

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.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 Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities 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 Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Right to Privacy against Mass Surveillance in Digital India: From Constitutional Silence to Fundamental Right and Beyond

KHUSHI GARG*

ABSTRACT

This paper examines the relationship between constitutional silence and the right to privacy in India, tracing the development of privacy from an unenumerated entitlement to a recognised fundamental right. Constitutional silence denotes the absence of express provisions in a constitution, leaving space for judicial interpretation and the recognition of implied rights. In India, the right to privacy evolved from such silence into a fundamental right, principally through landmark judicial pronouncements, most notably Justice K.S. Puttaswamy (Retd.) v. Union of India, which affirmed privacy as an integral component of the right to life under Article 21. The dynamism of digital technology has, however, transformed the character of state surveillance and tested privacy protection in novel ways. This paper analyses India's constitutional and legal framework for privacy protection, particularly against the backdrop of surveillance legislation such as the Indian Telegraph Act, 1885, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. It raises concerns regarding proportionality, oversight, and accountability, and argues that India's surveillance regime must be brought into conformity with constitutional norms and international best practices in order to protect individual autonomy and dignity.

Keywords: Right to privacy, Mass surveillance, Constitutional silence, Puttaswamy, Digital Personal Data Protection Act, Proportionality, Article 21.

I. INTRODUCTION

The concepts of constitutional silence and the right to privacy are intertwined in the discourse of fundamental rights and freedoms. Constitutional silence refers to the absence of explicit provisions in a constitution regarding certain rights, a feature that can give rise to interpretative challenges and judicial innovation. The right to privacy is recognised as a fundamental human right essential to individual autonomy and dignity, even though it is not explicitly stated in most constitutions.¹ Through judicial intervention, the right to privacy in India has developed from a

* Author is an Advocate in India.

¹ M.P. Singh, *Constitutional Silence and Judicial Activism: Fundamental Rights, Constitutional Morality and the Transformative Constitution of India*, 10(1) INDIAN J. CONST. L. 1 (2019).

matter of constitutional silence into a recognised fundamental right.² The path towards comprehensive privacy protection nevertheless remains incomplete, requiring sustained legislative implementation and continual adaptation to technological advancement. Constant effort is required to ensure that privacy rights are effectively protected and preserved in the light of emerging digital challenges.

II. OVERVIEW OF DIGITAL TECHNOLOGIES AND THE RISE OF SURVEILLANCE

Surveillance has evolved over time, moving from occasional, physical monitoring to ubiquitous, technologically advanced systems capable of gathering vast quantities of data. Contemporary technologies such as facial recognition, artificial intelligence, and automated interception systems (including NATGRID and India's Central Monitoring System) make unprecedented governmental oversight possible. Such measures carry the potential to erode democratic freedoms and privacy rights, even when justified on grounds of national security.³ Recent incidents, such as the Pegasus spyware controversy⁴ and alleged unlawful telephone-tapping cases,⁵ illustrate the misuse of surveillance powers. The absence of robust safeguards aggravates these risks, necessitating a re-evaluation of India's legal framework in the light of the *Puttaswamy* judgment.

III. EVOLUTION OF PRIVACY AS A FUNDAMENTAL RIGHT IN INDIA

Following decades of litigation, the right to privacy was enshrined as a constitutional right in India through the historic judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The development of this right can be traced through a chain of judicial pronouncements indicative of evolving understandings over time. At the outset, privacy was acknowledged without being categorically accorded fundamental status.⁶

The framers of the Indian Constitution did not envisage the right to privacy as a condition precedent to the exercise of search and seizure powers, as held in *M.P. Sharma v. Satish*

² *Id.*.

