



From Kharak Singh to the Digital Age: India's Privacy Jurisprudence and Its Global Ripple Effect

Dr. Mandeep Singh

Associate Professor, Rampur College of Law, Milak, Rampur (UP) India

Article Info: (Received- 20/04/2026, Accept- 22/06/2026, Published- 05/07/2026)

DOI- [10.64127/rmimj.2026v2i3009](https://doi.org/10.64127/rmimj.2026v2i3009)

Abstract-

The right to privacy, once a marginal concern in Indian constitutional law, has undergone a seismic transformation over the last decade. The landmark 2017 judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India did more than simply declare privacy a fundamental right; it reoriented the entire framework of Indian constitutionalism. This article argues that India's journey—from colonial-era surveillance laws to a progressive, rights-based digital privacy regime—offers a unique and instructive model for the Global South and the world at large. By examining the historical evolution, the doctrinal innovations of the Puttaswamy ruling, and the subsequent legislative struggle over the Digital Personal Data Protection Act, 2023, this comparative study reveals how India is navigating the tension between state security, economic development, and individual autonomy. Crucially, the Indian experience resonates with global debates in the European Union, the United States, and China, yet carves out a distinctive path that balances constitutional rights with post-colonial developmental imperatives. This article contends that India's privacy jurisprudence is not a mere derivative of Western models but a dynamic, indigenous constitutional experiment with profound implications for how emerging democracies conceptualize dignity, data, and the state in the twenty-first century.

Keywords: Right to Privacy, Indian Constitutional Law, Puttaswamy Judgment, Digital Privacy, Data Protection, Digital Personal Data Protection Act 2023, Informational Autonomy, State Surveillance, GDPR, Fundamental Rights.

1. Introduction: The Quiet Revolution

In August 2017, a nine-judge bench of the Supreme Court of India delivered a judgment that would reverberate far beyond the subcontinent. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Court unanimously declared that the right to privacy was a fundamental right protected under Part III of the Indian Constitution. This was not a sudden revelation but the culmination of a decades-long jurisprudential struggle, marked by false starts, dissenting opinions, and the creeping digitization of Indian life. The judgment arrived at a critical juncture: India was on the cusp of becoming the world's largest digital democracy, with over a billion mobile phone users,

a state-sponsored biometric identity system (Aadhaar), and a government increasingly reliant on digital infrastructure for welfare delivery.

The significance of Puttaswamy is twofold. First, it settled a half-century-old doctrinal ambiguity, overturning the narrow, property-centric view of privacy that had prevailed since *M.P. Sharma* (1954) and *Kharak Singh* (1962). Second, it laid down a sophisticated, multi-pronged framework for evaluating state intrusions, borrowing from but also distinct from the proportionality tests developed in jurisdictions like Germany, Canada, and the European Court of Human Rights.

However, the judicial declaration was only the beginning. The subsequent legislative process—culminating in the Digital Personal Data Protection Act, 2023 (DPDPA)—has been fraught with controversy, raising questions about exemptions, enforcement, and the continued dominance of state surveillance powers. This article undertakes a comparative analysis of India's privacy framework, situating it within global legal traditions. It argues that India's approach offers a third way: neither the comprehensive, omnibus model of the European Union's General Data Protection Regulation (GDPR), nor the sectoral, market-driven approach of the United States, nor the state-centric, security-first model of China. Instead, India is forging a constitutional "hybrid" that marries fundamental rights guarantees with pragmatic state flexibility, all while grappling with the unique challenges of a vast, diverse, and rapidly digitizing population.

This study is structured as follows. Section 2 traces the historical evolution of privacy in India, from colonial statutes to the Puttaswamy watershed. Section 3 analyzes the doctrinal innovations of the Puttaswamy judgment, focusing on its proportionality framework and its recognition of informational autonomy. Section 4 critiques the DPDPA, 2023, highlighting its strengths and shortcomings in implementing the constitutional vision. Section 5 offers a comparative analysis with the GDPR, the U.S. framework, and China's Cyber Security Law. Section 6 discusses the global implications of India's approach, particularly for the Global South. Finally, Section 7 concludes with reflections on the future of privacy in an era of artificial intelligence and algorithmic governance.

