
THE RIGHT TO PRIVACY IN THE DIGITAL AGE AN INDIAN CONSTITUTIONAL PERSPECTIVE

***Swati Mishra**

India.

Article Received: 16 September 2026

*Corresponding Author: Swati Mishra

Article Revised: 06 October 2026

India.

Published on: 26 October 2026

DOI: <https://doi-doi.org/101555/ijrpa.7682>

INTRODUCTION

In an era where every click, transaction, and location ping generates a digital trace, the question of privacy has moved from philosophical debate to constitutional necessity. India, home to over 850 million internet users and the world's largest biometric identity program, sits at the center of this tension. The Indian Constitution, drafted in 1950, makes no explicit mention of a "right to privacy." Yet through decades of judicial interpretation, privacy has emerged as one of the most significant fundamental rights of the digital era.

The Constitutional Silence and Its Resolution

Unlike some modern constitutions, India's founding document does not contain an express privacy clause. For years, this silence was interpreted narrowly. In *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962), the Supreme Court declined to recognize privacy as a distinct fundamental right, reasoning that the Constitution's framers had deliberately omitted it.

This position began shifting through a series of progressive judgments that read privacy into Article 21's guarantee of "life and personal liberty," interpreting the word "life" expansively to include dignity, autonomy, and personal space.

The Puttaswamy Watershed

The turning point arrived with *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge Constitution Bench decision. The case originated from petitions challenging the Aadhaar scheme's constitutional validity, but its scope expanded into a foundational inquiry: does India's Constitution guarantee a right to privacy at all?

The Court's unanimous answer was yes. Key holdings included:

- Privacy is intrinsic to Article 21 — it flows from the right to life and personal liberty, and also draws support from the freedoms guaranteed under Article 19.
- Privacy is not a monolith — it encompasses bodily autonomy, informational self-determination, decisional privacy, and protection of personal data.
- Privacy is not absolute — the state may restrict it, but only through a law that satisfies a three-fold test: legality (existence of law), necessity (a legitimate state aim), and proportionality (a rational nexus between the means adopted and the objective, with minimal infringement).

This proportionality standard became the yardstick against which all subsequent digital-age laws and state actions would be measured.

Digital Flashpoints Since Puttaswamy

1. Aadhaar and Biometric Identity

In the follow-up judgment, Puttaswamy II (2018), the Court upheld the core Aadhaar architecture as serving a legitimate welfare-distribution purpose, but struck down its mandatory linkage to bank accounts and mobile SIM cards as disproportionate. This drew a line between permissible state interest in service delivery and impermissible overreach into private life.

2. The Data Protection Framework

Puttaswamy explicitly called on Parliament to enact a data protection law. After a long legislative journey—including the Justice B.N. Srikrishna Committee's 2018 draft and several revised bills—India passed the Digital Personal Data Protection Act, 2023 (DPDP Act). It establishes:

- Consent-based processing of personal data
- Obligations on "data fiduciaries" (entities collecting data)
- Rights for individuals ("data principals") to access, correct, and erase their data
- A Data Protection Board for enforcement

Critics note that the Act grants broad exemptions to government agencies for reasons of national security and public order, potentially diluting the proportionality standard Puttaswamy demanded of state action.

3. Surveillance and Interception

State surveillance under the Telegraph Act, 1885, and the Information Technology Act, 2000, must now be tested against the proportionality framework. Concerns over projects like the Central Monitoring System, and revelations about spyware such as Pegasus, have kept judicial and public scrutiny alive on whether India's surveillance apparatus operates within constitutional limits or largely outside effective oversight.

4. Intermediary Regulation and Encryption

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, require significant social media intermediaries to enable traceability of message originators. This has triggered a direct conflict between law enforcement's investigative interests and the right to private, encrypted communication—an issue currently being litigated by platforms like WhatsApp.

5. Right to Be Forgotten

Though not yet codified in comprehensive form, several High Courts (Delhi, Karnataka, Kerala, Orissa) have recognized a limited "right to be forgotten," allowing individuals to seek removal of personal information from public records or search results in specific circumstances, such as matrimonial disputes or acquittals in criminal cases.

Structural Gaps

Despite the doctrinal clarity offered by Puttaswamy, implementation faces real challenges:

- **Enforcement capacity:** The Data Protection Board under the DPDP Act lacks the independence and resources of counterparts like the EU's data protection authorities.
- **State exemptions:** Broad carve-outs for government instrumentalities risk creating a two-tier privacy regime—robust against private companies, weak against the state.
- **Emerging technologies:** Facial recognition systems, deployed by police forces across states, largely operate without dedicated statutory backing or judicial guidelines, raising the same concerns Puttaswamy sought to address.
- **Cross-border data flows:** As Indian citizens' data increasingly moves across jurisdictions via cloud services, questions of extraterritorial protection remain unsettled.

CONCLUSION

India's constitutional journey on privacy reflects a broader global reckoning with technology's power to intrude on personal autonomy. Puttaswamy transformed privacy from an unstated assumption into an enforceable fundamental right, anchored in dignity and liberty. Yet the

digital age keeps generating new fronts—AI-driven surveillance, algorithmic profiling, biometric databases—faster than legislative and institutional safeguards can mature. The proportionality test remains the constitutional compass, but its real strength will be tested not in judgments alone, but in whether India's data protection institutions can independently hold both corporations and the state accountable.