing for the protection of personal data, the regulation of state surveillance, the decriminalisation of consensual same-sex conduct (which was subsequently achieved in Navtej Singh Johar v. Union of India, 2018) [9], the protection of reproductive autonomy, and the right to die with dignity. In each of these domains, the constitutional recognition of privacy as a fundamental right operates as a powerful constraint on legislative and executive action.

Privacy Challenges in the Digital Era

1. Data Protection and Informational Privacy

The rapid proliferation of digital technologies has created unprecedented challenges for informational privacy. In the digital environment, vast quantities of personal data are generated, collected, processed, and shared across complex networks of entities, often without the meaningful knowledge or consent of the individuals concerned. The Puttaswamy judgment's recognition of informational privacy as a dimension of the fundamental right to privacy has established a constitutional basis for data protection, but the translation of this constitutional guarantee into effective legal protection has been slow and contested.

India's first comprehensive data protection legislation, the Digital Personal Data Protection Act, 2023[13] (DPDPA), represents a significant step forward. The DPDPA establishes a framework for the collection, processing, and storage of digital personal data, introduces the concept of consent as the primary basis for data processing, and creates a data principal rights framework including rights of access, correction, and erasure. However, critics have pointed to significant gaps, including broad exemptions for the state, weak provisions on data localisation, and the absence of an independent data protection authority, as limitations that undermine the statute's effectiveness.

2. Aadhaar and State Surveillance

The Aadhaar biometric identification system represents perhaps the most significant and contested privacy challenge in contemporary India. Following the Puttaswamy judgment, the constitutional validity of Aadhaar was upheld by a three-to-two majority of the Supreme Court in Justice K.S. Puttaswamy v. Union of India (Aadhaar), (2018) [8] 1 SCC 809, subject to important limitations. The Court struck down the use of Aadhaar for purposes beyond entitlement to government benefits and services and prohibited private entities from mandating Aadhaar authentication.

The Aadhaar judgment illustrates the tension between the legitimate state interest in efficient service delivery and the constitutional imperative of privacy protection. The collection and centralised storage of biometric data by the government creates a potential infrastructure for mass surveillance that poses profound risks to civil liberties. Critics have argued that the safeguards affirmed in the Aadhaar judgment are insufficient and that the architecture of the system is inherently prone to abuse.

Beyond Aadhaar, the Indian State has deployed a range of surveillance technologies, including CCTV networks, facial recognition systems, and interception of electronic communications, often in the absence of adequate legal frameworks or judicial oversight. The absence of comprehensive surveillance legislation and an independent oversight body represents a significant lacuna in the protection of privacy rights.

3. Social Media, Artificial Intelligence and Emerging Threats

Social media platforms and artificial intelligence systems present novel and rapidly evolving challenges to privacy. The business models of major social media companies are predicated on the collection and monetisation of user data, creating structural incentives for privacy invasion. Indian users of these platforms are subject to extensive data profiling, targeted advertising, and algorithmic manipulation, often without adequate legal protection.

Artificial intelligence and machine learning technologies enable the analysis of vast datasets to infer sensitive attributes, including political opinions, religious beliefs, health conditions, and sexual orientation, from seemingly innocuous data. These capabilities create serious risks of discriminatory profiling, manipulation, and exploitation. The regulation of AI in the Indian context remains nascent, and the existing legal framework does not adequately address the privacy risks posed by AI-driven data processing.

Emerging technologies such as deepfakes, facial recognition, and behavioural biometrics further expand the frontier of privacy threats. Deepfake technology, which enables the creation of realistic synthetic media, poses particular risks to personal reputation and dignity. The absence of specific legislation addressing these threats creates a significant protection gap that the constitutional recognition of privacy alone cannot fill.

Critical Analysis and Future Directions

Indian privacy jurisprudence has achieved remarkable advances in a relatively short period. The Puttaswamy judgment stands as a testament to the Supreme Court's capacity for creative constitutional interpretation, providing a principled and comprehensive framework for the analysis of privacy claims. The proportionality standard adopted by the Court is well-suited to navigate the complex trade-offs between privacy and competing interests such as national security, public order, and the right to information.

The recognition of privacy as a multidimensional right encompassing bodily integrity, informational self-determination, and autonomy of choice is conceptually sophisticated and provides a flexible framework capable of adaptation to new contexts. The Court's grounding of privacy in the values of dignity and liberty ensures that it is not treated as a merely formal or procedural right but as a substantive guarantee of individual freedom.

Notwithstanding these strengths, significant gaps in legal protection persist. The most fundamental is the inadequacy of the legislative response to the constitutional mandate of privacy protection. The Digital Personal Data Protection Act, 2023[13], while a necessary first step, falls short in several respects. Its broad governmental exemptions, particularly those permitting state processing of data for reasons of national security and public order without adequate safeguards, risk creating a vast zone of unaccountable surveillance. The Act's consent framework has been criticised as insufficiently robust, permitting deemed consent in a range of situations that may not reflect genuine autonomy.

