



# Right to Privacy as a Fundamental Right: A Constitutional Analysis

Dr. Alka Nanda

Associate Professor, HRIT University

**Abstract:** *The right to privacy has emerged as one of the most significant fundamental rights in contemporary constitutional jurisprudence. This paper examines the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), where the Supreme Court of India unanimously recognized privacy as a fundamental right protected under Articles 14, 19, and 21 of the Indian Constitution. The research analyzes the constitutional evolution of privacy rights from early judicial interpretations to its present status as an intrinsic component of personal liberty and human dignity. Through a comprehensive examination of judicial precedents, constitutional provisions, and contemporary legal challenges, this paper demonstrates how privacy rights have transformed from judicial recognition to constitutional mandate. The study traces the development from the restrictive approach in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1962) to the expansive interpretation in the Puttaswamy judgment, which overruled earlier decisions. The research concludes that privacy as a fundamental right represents a necessary constitutional adaptation to modern technological challenges while balancing individual autonomy with legitimate state interests. The paper also examines the implementation of privacy protection through legislative frameworks, including the Digital Personal Data Protection Act, 2023, and its implications for constitutional governance in the digital age.*

**Keywords:** *Right to Privacy, Fundamental Rights, Constitutional Law, Article 21, Puttaswamy Judgment*

## 1. Introduction

The concept of privacy as a fundamental right represents one of the most significant developments in Indian constitutional jurisprudence in recent decades. Privacy, as recognized in Article 12 of the Universal Declaration of Human Rights, 1948, and Article 17 of the International Covenant on Civil and Political Rights, 1966, forms an essential component of human dignity and individual autonomy<sup>1</sup>. In the Indian context, the right to privacy gained constitutional recognition through judicial interpretation, culminating in the historic Puttaswamy

judgment of 2017<sup>2</sup>. The Supreme Court's unanimous declaration that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution" marked a watershed moment in constitutional history. This recognition came after decades of judicial deliberation and conflicting interpretations, finally settling the constitutional status of privacy rights in India. The significance of this development extends beyond mere legal doctrine. In an era of rapid digitalization, mass surveillance capabilities, and increasing data collection by both state and non-state actors, the constitutional protection of privacy rights assumes critical importance for democratic governance and individual freedom. The judgment acknowledges that privacy is required to be

<sup>1</sup>Universal Declaration of Human Rights, 1948, Art. 12; International Covenant on Civil and Political Rights, 1966, Art. 17.

<sup>2</sup>Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (nine-judge bench decision)



analyzed in an interconnected world, and the Supreme Court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world.

## 2. Objectives

1. To analyze the constitutional evolution of privacy rights from early judicial pronouncements to the Puttaswamy judgment.
2. To examine the scope and dimensions of privacy protection under Article 21 and other constitutional provisions.
3. To evaluate contemporary challenges and future implications of privacy as a fundamental right in digital governance.

## 3. Historical Development and Constitutional Framework

### Early Judicial Approach: The Restrictive Phase

The journey of privacy rights in Indian constitutional law began with judicial encounters that initially adopted a restrictive approach. The case of *M.P. Sharma v. Satish Chandra* (1954)<sup>1</sup> marked one of the first instances where the Supreme Court dealt with privacy-related issues while examining the validity of search and seizure provisions under the Criminal Procedure Code, 1898. In this case, an eight-judge bench of the Supreme Court held that the Indian Constitution did not guarantee a fundamental right to privacy, distinguishing the Indian constitutional framework from the Fourth Amendment protections available under the U.S. Constitution. The petitioner contended that since the search served as a stand-in for the subpoena's forced surrender, it constituted coerced testimony that was illegal under Article 20(3)<sup>2</sup>. However, the Court determined that the search and document seizure did not violate Article 20(3) since they did not amount to "compulsory testimony". This narrow interpretation established a precedent that would influence privacy jurisprudence for several decades.

<sup>1</sup>*M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (eight-judge bench)

<sup>2</sup>Constitution of India, Article 20(3) - "No person accused of any offence shall be compelled to be a witness against himself."