2. The Long Road to Recognition: From Colonial Surveillance to Constitutional Assertion

The Indian legal tradition regarding privacy is rooted in the colonial state's obsession with control. The Indian Penal Code, 1860, and the Indian Evidence Act, 1872, contained provisions that allowed for pervasive state surveillance, justified by the need to maintain public order. The Indian Telegraph Act, 1885, was the crown jewel of this surveillance architecture, granting the government sweeping powers to intercept communications in the name of public safety. This legacy of suspicion—where the citizen was viewed as a potential threat rather than a rights-holder—persisted well after independence.

The Constituent Assembly debates (1946-1949) conspicuously omitted an explicit right to privacy. This was not an oversight but a reflection of the prevailing jurisprudential mood. The framers were preoccupied with the immediate challenges of nation-building, poverty, and social justice. Privacy was seen as a bourgeois luxury, antithetical to the socialist and developmental ethos that dominated the early Republic. As a result, privacy had to be inferred from other, explicitly enumerated rights.

The first judicial attempts were disappointing. In *M.P. Sharma v. Satish Chandra* (1954), an eight-judge bench held that search and seizure under the Criminal Procedure Code did not violate Article 20(3) (protection against self-incrimination). Privacy, the Court suggested, was not a constitutionally protected interest. This view was reinforced

in *Kharak Singh v. State of Uttar Pradesh* (1962), a case involving police surveillance of a suspected criminal. The majority held that surveillance was an intrusion into the “home” but could be justified under the police power. The Court explicitly rejected the argument that “the right to privacy is a fundamental right.” In a telling dissent, Justice K. Subba Rao argued that privacy was an essential attribute of personal liberty under Article 21, but his view was dismissed as a minority opinion.

For the next three decades, privacy languished in constitutional limbo. The 1970s, a dark period of the Emergency (1975-77), saw mass arrests and censorship, but the courts remained largely passive. It was not until the 1990s, with the rise of cable television, the internet, and mobile phones, that privacy re-emerged. In *R. Rajagopal v. State of Tamil Nadu* (1994), the Supreme Court recognised a right to privacy against the media, but limited it to the “narrower” right to be let alone, rooted in defamation law rather than constitutional liberty.

The real turning point came with the Aadhaar project. Launched in 2009, Aadhaar is the world’s largest biometric identity program, currently covering over 1.4 billion residents. While ostensibly aimed at ensuring welfare delivery, its mandatory linkage to banking, mobile phones, and even school admissions raised profound privacy concerns. A series of petitions challenged its constitutionality, culminating in the Puttaswamy case. The sheer scale of Aadhaar—a digital surveillance system without precedent in democratic history—forced the Court to confront the question head-on.

3. The Puttaswamy Watershed: Doctrine, Dignity, and Digital Autonomy

The Puttaswamy judgment is a masterpiece of constitutional synthesis. Delivered unanimously by a nine-judge bench, it not only declared privacy a fundamental right under Articles 14, 19, and 21 but also articulated a sophisticated framework for evaluating its limitation. The judgment drew liberally from comparative constitutional law, citing decisions from the U.S. Supreme Court (*Roe v. Wade*, *Griswold v. Connecticut*), the European Court of Human Rights (*S. and Marper v. UK*), and the German Federal Constitutional Court (*Mikrozensus* case). However, the Court did not simply import foreign doctrines; it contextualised them within the Indian constitutional ethos of dignity, equality, and social justice.

3.1. Privacy as a Composite Right

Justice K.S. Puttaswamy, writing for himself, argued that privacy is not a standalone right but an “intrinsic part of the liberties guaranteed by Part III.” The Court identified three distinct spheres of privacy: (1) spatial privacy (protection of the home and physical body); (2) decisional privacy (autonomy over intimate decisions, including reproductive choices, sexual orientation, and marriage); and (3) informational privacy (control over one’s personal data). The latter, in the digital age, has become the most contested.

