



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA (2017): EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

Aradhya Singh

INTRODUCTION

The 2017 landmark judgment in *Justice K.S. Puttaswamy v. Union of India* marks a historic constitutional renaissance in Indian jurisprudence.¹ Triggered by a retired judge's challenge to the biometric Aadhaar project, the Union of India argued that privacy was not a guaranteed fundamental right, relying on antiquated post-independence precedents.

Overturning decades of state-centric rulings, a unanimous nine-judge bench of the Supreme Court declared the Right to Privacy an intrinsic part of the Right to Life and Personal Liberty under Article 21. The court recognized privacy as an inalienable, natural right essential for human dignity and autonomy, classifying it into spatial, informational, and bodily dimensions.²

This case comment critically analyzes the evolution of privacy jurisprudence in India. It examines the court's legal reasoning, evaluates the structural "proportionality test" established to counter state overreach, and assesses the judgment's enduring impact on digital data protection and individual liberty.

FACTS OF THE CASE

The genesis of this landmark litigation lies in the implementation of the Aadhaar project by the Government of India. In January 2009, the Union Government established the Unique Identification Authority of India (UIDAI) through an executive notification. The primary

¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India)

² *Id.*

objective was to issue a 12-digit unique identity number to all Indian residents to streamline the distribution of welfare subsidies and eliminate leakages in public distribution systems.³

To issue Aadhaar cards, the UIDAI collected extensive personal data, including demographic details and sensitive biometrics like fingerprints and iris scans. Crucially, during its initial years, this massive data collection drive lacked any legislative backing and operated purely through executive orders.

In 2012, Justice K.S. Puttaswamy, a 91-year-old retired judge of the Karnataka High Court, filed a Writ Petition under Article 32 before the Supreme Court.⁴ He challenged the constitutional validity of the scheme, arguing that the mandatory collection of biometrics violated an individual's right to bodily autonomy and privacy. Furthermore, he highlighted that the state lacked a robust statutory framework to protect this digital data from cyber threats or unauthorized surveillance.

The Union of India countered with a major threshold objection, arguing that the petitioner could not claim a violation of privacy because the Indian Constitution did not explicitly guarantee a Right to Privacy. The state relied on two older, larger-bench precedents: *M.P. Sharma v. Satish Chandra* (1954) (eight judges) and *Kharak Singh v. State of U.P.* (1962) (six judges), which held that privacy was not a fundamental right.⁵

To resolve this profound legal deadlock and review the correctness of these past judgments, the matter was referred to a historic nine-judge constitutional bench, tasking them with authoritatively determining the status of privacy in India.

ISSUES BEFORE THE COURT

The historic nine-judge constitutional bench of the Supreme Court of India was primarily tasked with resolving a fundamental jurisdictional deadlock rather than deciding the operational validity of the Aadhaar scheme itself. The core legal issues framed before the Court were:

³ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India)

⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁵ *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India); *Kharak Singh v. State of U.P.*, A.I.R. 1963 S.C. 1295 (India)

1. **EXISTENCE OF THE RIGHT:** Whether the Right to Privacy is a constitutionally protected, fundamental right under the Constitution of India, despite its absence from the explicit text of Part III.⁶
2. **CONSTITUTIONAL ANCHOR:** If privacy is a fundamental right, where does it find its primary source and constitutional anchor—specifically, is it an implicit, intrinsic facet of the Right to Life and Personal Liberty guaranteed under Article 21?
3. **VALIDITY OF PRECEDENTS:** Whether the prior decisions of the larger benches in *M.P. Sharma v. Satish Chandra (1954)* (eight-judge bench) and *Kharak Singh v. State of U.P. (1962)* (six-judge bench) which held that privacy is not a fundamental right were correctly decided and remained good law.

ARGUMENTS BY THE PARTIES

ARGUMENTS ON BEHALF OF THE PETITIONERS

The petitioners, led by senior advocates representing Justice K.S. Puttaswamy, argued that the Right to Privacy is a multi-dimensional, natural right that inheres in every human being. Their core submissions included:

- **CONSTITUTIONAL ANCHOR:** Privacy is an essential, intrinsic element of Part III of the Constitution, flowing directly from the Right to Life and Personal Liberty under Article 21, and the freedom of speech and movement under Article 19.⁷
- **DIGNITY AND AUTONOMY:** Relying on the progressive jurisprudence established in *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248, they asserted that a life with dignity is impossible without personal autonomy⁸, informational control, and bodily integrity.
- **OUTDATED PRECEDENTS:** They argued that *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300, and *Kharak Singh v. State of U.P.*, A.I.R. 1963 S.C. 1295, reflected an obsolete, siloed approach to fundamental rights that was no longer good law in a modern digital democracy.

⁶ *Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1.

⁷ INDIA CONST. arts. 19, 21.

⁸ *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248 (India).

ARGUMENTS ON BEHALF OF THE RESPONDENTS

The Union of India and various state governments vigorously countered the petition, presenting a literalist and state-centric defense:

- **TEXTUAL ABSENCE:** The state contended that the framers of the Constitution deliberately chose not to explicitly include privacy as a standalone fundamental right in Part III.
- **BINDING PRECEDENTS:** They argued that the larger benches in *M.P. Sharma* (eight judges) and *Kharak Singh* (six judges) bindingly settled that privacy is merely a common law or statutory right, not a fundamental one.
- **WELFARE IMPERATIVE:** The state asserted that for a developing nation, socio-economic rights and the seamless distribution of public welfare subsidies—facilitated securely via Aadhaar—must take precedence over an elusive, elitist claim to absolute personal privacy.