The subsequent case of *Kharak Singh v. State of U.P.* (1962)<sup>3</sup> presented another opportunity for the Court to examine privacy rights, this time in the context of police surveillance under Chapter 20 of U.P. Police Regulations. The case involved surveillance measures including domiciliary visits, picketing, and shadowing of suspected criminals. While the Court struck down nighttime domiciliary visits as violative of personal liberty under Article 21<sup>4</sup>, it upheld other surveillance measures, maintaining that there was no general fundamental right to privacy under the Constitution. The Court's rejection of *Kharak Singh* was later based on two prongs. First, it held that the judgment was internally contradictory, because the Court could not have struck down domiciliary visits on any other ground but that of privacy; indeed, in doing so, the Court had itself quoted American judgments affirming a right to privacy.

### Constitutional Provisions and Interpretative Evolution

The Indian Constitution, while not explicitly mentioning privacy as a fundamental right, contains several provisions that form the constitutional foundation for privacy protection. Article 21<sup>5</sup>, which guarantees that "no person shall be deprived of his life or personal liberty except according to procedure established by law," has been the primary vehicle through which privacy rights have been recognized and protected. Article 21 asserts that no person shall be deprived of their life except according to the procedure established by law. The right to life encompasses various aspects, including the right to live with dignity, the right to livelihood, and the right to a healthy environment. The Supreme Court's expansive interpretation of "life" and "personal liberty" in Article 21 has enabled the recognition of various unenumerated rights, including the right to privacy. The extension in the dimensions of Article 21 has been made possible by giving an extended meaning to the words 'life' and 'liberty' in Article 21. These two words are not to be read narrowly but are organic terms which are to be construed meaningfully. This interpretative approach has allowed the Constitution to evolve with changing social needs and technological developments.

<sup>3</sup>*Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (six-judge bench)

<sup>4</sup>Constitution of India, Article 21 - "No person shall be deprived of his life or personal liberty except according to procedure established by law."

<sup>5</sup>Constitution of India, Article 21 - "No person shall be deprived of his life or personal liberty except according to procedure established by law."

**Intermediate Developments: Gradual Recognition**

The period between the early restrictive judgments and the Puttaswamy decision witnessed gradual judicial recognition of privacy rights in specific contexts. In the case of *State of Maharashtra v. Madhukar Narayan Mardikar* (1991)<sup>1</sup>, it was held by the Supreme Court that every person has the right to privacy and can seek the protection of the same, even when the person is a woman of easy virtue. This judgment marked a significant departure from the earlier restrictive approach and recognized privacy as a broader principle applicable to all individuals regardless of their social status or moral character. In the landmark case concerning telephonic surveillance, the Supreme Court held that the right to have a telephonic conversation without intrusion is a part of the right to privacy under Article 21 and cannot be curtailed except by procedures established by law<sup>2</sup>. The Court noted that procedural safeguards for fair and reasonable exercise of substantive power of surveillance were essential to prevent arbitrary state action. These intermediate decisions laid the groundwork for the eventual comprehensive recognition of privacy rights in the Puttaswamy judgment. They demonstrated the Court's evolving understanding of privacy as an essential component of human dignity and personal autonomy.

**3. The Puttaswamy Landmark: Constitutional Recognition****Background and Constitutional Question**

The constitutional question regarding privacy as a fundamental right arose in the context of challenges to the Aadhaar scheme<sup>3</sup>, a nationwide biometric identification system. Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition in the Supreme Court challenging the constitutional validity of the Aadhaar scheme introduced by the UPA Government. The constitutional validity of the Aadhaar system (a nationwide biometric identification system) had been challenged before the Supreme Court. This issue was before a 5 judge bench of the Court ("Aadhaar Bench"). One of the key

issues was whether the norms for compilation of the demographic biometric data by the government violates the right to privacy. The constitutional question became more complex when the Attorney-General for India, representing the Union of India, argued that the Constitution did not guarantee any fundamental right to privacy. This declaration during the challenge to the Aadhaar Scheme led to the three judges hearing the case referring the constitutional question to a larger bench of five judges which, in turn, referred it further to a nine-judge bench.