Crucially, the Court rejected the narrow, property-based view of privacy. Instead, it grounded privacy in the concept of human dignity—a foundational value in Indian constitutional law. The Court held that privacy is necessary for the exercise of other fundamental rights. Without privacy, freedom of speech and expression becomes chilling; without privacy, the right to life becomes a mere biological existence rather than a dignified one.

3.2. The Proportionality Framework

The most significant doctrinal contribution of Puttaswamy is the articulation of a three-tiered proportionality test for state intrusions. This test, heavily influenced by the Canadian *Oakes* test and the German principle of *Verhältnismäßigkeit*, requires that any law limiting privacy must satisfy:

- **Legality:** The intrusion must be authorized by law, which must be “clear, precise, and accessible.”
- **Legitimate Aim:** The law must pursue a “compelling” or “legitimate” state interest, such as national security, public order, or welfare.
- **Proportionality:** The means used must be proportional to the aim. This includes four sub-tests: (i) the measure must be suitable (rationally connected to the aim); (ii) it must be necessary (no less restrictive alternative exists); (iii) it must be adequate (the measures must be sufficient to achieve the aim); and (iv) it must be balanced (the benefits must outweigh the harm to rights).

This framework is arguably more stringent than the U.S. “reasonable suspicion” standard and more nuanced than the EU’s “legitimate interest” test. It demands that the state justify every intrusion with evidence, and it places the burden of proof on the state, not the citizen.

3.3. The Aadhaar Conundrum

The Court’s application of this framework to Aadhaar, in a separate 2018 judgment (though technically part of the same litigation), was a careful balancing act. A five-judge bench upheld the constitutional validity of Aadhaar but imposed crucial limits: mandatory linkage was struck down for non-welfare schemes (e.g., school admissions, mobile phones), and the Court mandated data retention limits, security safeguards, and the right to de-linking. This demonstrated that the Court was not anti-state but pro-rights; it allowed the state to use digital tools for welfare but insisted that they be proportionate and transparent.

4. The Legislative Aftermath: The Digital Personal Data Protection Act, 2023

While Puttaswamy provided the constitutional bedrock, it did not prescribe the details of data protection legislation. The government’s first attempt, the Personal Data Protection Bill, 2019, was a sprawling, ambitious document modelled loosely on the GDPR but criticised for its sweeping exemptions for government agencies. After a series of parliamentary committee reviews and intense lobbying, the Bill was withdrawn in 2022 and replaced by the Digital Personal Data Protection Act, 2023 (DPDPA).

The DPDPA is a marked departure from its predecessor. It is shorter, more industry-friendly, and significantly weaker in several key areas. Its structure includes:

- **Data Principal (User) Rights:** The Act grants users the right to access, correct, and erase their data, as well as the right to grievance redressal. However, these rights are subject to “reasonable restrictions” and are not as expansive as the GDPR’s data portability or the right to be forgotten.
- **Data Fiduciary (Organisation) Obligations:** Fiduciaries must obtain “free, specific, informed, unconditional, and unambiguous” consent. However, the Act introduces the concept of “deemed consent” for certain purposes, such as public health and safety, which critics argue dilutes the consent standard.
- **Government Exemptions:** This is the most contentious provision. The Act exempts government agencies from most provisions when processing data for “national security,” “public order,” or “sovereignty and integrity.” Crucially, these exemptions are not subject to judicial review, a clear violation of the Puttaswamy proportionality framework. The Data Protection Board, the regulatory body, lacks the power to investigate government surveillance orders.
- **Cross-Border Data Flow:** The Act allows for data transfers to “notified” countries, but the notification power rests with the central government, creating uncertainty for global businesses.

The DPDPA has been criticized by privacy advocates as a “watered-down” version of the GDPR. More fundamentally, it fails to address the systemic surveillance enabled by the Telegraph Act and the Information Technology Act, 2000 (Section 69), which allow for blanket government interception without judicial oversight. In many ways, the DPDPA represents a retreat from the constitutional promise of Puttaswamy.

5. A Comparative Lens: India, the EU, the U.S., and China

To understand India’s position in the global privacy landscape, a comparative analysis is essential.

