

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 6

2025

© 2025 International Journal of Legal Science and Innovation

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in the International Journal of Legal Science and Innovation after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Legal Science and Innovation, kindly email your Manuscript to submission@ijlsi.com.

The Constitutional Conundrum of Privacy: Balancing Human Dignity, State Sovereignty, and Biometric Surveillance in India

NIKET*

ABSTRACT

This paper explores the evolution of the right to privacy in India, evaluating its intricate relationship with human dignity and state sovereignty. By tracing the judicial shift from structural positivism to transformative constitutionalism, the study maps the trajectory from the early reluctance in M.P. Sharma and Kharak Singh to the landmark proclamation in K.S. Puttaswamy. It then examines the contemporary challenges posed by biometric technology and digital data collection, analysing how the Digital Personal Data Protection (DPDP) Act seeks to balance legitimate state interests with individual autonomy.

Keywords: *Right to Privacy, Article 21, Biometrics, Constitutional Law, Puttaswamy Judgment, DPDP Act*

I. INTRODUCTION: THE ONTOLOGICAL INTERSECTION OF PRIVACY AND HUMAN DIGNITY

The concept of privacy is not a modern political luxury; it is the fundamental core of human existence. At its heart, privacy is the control that an individual exercises over their own body, thoughts and personal information. To be human is to possess an inherent space that is sacred, inviolable and free from the uninvited gaze of the outside world. When this space is protected, human dignity thrives. Conversely, when this space is systematically dissolved, individual liberty ceases to exist.

In the contemporary digital landscape, the traditional boundaries of privacy have been completely rewritten. The historical conception of privacy, which was largely confined to the physical protection of one's home against unlawful entry, has evolved into an urgent struggle for informational self-determination. Today, our identities are no longer merely physical; they are digital, comprising biometrics, algorithms and data trails. Protecting privacy is therefore no longer merely a matter of protecting property; it is a matter of defending the very essence of human dignity against psychological and systemic subjugation.

* Author is a Student at Vaish College of Law (Maharshi Dayanand University), Rohtak, Haryana, India.

II. THE THEORETICAL DIVIDE: NATURAL RIGHTS VERSUS POSITIVE LAW

To understand the legal standing of privacy, one must examine the classical tension between natural law and legal positivism.

A. The natural law perspective

Under the doctrine of natural law, certain rights are inherent to human nature and vest by virtue of birth itself. Philosophers such as John Locke argued that individuals possess fundamental rights to life, liberty and estate that exist prior to the formation of any government or social contract.¹ In this light, privacy is a natural right. It is not a privilege granted by a sovereign ruler, nor is it a benefit written into a statute book. The State does not create privacy; the State merely recognises it. Consequently, no government possesses the moral or legitimate authority to strip a citizen of privacy entirely, since doing so would be an assault on the citizen's natural humanity.

B. The positivist challenge

In sharp contrast, legal positivism, championed by jurists such as John Austin and Jeremy Bentham, posits that rights are real only if they are explicitly recognised by the written law of the State (*positus*). From this strict viewpoint, unless a right is clearly codified within a constitution or a statute, it remains a mere moral aspiration rather than an enforceable legal reality. For decades, the Indian legal system operated under the heavy shadow of this positivist approach, frequently questioning whether a right to privacy could truly exist when the text of the Indian Constitution did not explicitly mention the word "privacy".

III. THE STATE, THE SOCIAL CONTRACT, AND THE PURPOSE OF GOVERNMENT

The justification for state intervention in the private lives of citizens is historically rooted in the theory of the social contract. As articulated by Thomas Hobbes, in the hypothetical "state of nature" life was solitary, poor, nasty, brutish and short, because there was no central authority to maintain order.² To escape this chaos, individuals surrendered a portion of their absolute freedom to a sovereign ruler in exchange for collective security, stability and protection against fraud and violence.

In the modern context, this contract justifies the State's use of technology and data collection. The government requires information to govern effectively, prevent economic fraud, maintain public order and ensure that social welfare schemes reach the poorest citizens without leakages.

¹ JOHN LOCKE, TWO TREATISES OF GOVERNMENT bk. II, ch. VII, § 87 (1689).

² THOMAS HOBBS, LEVIATHAN ch. XIII (1651).

Biometric identification systems, such as fingerprinting and iris scanning, serve as powerful tools for fulfilling this state obligation.