JUDGEMENT

On August 24, 2017, a historic nine-judge constitutional bench of the Supreme Court of India delivered a unanimous 9:0 verdict declaring the **Right to Privacy a fundamental right**.⁹ The apex court explicitly overruled the long-standing precedents of *M.P. Sharma v. Satish Chandra (1954)* (eight-judge bench) and *Kharak Singh v. State of U.P. (1962)* (six-judge bench) to the extent that they held privacy was not constitutionally protected.

The Court held that privacy is an elemental right that serves as a prerequisite for the exercise of all other fundamental freedoms.¹⁰ While the bench affirmed that privacy is not absolute and remains subject to reasonable restrictions, it mandated that any state intrusion must clear the highest threshold of constitutional scrutiny. The matter was subsequently referred back to a regular bench to decide the operational validity of the Aadhaar scheme based on these newly established constitutional principles.

RATIO DECIDENDI

⁹ *Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1.

¹⁰ *Id.*

The core *ratio decidendi* rests on the principle that the Right to Privacy is an **inalienable, natural right** inherent to human dignity, autonomy and liberty.¹¹ It is not a statutory creation or a gift from the state, but a right that flows inherently from **Article 21** (Right to Life and Personal Liberty) and is deeply intertwined with the guarantees of Articles 14 and 19.

To regulate state infractions, the Court established a strict **three-fold proportionality test**.¹² For a state infringement on privacy to be constitutionally permissible, it must satisfy three cumulative conditions:

1. **LEGALITY:** The state action must be backed by a clear, existing law.
2. **LEGITIMATE AIM:** The law must serve a valid, justifiable state objective (such as public welfare or national security).
3. **PROPORTIONALITY:** There must be a rational nexus between the object sought and the means adopted, ensuring the least intrusive method is used.

CRITICAL ANALYSIS

The *Puttaswamy* judgment is a watershed moment, dismantling decades of state-centric jurisprudence by explicitly overruling *M.P. Sharma (1954)* and *Kharak Singh (1962)*.¹³ By anchoring privacy within Article 21 and the "Golden Triangle," the Court discarded narrow textualism for a progressive, person-centric approach, dividing privacy into spatial, bodily, and informational dimensions. This conceptual shift effectively catalyzed historic reforms, including the decriminalization of homosexuality in *Navtej Singh Johar (2018)*.¹⁴

However, a sharp dichotomy exists between the judgment's lofty theory and its practical execution. The subjective nature of the newly introduced "proportionality test" became evident when a subsequent bench upheld the Aadhaar project, prioritizing welfare distribution over data privacy. Ultimately, while *Puttaswamy* constructed a magnificent constitutional fortress on paper, its execution remains vulnerable to administrative convenience and leaves the horizontal threat of corporate Big Tech surveillance largely to statutory remedy.

IMPACT OF THE JUDGEMENT

¹¹ Id.

¹² Id.

¹³ *Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1.

¹⁴ *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1 (India).

The *Puttaswamy* verdict triggered a paradigm shift across India's legislative and social landscapes. By elevating privacy to an unalienable constitutional guarantee, it acted as a legal catalyst, stripping away state immunities regarding surveillance and personal choices.

Socially, the judgment's emphasis on bodily autonomy permanently transformed civil liberties. It served as the structural foundation for the decriminalization of consensual same-sex relationships in *Navtej Singh Johar v. Union of India*, (2018) 1 S.C.C. 1,¹⁵ and strengthened constitutional protections surrounding reproductive rights, gender identity, and marital choices.

Statutorily, *Puttaswamy*'s mandate on informational privacy forced a complete overhaul of India's digital architecture. It directly compelled the enactment of the comprehensive **Digital Personal Data Protection (DPDP) Act**,¹⁶ followed by the operationalization of the **DPDP Rules**, establishing a strict regulatory framework governing data fiduciaries, mandatory consent protocols, and citizen digital rights.

CONCLUSION

The *Puttaswamy* judgment stands as an immortal monument in India's constitutional history, marking the evolution of a text-bound judiciary into a dynamic guardian of human dignity. By unanimously recognizing the Right to Privacy as an intrinsic component of Article 21, the Supreme Court successfully emancipated Part III of the Constitution from the restrictive, post-independence constraints of *M.P. Sharma* and *Kharak Singh*.

While the practical application of the judgment has faced legitimate criticism—particularly regarding the subsequent judicial leeway granted to the Aadhaar project—its structural legacy is irreversible. *Puttaswamy* provided the vital legal vocabulary needed to dismantle archaic social laws, directly inspiring the decriminalization of homosexuality in *Navtej Singh Johar v. Union of India*, (2018) 1 S.C.C. 1, and forcing the state to construct a comprehensive legislative framework through the Digital Personal Data Protection Act.

Ultimately, *Puttaswamy* ensures that as India advances into an era dominated by artificial intelligence, biometrics, and corporate data mining, the state cannot weaponize technology to

¹⁵ Id.

¹⁶ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

eclipse individual liberty. It cements privacy not as a concession granted by the government, but as an inalienable right essential for a free, autonomous, and democratic citizenry.