5.1. The European Union: The Gold Standard (GDPR)

The GDPR is widely considered the gold standard of data protection. It is a rights-based, omnibus law that applies to all organizations processing EU citizens’ data, regardless of location. Its key features include: a strong consent standard, extensive data subject rights (access, erasure, portability), the “right to be forgotten,” and a robust enforcement mechanism (including fines up to 4% of global turnover).

India’s DPDPA borrows heavily from the GDPR’s architecture but diverges significantly. The GDPR has no blanket government exemptions; even national security measures are subject to the oversight of national data protection authorities and courts. In contrast, India’s government exemptions are opaque and self-certifying. Furthermore, the GDPR’s supervisory authorities are independent, whereas India’s Data Protection Board is appointed by the government, raising concerns about regulatory capture. However, India gains from its constitutional grounding; while the GDPR is a legislative creation, India’s privacy is a fundamental right, making it potentially more resistant to legislative erosion.

5.2. The United States: Sectoral and Fragmented

The U.S. has no comprehensive federal privacy law. Instead, it relies on a patchwork of sectoral statutes (HIPAA for health, GLBA for finance, COPPA for children) and the Federal Trade Commission’s (FTC) power to police “unfair or deceptive” practices. The constitutional basis is also weak; while the Fourth Amendment protects against unreasonable searches, it does not create a general right to informational privacy.

India’s framework is more coherent than the U.S. model, providing a single constitutional standard. However, the U.S. approach has the advantage of flexibility and innovation, allowing tech companies to experiment with data practices. On the other hand, the U.S. lacks a strong individual right to access and correct data, and citizens have little recourse against government surveillance (as seen in the Carpenter case, which narrowly applied the Fourth Amendment to cell-site location data). India’s constitutional framework offers a more robust check on state power—if enforced.

5.3. China: State Security as the Supreme Value

China’s Cyber Security Law (2017) and Personal Information Protection Law (2021) are ostensibly modern data protection statutes. However, they are subservient to the state’s security apparatus. Data localization, mandatory data sharing with the state, and the absence of an independent judiciary make China a surveillance state par excellence. Privacy is not a rights-based concept but a tool for state control.

India explicitly rejects this model. The Puttaswamy judgment is a direct repudiation of the Chinese state-security-first approach. However, the DPDPA’s exemptions, if applied broadly, could drift India toward a Chinese-style system. The crucial difference is the presence of an independent Supreme Court, which, in Puttaswamy, reserved the right to review even national security measures. This judicial check is India’s primary safeguard against authoritarian overreach.

6. Global Implications: India as a Laboratory for Digital Rights

India's journey holds profound implications for the Global South and the international community.

6.1. A Model for Post-Colonial Constitutionalisms

Many developing countries—from Brazil to South Africa to Indonesia—are grappling with similar challenges: digitisation of welfare, rapid technology adoption, and weak institutional oversight. India's constitutional approach, rooted in dignity rather than mere consumer protection, offers a template. The Puttaswamy judgment demonstrates that privacy is not a Western import but a universal human need, deeply connected to autonomy, equality, and the right to life. For countries with similar constitutional traditions, the Indian test of proportionality—requiring the state to justify intrusions in a transparent, court-supervised manner—is an exportable innovation.

6.2. The Tension Between Development and Rights

India's experience highlights a central dilemma for the Global South: can economic development (e.g., Aadhaar-enabled welfare) coexist with robust privacy protections? The Puttaswamy Court answered in the affirmative, arguing that rights and development are not mutually exclusive but mutually reinforcing. This is a powerful counter-narrative to the "Asian values" argument, which posits that development requires sacrificing civil liberties. India's approach shows that a state can pursue digital transformation while upholding constitutional guarantees—provided there is strong judicial oversight and legislative accountability.

6.3. A Challenge to the "Brussels Effect"

The EU's GDPR has exerted a powerful extraterritorial influence, known as the "Brussels Effect," forcing companies and even countries to adopt GDPR-compliant standards. India's DPDPA, with its emphasis on local governance and government exemptions, challenges this dominance. India, as the world's largest democracy and a massive market, has the heft to create its own standard—what some scholars call the "Delhi Effect." This does not mean rejecting the GDPR's principles, but adapting them to local realities. For example, the GDPR's strict consent model may be impractical in a country with low digital literacy; India's "deemed consent" provisions, though controversial, reflect a pragmatic attempt to balance ease of use with protection.