³ Pranesh Prakash, *How Surveillance Works in India*, India Ink (July 10, 2013), <https://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/>; *Govt to Launch Internet Spy System "Netra" Soon*, TIMES OF INDIA (Jan. 6, 2014), <https://timesofindia.indiatimes.com/tech-news/govt-to-launch-internet-spy-system-netra-soon/articleshow/28456222.cms>; see also Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No. 3493 (Lok Sabha, Aug. 11, 2015), <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015-pdfs/ls-110815/3493.pdf>.

⁴ *India Targets Apple Over Its Phone Hacking Notifications*, WASHINGTON POST (Dec. 28, 2023).

⁵ TOI City Desk, *Case Filed Against Kerala MLA P.V. Anvar for Allegedly Tapping Senior Officials' Phones*, TIMES OF INDIA (Sept. 29, 2024), <https://timesofindia.indiatimes.com/city/kochi/case-filed-against-kerala-mla-pv-anvar-for-allegedly-tapping-senior-officials-phones/articleshow/113783040.cms>; *Phones of Indian Politicians, Journalists Hacked Using Pegasus: 10 Facts on Report*, NDTV.

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

Chandra. That judgment did not address the question whether privacy could be safeguarded under other fundamental rights, such as the right to life and personal liberty.⁷

A six-judge bench later held, in *Kharak Singh v. State of Uttar Pradesh*, that the right to privacy was not a fundamental right. The Court nevertheless disapproved of police domiciliary visits at midnight as an unjustified intrusion upon individual freedom, a position that revealed a cautious leaning towards a broader interpretation of Article 21.⁸ The Supreme Court's decision in *Maneka Gandhi v. Union of India* furthered this view by holding that legal procedures must be reasonable, fair, and just.⁹

The Court further affirmed the right to privacy in *State of Maharashtra v. Madhukar Narain*, holding that women engaged in sex work were entitled to privacy and dignity.¹⁰ According to the Supreme Court's formulation in *R. Rajagopal v. State of Tamil Nadu*, the right to privacy is implicit in Article 21 and amounts to the right to be let alone.¹¹ As reaffirmed in *Mr. X v. Hospital Z*, however, the Court made clear that this right was not unqualified and could be restricted for reasons such as the maintenance of public order, the prevention of crime, and the protection of the rights of others.¹²

PUCL v. Union of India, otherwise known as the Phone Tapping Case, emphasised that illegal telephone tapping constitutes a serious breach of personal rights, thereby reinforcing the importance of privacy.¹³ In *Selvi v. State of Karnataka*, the Supreme Court declared that, in the absence of public-safety considerations, involuntary narco-analysis, polygraph tests, and brain-mapping infringe an individual's right to privacy.¹⁴

In *Ram Jethmalani v. Union of India*, the Court emphasised that privacy is central to the right to life, observing that human beings require spheres free from unwanted public gaze, except where their conduct is criminal.¹⁵

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge bench finally overruled the earlier decisions in *M.P. Sharma* and *Kharak Singh* and clearly enshrined the right to privacy as a fundamental right under Article 21.¹⁶ While the Court referred a number of questions

⁷ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

⁸ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).

⁹ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

¹⁰ *State of Maharashtra v. Madhukar Narain*, (1991) 1 SCC 57 (India).

¹¹ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

¹² *Mr. X v. Hospital Z*, (1998) 8 SCC 296 (India).

¹³ *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).

¹⁴ *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).

¹⁵ *Ram Jethmalani v. Union of India*, (2011) 8 SCC 1 (India).

¹⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

concerning possible privacy violations to a narrower bench, this historic judgment arose from cases questioning the constitutionality of Aadhaar's collection of biometric data. The Aadhaar litigation is an important chapter in the history of India's Constitution, having generated controversy over mass surveillance, consent, conditional welfare, and potential privacy violations.