However, a critical constitutional danger arises when the State oversteps its role as a protective trustee and transforms into an all-powerful observer. If the government uses the social contract as a licence to establish perpetual, round-the-clock surveillance over its population, the contract is broken. A citizen living under constant, unregulated surveillance can never truly be free; the psychological pressure of being perpetually watched inevitably breeds fear, crushes dissent and destroys the joy of a dignified life. The ultimate purpose of government must therefore be a delicate act of balance: using data to secure the population without reducing the citizen to a transparent object of state control.

IV. THE PRE-PUTTASWAMY ERA: JUDICIAL RELUCTANCE AND HISTORICAL EVOLUTION

The path toward recognising privacy in India was paved with deep judicial hesitation. For over sixty years, the Supreme Court of India adopted a literal and restrictive reading of fundamental rights, consistently refusing to recognise an independent right to privacy.

A. *M.P. Sharma v. Satish Chandra* (1954)

The question of constitutional privacy first arose before an eight-judge bench of the Supreme Court in *M.P. Sharma v. Satish Chandra*.³ The case involved a challenge to the legality of search and seizure operations conducted against a company suspected of financial fraud. The petitioners argued that such intrusive searches violated their fundamental rights.

The Supreme Court, heavily influenced by strict textual positivism, rejected the argument outright. The Court noted that the makers of the Indian Constitution had deliberately chosen not to include a provision analogous to the Fourth Amendment to the United States Constitution, which explicitly protects citizens against unreasonable searches and seizures.⁴ The Bench ruled that an independent right to privacy could not be read into the Constitution through a strained process of interpretation, thereby setting a rigid precedent that left citizens vulnerable to state overreach for decades.

B. *Kharak Singh v. State of U.P.* (1962)

The structural conflict between police power and personal liberty came to a head in the historic case of *Kharak Singh v. State of U.P.*⁵ The petitioner, Kharak Singh, had been charged in a

³ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

⁴ *M.P. Sharma*, *supra* note 3; U.S. CONST. amend. IV.

⁵ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).

dacoity case but was released for want of evidence. However, under Regulation 236 of the Uttar Pradesh Police Regulations, the police opened a history sheet against him and subjected him to intense surveillance. Police officers conducted “domiciliary visits”, which involved entering his home late at night, waking him up and constantly monitoring his movements.

The six-judge bench delivered a fractured judgment that perfectly captured the judicial tension of the era.

The majority view. The majority struck down Regulation 236(b), which authorised night-time domiciliary visits, as unconstitutional, invoking the common law maxim that every man’s house is his castle and holding that such unauthorised intrusion violated the personal liberty guaranteed by Article 21. The majority did not, however, accept that the remaining surveillance measures infringed the freedom of movement under Article 19(1)(d), and it explicitly reiterated the stance taken in *M.P. Sharma*, stating that the right to privacy is not a guaranteed right under the Constitution.⁶

The revolutionary dissent of Justice Subba Rao. In a brilliant flash of constitutional foresight, Justice Subba Rao wrote a dissenting opinion that would later become the foundational philosophy of modern Indian jurisprudence. He argued that the right to personal liberty under Article 21 is not merely the right to be free from physical confinement but a comprehensive right to live with dignity. Justice Subba Rao famously observed that “the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty.”⁷

C. The transition phase: incremental recognition

Following the strict interpretations in *M.P. Sharma* and *Kharak Singh*, the Indian judiciary did not remain static. Over the subsequent decades, the Supreme Court began to recognise that “personal liberty” under Article 21 would be rendered illusory without protection of the private domain of citizens.

In *Gobind v. State of Madhya Pradesh* (1975), the Court took a significant step forward.⁸ While it did not declare privacy an absolute right, it acknowledged for the first time that a limited right

⁶ *Kharak Singh*, *supra* note 5 (Ayyangar, J., for the majority); INDIA CONST. arts. 19(1)(d), 21.

⁷ *Kharak Singh*, *supra* note 5 (Subba Rao, J., dissenting).

⁸ *Gobind v. State of Madhya Pradesh*, AIR 1975 SC 1378 (India).

to privacy emanates from the penumbras of Articles 19 and 21. Justice Mathew noted that any state intrusion into privacy must be justified by a compelling state interest.

This judicial evolution was further strengthened in *R. Rajagopal v. State of Tamil Nadu* (1994), where the Court explicitly linked privacy to the “right to be let alone” in personal matters such as family, marriage and motherhood.⁹ Finally, in *PUCL v. Union of India* (1997), a case dealing with unauthorised telephone tapping, the Court ruled that telephone conversations are an integral part of private life, thereby establishing that technological surveillance by the State must follow a fair procedure established by law.¹⁰

V. THE PUTTASWAMY REVOLUTION: PRIVACY AS A CONSTITUTIONAL CORE

The turning point in India’s constitutional history came on 24 August 2017, when a nine-judge constitution bench of the Supreme Court delivered its unanimous verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹¹ This landmark ruling completely restructured the jurisprudence of rights in the digital age.