**The Nine-Judge Bench Decision**

On August 24, 2017, a nine-judge bench of the Supreme Court consisting of J.S. Khehar, J. Chelameswar, S.A. Bobde, R.K. Agrawal, R.F. Nariman, A.M. Sapre, D.Y. Chandrachud, S.K. Kaul, and S.A. Nazeer unanimously held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21<sup>4</sup> and as a part of the freedoms guaranteed by Part III<sup>5</sup> of the Constitution." The Privacy Bench unanimously held that the right to privacy is a fundamental right protected under the Constitution. The judges delivered 6 judgments: Justice Chandrachud wrote on behalf of himself, Chief Justice JS Khehar, Justice Agrawal and Justice Abdul Nazeer ("Lead Judgment"). Justice Chelameswar, Justice Bobde, Justice Sapre, Justice Nariman and Justice Kaul wrote separate judgments providing their own findings, conclusions and observations. The judgment explicitly overruled previous judgments of the Supreme Court in *Kharak Singh*<sup>6</sup> vs. *State of UP* and *M.P. Sharma*<sup>7</sup> vs. *Sharma vs. Union of India*, which held that there is no fundamental right to privacy under the Indian Constitution. This constitutional clarification settled decades of judicial uncertainty and established privacy as an inviolable fundamental right.

**Doctrinal Framework and Constitutional Basis**

The Lead Judgment started by acknowledging that (i) Privacy allows each individual/person to be left alone in a core which is inviolable; (ii) this autonomy is conditioned by their relationships with the rest of society; (iii) those relationships pose questions to autonomy and free choice.

<sup>1</sup>*State of Maharashtra v. Madhukar Narayan Mardikar*, (1991) 1 SCC 57

<sup>2</sup>Constitution of India, Article 21 - "No person shall be deprived of his life or personal liberty except according to procedure established by law."

<sup>3</sup> Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

<sup>4</sup>Constitution of India, Article 21 - "No person shall be deprived of his life or personal liberty except according to procedure established by law."

<sup>5</sup>Constitution of India, Part III (Fundamental Rights)

<sup>6</sup>*Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (six-judge bench)

<sup>7</sup>*M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (eight-judge bench)



The judgment recognized that privacy operates within a social framework and must be balanced with other constitutional values and state interests. The Court adopted the three-pronged test required for the encroachment of any Article 21<sup>1</sup> right – legality – i.e. through an existing law; necessity, in terms of a legitimate state objective and proportionality, that ensures a rational nexus between the object of the invasion and the means adopted to achieve that object. This test provides a constitutional framework for evaluating any restrictions on privacy rights, ensuring that such restrictions meet stringent constitutional standards. The Court declared that the protection of privacy was included in the expanded definition of personal liberty. The Supreme Court specifically adopted the three criteria that must be met before Article 21 rights can be infringed upon: legality, necessity, and proportionality.

#### 4. Scope and Dimensions of Privacy Rights

##### Constitutional Scope under Article 21

The Supreme Court of India has extended the purview of Article 21 to include the right to privacy as part of the Right to Life and Liberty. Article 21 speaks about the right to life and personal liberty, applicable to both citizens and non-citizens, which cannot be taken away by the state except under procedure as prescribed by law.

The constitutional recognition of privacy under Article 21 encompasses multiple dimensions:

- **Personal Autonomy and Dignity:** Privacy is a right enjoyed by every human being by virtue of their existence. It can extend to other aspects such as bodily integrity, personal autonomy, and protection from state surveillance, dignity, confidentiality, etc. The right ensures that individuals have control over their personal choices and can make decisions about their private lives without unwarranted interference.
- **Informational Privacy:** The judgment especially declared that, in this new technological era, the personal data of a person, especially his biometric data, forms valuable information and can be used by another having unauthorized access; hence, protection of informational privacy needs to be guaranteed. This aspect has become increasingly crucial in the digital age where vast amounts of

personal data are collected, processed, and stored by various entities.