IV. LEGAL FRAMEWORK OF SURVEILLANCE IN INDIA

The constitutional basis of state interception lies in Section 5(2) of the Indian Telegraph Act, 1885, which permits interception in the event of a public emergency or in the interest of public safety. In order to forestall abuse of this power, the landmark decision in *PUCL v. Union of India* established a number of procedural checks and balances, including the requirement of written interception orders issued by the Home Secretary, a validity period of sixty days (extendable to one hundred and eighty days), and oversight by a Review Committee comprising high-ranking government functionaries. These safeguards have nevertheless been criticised for serious shortcomings. In the absence of any pre-interception judicial clearance, executive officers alone are empowered to issue interception orders without independent review, creating scope for abuse.¹⁷

The Indian legal foundation of state surveillance is thus rooted in Section 5(2) of the Indian Telegraph Act, 1885, which provides for interception in cases of public emergency or in the interest of national security. The *PUCL* case introduced procedural safeguards in the form of written interception orders, a sixty-day (extendable to one hundred and eighty days) validity period, and supervision by a Review Committee. These safeguards have been criticised, however, for lacking judicial sanction, leaving interception orders in the hands of the executive alone.¹⁸ Sections 69 and 69B of the Information Technology Act, 2000, advance the government's surveillance powers further by permitting the interception, monitoring, and decryption of electronic communications on ambiguous grounds such as public order, a lower threshold than public emergency.¹⁹ Although the 2009 Rules under the Information Technology Act impose some restrictions, they fail to ensure transparency or accountability. This framework suffers from three major flaws: first, excessive executive discretion without judicial oversight; second, vague terms such as public order that enable abuse; and third, the absence of independent citizen redress mechanisms. Evaluated under the *Puttaswamy* proportionality test,

¹⁷ See Usha Ramanathan, *Surveillance and the Right to Privacy*, in *The Social and Political Foundations of Constitutions* 305 (Kalpana Kannabiran ed., 2013).

¹⁸ *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).

¹⁹ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 69, 69B (India).

these flaws raise serious constitutional concerns about privacy rights and the legality of unchecked state surveillance.²⁰

Sections 7, 17, and 36 of the Digital Personal Data Protection Act, 2023, grant broad exemptions to government agencies, permitting the processing of personal data without the consent of the individual in the context of public order, national security, or other ill-defined state interests.²¹ Absent the robust safeguards required by the Supreme Court's *Puttaswamy* judgment, these provisions effectively legalise the indiscriminate collection of information by the state. Two inherent flaws are particularly pertinent. First, *Puttaswamy*'s requirement of institutional checks and balances is not met, since there is no process of judicial review, with the result that executive surveillance powers are exercised unilaterally. Second, serious concern arises from the Act's failure to define significant phrases such as national security in a clear manner, which may facilitate disproportionate or arbitrary state action.

The principles of proportionality and legality articulated in *Puttaswamy* are likewise breached by Sections 91 and 92 of the Code of Criminal Procedure, 1973, and by police manuals that permit unlimited data collection and suspicion-based profiling without court oversight or privacy safeguards. These provisions confer excessive surveillance power upon the government without providing the protection required to guard against deliberate invasion of citizens' privacy.²²

V. TESTING SURVEILLANCE PROGRAMMES AGAINST PUTTASWAMY

In a unanimous ruling, the nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* held that privacy is an integral component of a person's right to life and liberty under Article 21 of the Constitution. The decision represented the culmination of a revolutionary evolution of the right to privacy in India.²³ The judgment established a strict four-pronged test, comprising legality, legitimate purpose, proportionality, and procedural safeguards, by which any state action intruding upon privacy is to be assessed. In the context of mass surveillance, this framework requires any intrusion to be authorised by law, to pursue a legitimate state interest, to be necessary and proportionate to the interest sought, and to be supported by robust procedural safeguards against abuse. India's existing surveillance regime, governed by statutes such as the Indian Telegraph Act, 1885,²⁴ the Information Technology Act,

²⁰ The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).

²¹ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, §§ 7, 17, 36 (India).

²² The Code of Criminal Procedure, 1973, No. 2, Acts of Parliament, 1974, §§ 91, 92 (India).