A. Overruling textual positivism

The Court expressly overruled the majority decisions in *M.P. Sharma* and *Kharak Singh* to the extent that they held that privacy is not protected by the Constitution.¹² It rejected the outdated positivist view that a right must be explicitly written in the constitutional text in order to exist. The Bench declared that privacy is an unwritten but inherent natural right that forms the foundational bedrock of all the explicit fundamental freedoms.

B. The triple test of proportionality

The *Puttaswamy* judgment recognised that the right to privacy is not absolute and can be restricted by the State. However, to ensure that the government does not use national security or administrative convenience as a blanket excuse for mass surveillance, the Court laid down a strict three-pronged test.¹³ Any state action infringing privacy must satisfy three cumulative conditions:

Legality. There must be an explicit, written law passed by the legislature authorising the state action. Administrative orders or executive whims are insufficient.

⁹ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

¹⁰ *People’s Union for Civil Liberties v. Union of India*, AIR 1997 SC 568 (India).

¹¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

¹² *Puttaswamy*, *supra* note 11.

¹³ *Puttaswamy*, *supra* note 11 (Chandrachud, J.).

Legitimate aim. The restriction must serve a valid and necessary state purpose, such as safeguarding national security, preventing public disorder or ensuring the equitable distribution of social welfare benefits.

Proportionality. The means adopted by the State must be proportionate to the objective sought to be achieved. The State cannot use an excessively intrusive method if a less intrusive alternative is available to achieve the same result.

VI. CONTEMPORARY DIGITAL CHALLENGES: BIOMETRICS, SURVEILLANCE, AND THE DPDP ACT

In the modern legal framework, the constitutional principles laid down in *Puttaswamy* face their greatest test from rapid advances in biometric technology, facial recognition systems and algorithmic tracking. Today, surveillance has shifted from physical policing to invisible, persistent data collection.

A. The biometric dilemma

Biometric data, such as fingerprints, iris scans and facial templates, presents a unique legal dilemma. On the one hand, as discussed under the modern social contract, the collection of biometric data is highly effective for preventing financial fraud, securing identity verification and eliminating corruption in welfare schemes. On the other hand, unlike a password, biometric data cannot be changed once leaked. The perpetual collection of such data creates a profound psychological risk of mass surveillance. When citizens know they are under constant digital observation, their behaviour is fundamentally altered, free thought is stifled and human dignity is eroded.

B. The Digital Personal Data Protection (DPDP) Act: a regulatory framework

To bridge the gap between technological advancement and constitutional mandates, India enacted the Digital Personal Data Protection Act, 2023.¹⁴ The Act introduces critical legal concepts to safeguard informational privacy.

The principle of consent. The Act shifts the power dynamic back to the citizen, designated as the “Data Principal”. The State or a private entity (the “Data Fiduciary”) may process personal data on the basis of consent only where that consent is free, specific, informed, unconditional and unambiguous, given for a specified purpose, and it remains revocable at any time.¹⁵

¹⁴ The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

¹⁵ *Id.* § 6.

Purpose limitation and data minimisation. Entities cannot collect more data than is necessary for the specified purpose, nor can they retain it indefinitely once that purpose has been served.¹⁶

Accountability and penalties. The framework establishes severe financial penalties for data breaches, compelling both corporate and state actors to maintain robust security infrastructures.¹⁷

VII. CONCLUSION AND THE WAY FORWARD

The journey of the right to privacy in India reflects a transition from rigid legal positivism to a vibrant, dignity-centric constitutionalism. From the total denial in *M.P. Sharma* to the comprehensive framework of the *Puttaswamy* judgment and the DPDP Act, the law has evolved to protect the individual in an increasingly transparent digital world.

The ultimate solution lies neither in rejecting technology nor in surrendering individual autonomy to state sovereignty. The way forward requires strict judicial and legislative oversight to ensure that data collection remains a tool of governance rather than an instrument of control. Biometric systems must be securely ring-fenced with state-of-the-art encryption, and independent regulatory authorities must actively penalise breaches. Only when the State respects the boundary between administrative necessity and personal dignity can India truly fulfil its constitutional promise of a free, democratic and dignified society.

¹⁶ *Id.* §§ 6(1), 8(7).

¹⁷ *Id.* § 33 & sched.