- **Physical Privacy:** The protection extends to physical spaces and bodily integrity, ensuring freedom from unreasonable searches, surveillance, and interference with one's physical person and property.

##### Relationship with Other Fundamental Rights

By declaring that privacy is inherent to every fundamental liberty provided in Part III<sup>7</sup> of the Constitution, the Supreme Court has made privacy an essential ingredient of other important fundamental freedoms. Privacy rights intersect with and reinforce other constitutional guarantees:

- **Article 14<sup>2</sup> (Right to Equality):** Privacy protection ensures equal treatment in matters of personal autonomy and prevents discriminatory interference with individual choices.
- **Article 19<sup>3</sup> (Freedom of Speech and Expression):** Privacy enables free expression by ensuring individuals can express, explore, and share their ideas without fear of judgment or retribution, which strengthens democratic discourse and personal development.
- **Articles 25-28<sup>4</sup> (Freedom of Religion):** Privacy protections extend to religious beliefs and practices, ensuring freedom of conscience and religious expression.

#### 5. Contemporary Challenges and Legislative Response

##### Digital Age Challenges

The Court adopted a liberal interpretation of the fundamental rights to meet the challenges posed by an increasing digital age. It held that individual liberty must extend to digital spaces and individual autonomy and privacy must be protected. The digital revolution has created new challenges for privacy protection that require both constitutional and legislative responses.

The proliferation of digital technologies has led to:

<sup>2</sup>Constitution of India, Article 14 - "The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India."

<sup>3</sup>Constitution of India, Article 19 - "All citizens shall have the right to freedom of speech and expression."

<sup>4</sup>Constitution of India, Articles 25-28 (Freedom of Religion)

<sup>1</sup>Constitution of India, Article 21 - "No person shall be deprived of his life or personal liberty except according to procedure established by law."





- **Mass Data Collection:** Online platforms, mobile applications, and digital services collect vast amounts of personal data, often without explicit user consent or awareness.
- **State Surveillance Capabilities:** Advances in technology have expanded government surveillance capabilities, raising concerns about the balance between security and privacy.
- **Cross-Border Data Flows:** Globalization of digital services has complicated jurisdiction and enforcement of privacy protections.
- **Algorithmic Decision-Making:** Automated systems increasingly make decisions affecting individuals' lives, raising questions about transparency and accountability.

#### **Legislative Framework: Digital Personal Data Protection Act, 2023**

The Indian parliament enacted India's first comprehensive data protection law on 11 August 2023, namely the Digital Personal Data Protection Act 2023 (the DPDPA)<sup>1</sup>. The DPDPA will replace India's existing patchwork of data protection rules and is expected to trigger significant changes in how companies subject to Indian data protection laws process personal data.

Key provisions of the DPDPA include:

- **Scope and Application:** The Act covers personal data, i.e., data about an individual that can identify them. This includes identifiers like name, phone number, email address, postal address and Aadhaar number. It also includes profiling data or usage data, for e.g., a user's preferences. It only covers 'digital' data, not offline records unless they are digitised.
- **Consent Framework:** The DPDPA's consent standard requires consent to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action" and, unlike the GDPR, it does not permit processing under the lawful bases of contractual necessity or legitimate interests.
- **Individual Rights:** Data principals will have certain rights similar to those under the GDPR for data subjects (i.e., rights of access, correction, or erasure), they will also benefit from a number of new rights which are unique to the DPDPA, i.e., the right to a readily available and effective means of grievance redressal and the right to nominate an individual who will be able to

exercise the rights of the data principal in the event of death or incapacity.

#### **Implementation Challenges**

The implementation of privacy rights in the digital context faces several significant challenges that require coordinated responses from multiple stakeholders. Technological complexity remains a primary concern as the rapid pace of technological change often outpaces legal and regulatory responses, creating gaps in protection that can be exploited by both state and private actors. The development of new technologies such as artificial intelligence, machine learning, and blockchain creates novel privacy risks that existing legal frameworks may not adequately address. Enforcement mechanisms present another significant challenge, as ensuring compliance with privacy laws requires robust institutional capacity and adequate resources for regulatory bodies. The cross-border nature of digital services complicates jurisdictional issues and creates opportunities for regulatory arbitrage, where entities can avoid compliance by operating from jurisdictions with weaker privacy protections.