²³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

²⁴ The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).

2000,²⁵ and the recently enacted Digital Personal Data Protection Act, 2023, falls short of these constitutional standards, giving rise to grave fears of executive abuse and the erosion of civil liberties.²⁶

The *Puttaswamy* judgment reaffirmed a democratic principle: any restriction of privacy must originate from legislation that is specific, clear, and readily comprehensible to the public. The Court rightly cautioned that imprecise legislation produces a chilling effect, as individuals are left uncertain about the circumstances in which their personal liberties may be curtailed.²⁷ This principle is especially crucial for surveillance law, which must delineate the limits of state power in clear terms. Although existing legislation such as the Telegraph Act and the Information Technology Act permit surveillance, their imprecise terminology, such as public emergency or national security, affords excessive latitude to government agencies. These vague provisions cannot satisfy *Puttaswamy*'s requirement of clarity in law, thereby permitting unrestrained executive discretion over the communications of private citizens. In the absence of clear statutory definitions separating genuine security concerns from ordinary events, such legislation risks becoming an instrument of arbitrary invasion of privacy rather than a finely calibrated tool of public safety. The judgment is a reminder that, in a rights-based democratic order, the law of state surveillance must be as clear and comprehensible as the rights it may limit or restrict.²⁸

Section 5(2) of the Telegraph Act renders the interception of communications lawful in vaguely defined situations of public emergency or public safety, terms whose deliberate indeterminacy renders them open to broad bureaucratic construction.²⁹ Similarly, Section 69 of the Information Technology Act renders cyber surveillance lawful on comparably amorphous grounds such as the preservation of public order or the prevention of vaguely defined incitement, without prescribing precise criteria for such invasive activities.³⁰ The Digital Personal Data Protection Act compounds these problems by introducing blanket exceptions permitting government access to data without consent under loosely articulated categories such as national security, thereby institutionalising unrestricted surveillance power. This legislative vagueness directly offends the constitutional warning contained in *Puttaswamy*, which cautioned against enacting legislation that creates a chilling effect through undefined exceptions to privacy rights. Despite this explicit constitutional warning, India's surveillance regime continues to retain these

²⁵ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁶ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

²⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

²⁸ *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).

²⁹ The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885, § 5(2) (India).

³⁰ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69 (India).

dangerously vague provisions, systematically exposing citizens to potential state excess without sufficient protection or definitional check upon executive discretion.³¹

The *Puttaswamy* judgment established proportionality as the general test for determining privacy violations, requiring government measures to be suitably calibrated, minimally intrusive, and carefully weighed against fundamental rights.³² This test is exacting for blanket surveillance systems such as India's Central Monitoring System, which violate proportionality by indiscriminately collecting vast quantities of data encompassing both innocent persons and suspected threats. Blanket surveillance cannot satisfy any of the three prongs of the proportionality test: it lacks focused targeting (rational connection), harvests disproportionate and unnecessary information (minimal impairment), and produces privacy violations that are disproportionate to the alleged security benefits.³³ The Court categorically disapproved of such blanket approaches, reaffirming the view of the United Nations that mass surveillance dangerously transforms the relationship between citizen and state into one of mutual observation and suspicion.

The Digital Personal Data Protection Act compounds these concerns by permitting government access to highly sensitive personal data, ranging from fingerprints to medical history to political opinions, without requiring officials to demonstrate why narrower measures would not suffice. This directly contravenes *Puttaswamy*'s least-restrictive-means requirement and revives the practice of general warrants against which the Court warned, whereby broad surveillance powers are routinely approved without case-specific justification. The Pegasus revelations tragically illustrated these dangers, showing how unchecked surveillance tools may target critics and activists, chilling free expression and democratic participation. Where interception orders require only bureaucratic approval rather than judicial scrutiny, and where laws permit access to intimate personal data without any demonstration of necessity, the result is a surveillance apparatus that fundamentally contradicts India's constitutional vision of privacy as a safeguard for democratic freedoms.³⁴

Equally troubling is India's failure to implement the procedural safeguards mandated by *Puttaswamy*. The existing surveillance systems contain no such protections in the form of judicial warrants or independent monitoring, with interception orders sanctioned by bureaucrats rather than by courts. The Digital Personal Data Protection Act adds to this lack of

³¹ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

³² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

³³ *Id.*.