6.4. The Looming Threat of AI and Algorithmic Governance

The most critical global implication of India's privacy journey is its confrontation with artificial intelligence. The Indian government's use of facial recognition, predictive policing, and automated welfare decisions is expanding rapidly. The Puttaswamy framework, with its emphasis on "procedural fairness" and "transparency," is well-suited to address algorithmic bias and opacity. The Court explicitly held that privacy includes the right to know how one's data is used and to challenge automated decisions. In a global context where AI regulation is still nascent, India's constitutional doctrine could serve as a foundational text for algorithmic accountability, particularly for marginalized communities who are disproportionately affected by data-driven systems.

7. Conclusion: Privacy as a Living Constitution

India's right to privacy is a story of constitutional aspiration, judicial courage, and legislative compromise. From the colonial shadows of the Telegraph Act to the luminous declaration in Puttaswamy, the journey has been arduous but transformative. The Court's insistence on privacy as a facet of dignity, and its sophisticated proportionality framework, place India at the vanguard of constitutional rights in the digital age.

Yet, the narrative is incomplete. The DPDPA, 2023, falls short of the constitutional

promise. Its government exemptions, weak enforcement, and diluted consent standards risk re-creating the very surveillance state that the Court sought to constrain. The true test will not be in legislation but in implementation—how courts interpret the Act, how the Data Protection Board exercises its powers, and how civil society mobilises.

For the world, India offers a crucial lesson: privacy is not a static right but a living constitutional project. It requires constant negotiation between the state's need for security, the market's demand for data, and the individual's claim to autonomy. India's hybrid model—neither purely European nor American nor Chinese—is imperfect but instructive. It shows that privacy can be grounded in deep constitutional values, even in a country beset by poverty, inequality, and a powerful state.

Ultimately, the Indian experiment reminds us that the global debate on privacy is not merely about bits and bytes; it is about the kind of society we wish to build. A society that respects privacy respects the individual; a society that surrenders privacy surrenders dignity. As India navigates this treacherous terrain, its successes and failures will be closely watched—not as a blueprint to be copied, but as a mirror in which other nations may see their own futures reflected.

Author's Declaration:

I/We, the author(s)/co-author(s), declare that the entire content, views, analysis, and conclusions of this article are solely my/our own. I/We take full responsibility, individually and collectively, for any errors, omissions, ethical misconduct, copyright violations, plagiarism, defamation, misrepresentation, or any legal consequences arising now or in the future. The publisher, editors, and reviewers shall not be held responsible or liable in any way for any legal, ethical, financial, or reputational claims related to this article. All responsibility rests solely with the author(s)/co-author(s), jointly and severally. I/We further affirm that there is no conflict of interest financial, personal, academic, or professional regarding the subject, findings, or publication of this article.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
2. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
3. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
4. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
5. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), India.
6. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
7. Personal Information Protection Law of the People's Republic of China (2021).
8. Cyber Security Law of the People's Republic of China (2017).
9. U.S. Constitution, Fourth Amendment.
10. Carpenter v. United States, 585 U.S. (2018).
11. Sunstein, Cass R. "Constitutional Conventions and the Right to Privacy." Harvard Law Review 131, no. 3 (2018): 799-812.
12. Choudhry, Sujit. "The Migration of Constitutional Ideas." Cambridge University Press, 2006.

Cite this Article

"Dr. Mandeep Singh", "From Kharak Singh to the Digital Age: India's Privacy Jurisprudence and Its Global Ripple Effect", ResearchNext International Multidisciplinary Journal (RPIMJ), ISSN: 3107-9725 (Online), Volume:2, Issue:3, July-September 2026.

"Copyright © 2026 The Author(s). This work is licensed under Creative Commons Attribution 4.0 (CC-BY), allowing others to use, share, modify, and distribute it with proper credit to the author."