A further gap lies in the absence of institutional infrastructure for privacy protection. The Data Protection Board of India, established under the DPDPA, lacks the independence, resources, and powers necessary to serve as an effective regulator. An independent, adequately funded, and technically expert data protection authority, modelled on the best international practices, is essential for the effective enforcement of privacy rights.

Looking to the future, three directions appear particularly important. First, Parliament should enact comprehensive surveillance legislation that establishes a clear legal basis for state interception and surveillance activities, provides for independent judicial or quasi-judicial oversight, and creates effective remedies for victims of unlawful surveillance. Second, the regulatory framework for artificial intelligence should incorporate strong privacy-by-design requirements and establish clear accountability standards for entities deploying AI systems that process personal data. Third, public education and awareness about privacy rights and remedies must be strengthened, enabling individuals to effectively assert their constitutional entitlements.

Conclusion

The evolution of the right to privacy in India is a story of constitutional growth through judicial creativity. From the narrow, text-bound approach of M.P. Sharma in 1954[1], through the incremental recognition of privacy as a qualified right in Govind, Rajagopal, and PUCL, to the unanimous and expansive affirmation of privacy as a fundamental right in Puttaswamy in 2017[24], the trajectory of Indian privacy law reflects the Constitution's living character and the judiciary's role as its authoritative interpreter.

The Puttaswamy judgment is more than a decision about privacy; it is a statement about the kind of constitutional republic India aspires to be. By grounding privacy in dignity, liberty, and autonomy — the deepest values of the constitutional order — the Supreme Court has affirmed that individuals are not merely subjects of state power but bearers of rights that the state must respect, protect, and fulfil. The constitutional significance of this affirmation cannot be overstated.

At the same time, the translation of constitutional recognition into effective legal protection remains an incomplete project. The Digital Personal Data Protection Act, 2023[13] represents progress but requires strengthening. Surveillance law, AI regulation, and institutional infrastructure for privacy protection demand urgent attention. The right to privacy, having been so laboriously established as a constitutional fundamental, now requires robust legislative and institutional scaffolding to become a lived reality for all Indians.

The future of privacy rights in India will be shaped by the interplay of technological change, legislative action, judicial oversight, and civil society advocacy. This paper has sought to contribute to that ongoing conversation by providing a comprehensive constitutional analysis of the evolution of the right to privacy, identifying its foundations and achievements, and charting the directions in which further progress is necessary. Privacy, as the Supreme Court has affirmed, is not a privilege of the few; it is a fundamental right of every person, and its effective protection is a measure of the health of Indian constitutional democracy.

References

1. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
2. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
3. Govind v. State of Madhya Pradesh, AIR 1975 SC 1378.
4. Maneka Gandhi v. Union of India, AIR 1978 SC 597.
5. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
6. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
7. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
8. Justice K.S. Puttaswamy v. Union of India (Aadhaar judgment), (2018) 1 SCC 809.
9. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.
10. The Constitution of India, 1950.
11. The Information Technology Act, 2000 (as amended in 2008).
12. The Unique Identification Authority of India Act, 2016.
13. The Digital Personal Data Protection Act, 2023.
14. The Telegraph Act, 1885.
15. Bhatia G. The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India, 2019.
16. Austin G. The Indian Constitution: Cornerstone of a Nation. Oxford University Press, 1966.
17. Seervai HM. Constitutional Law of India (4th ed.). N.M. Tripathi, 1996.
18. Jain MP. Indian Constitutional Law (7th ed.). LexisNexis, 2014.
19. Solove DJ. Understanding Privacy. Harvard University Press, 2008.
20. Warren SD, Brandeis LD. The right to privacy. Harvard Law Review,1890:4(5):193–220.
21. Chandrachud DY. Privacy as a constitutional value. Indian Journal of Constitutional Law,2020:12(1):1–22.
22. Bhandari V. Privacy after Puttaswamy: Implications for data protection law in India. National Law School of India Review,2018:30(1):1–35.
23. Parsheera S. Data protection in India: Looking beyond Puttaswamy. The Leap Blog, IFMR Finance Foundation, 2018.
24. Khosla M. Privacy as a constitutional value: Reflections on Puttaswamy. Economic and Political Weekly,2017:52(42):29–34.
25. Narayan A. Aadhaar, privacy and the law. Journal of Indian Law and Society,2019:10(2):45–72.
26. Ray A. The right to privacy in the age of artificial intelligence: An Indian perspective. NLSIU Law Review,2019:31(2):88–110.