Furthermore, balancing innovation with protection remains a delicate task, as overly restrictive regulations may stifle technological development and economic growth, while insufficient protections leave individuals vulnerable to privacy violations. The need for public awareness and digital literacy also presents ongoing challenges, as effective privacy protection requires informed users who understand their rights and how to exercise them. Additionally, the integration of privacy protection with existing legal frameworks, particularly in areas such as freedom of information and transparency requirements, requires careful consideration to avoid conflicting obligations. These implementation challenges underscore the need for adaptive legal frameworks, strong institutional capacity, international cooperation, and continued stakeholder engagement to ensure effective privacy protection in the digital age.

## **6. Comparative Analysis and International Perspectives**

### **International Framework**

Privacy rights are recognized internationally through Article 12 of the Universal Declaration of Human Rights, 1948<sup>2</sup> and Article 17 of the International Covenant on

<sup>1</sup>The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023

<sup>2</sup>Universal Declaration of Human Rights, 1948, Article 12



Civil and Political Rights, 1966<sup>1</sup>, which establish legal safeguards against "arbitrary interference" with an individual's privacy, family, home, correspondence, dignity, and reputation. The Indian approach to privacy rights draws from international human rights law while adapting to domestic constitutional requirements. The Supreme Court stated that constitutional provisions must be read and interpreted in a manner which would enhance their conformity with international human rights instruments ratified by India.

#### **Comparative Constitutional Approaches**

- **United States:** The U.S. Constitution's Fourth Amendment provides explicit protection against unreasonable searches and seizures, while substantive due process has been interpreted to protect various privacy rights.
- **European Union:** The EU has developed a comprehensive framework through the General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights, providing strong privacy protections.
- **Canada:** Canadian privacy law is derived from the common law, statutes of the Parliament of Canada and the various provincial legislatures, and the Canadian Charter of Rights and Freedoms.

## **7. Conclusion**

The constitutional recognition of privacy as a fundamental right in India through the Puttaswamy judgment represents a landmark achievement in constitutional jurisprudence. This judgment settled the position of law and clarified that the Right to Privacy could be infringed only when there was a compelling state interest for doing so, placing it on the same footing as other fundamental rights. The journey from the restrictive interpretations in *M.P. Sharma* and *Kharak Singh* to the comprehensive recognition in *Puttaswamy* demonstrates the Constitution's capacity for evolutionary interpretation while maintaining its core commitment to human dignity and freedom. The recognition acknowledges that in an interconnected digital world, privacy protection is not merely a luxury but a necessity for preserving individual autonomy and democratic values. The right to privacy is fundamental for safeguarding individual autonomy, dignity, and freedom. Recognised in the *Puttaswamy* Judgment, it ensures

protection from surveillance, enables free expression, and secures personal data, strengthening democratic values.

As India continues to develop its privacy protection framework through legislation like the Digital Personal Data Protection Act, 2023, the constitutional foundation established by *Puttaswamy* provides a robust basis for protecting individual rights while enabling legitimate state functions. The challenge ahead lies in translating constitutional principles into effective legal and technological safeguards that can adapt to evolving technological landscapes while maintaining the fundamental commitment to human dignity and individual freedom. The recognition of privacy as a fundamental right thus represents not an end but a beginning – the beginning of a new era in constitutional governance where individual autonomy and dignity are accorded their rightful place in the digital age. The success of this constitutional evolution will depend on continued vigilance by the judiciary, proactive legislation by Parliament, effective enforcement by regulatory bodies, and active participation by civil society in ensuring that the promise of privacy protection is realized for all citizens.

---

<sup>1</sup>International Covenant on Civil and Political Rights, 1966, Article 17