³⁴ Report of the Committee of Inquiry under Justice R.V. Raveendran 45-48 (2022); Amnesty International, Technical Findings on Pegasus Spyware (2021).

accountability by establishing a state-run Data Protection Board in place of an independent monitor. Transparency fares no better, as authorities habitually decline to provide even rudimentary statistics on surveillance operations and disclose nothing to those who are surveilled.³⁵ This opacity undermines the ability of citizens to challenge intrusions into their privacy, in violation of *Puttaswamy*'s categorical insistence that privacy rights cannot be subject to executive whim. When surveillance systems operate beyond judicial oversight, independent audit, or public scrutiny, they shift from protective to potentially repressive instruments, an eventuality that the protections enshrined in *Puttaswamy* were intended to preclude. The persistent gap between these constitutional aspirations and the present reality of surveillance in India underscores the need for sweeping reform.³⁶

VI. CONCLUSION AND SUGGESTIONS

India's surveillance regime stands at a critical juncture and requires immediate reform to meet the constitutional right to privacy as enshrined in the *Puttaswamy* judgment. The current legal framework, with its vague concepts such as national security and its overbroad executive authority, fails to satisfy the Supreme Court's tests of necessity, proportionality, and accountability. To address these deficiencies, the adoption of three structural reforms is imperative.³⁷

First, parliamentary transparency must supplant the prevailing culture of secrecy. Clear definitions underpinning surveillance activities should be expressly enunciated to forestall abuse, and judicial warrant requirements for interception orders are essential to bring the era of unrestricted executive power to a close. Second, institutional safeguards should be consolidated through the establishment of an independent oversight body composed of judges, technologists, and civil-society specialists, supported by open reporting mechanisms that reveal surveillance patterns without compromising the integrity of legitimate security operations. Third, the legal framework for protective technology should be codified, including a comprehensive prohibition on encryption backdoors and adherence to strict data-minimisation practices, in order to keep state power within constitutional bounds.³⁸

³⁵ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 19(1) (India).

³⁶ UN Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).

³⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

³⁸ See Vrinda Bhandari, Smriti Parsheera & Faiza Rahman, *Reforming the Surveillance Framework in India*, Nat'l L. Sch. India Rev. (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3913662; see also Internet Freedom Foundation, *Modernising Surveillance Oversight in India: The Need for Legislative Reform* (2021), <https://internetfreedom.in/surveillance-reform-paper/>.

VII. BIBLIOGRAPHY

1. The Code of Criminal Procedure, 1973, No. 2, Acts of Parliament, 1974 (India).
2. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
3. The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
4. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
5. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).
6. UN Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).
7. Report of the Committee of Inquiry under Justice R.V. Raveendran 45-48 (2022).
8. Amnesty International, Technical Findings on Pegasus Spyware (2021).
9. *Delhi: 176 Violators Booked as AAP Government Turns to Phone Tracking to Check Movement of Those Under Home Quarantine*, FINANCIAL EXPRESS, <https://www.financialexpress.com/india-news/delhi-176-violators-booked-as-aap-government-turns-to-phone-tracking-to-check-movement-of-those-under-home-quarantine/1920086/>.
10. *Phones of Indian Politicians, Journalists Hacked Using Pegasus: 10 Facts on Report*, NDTV.
11. Pranesh Prakash, *How Surveillance Works in India*, India Ink (July 10, 2013), <https://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/>.
12. *Govt to Launch Internet Spy System "Netra" Soon*, TIMES OF INDIA (Jan. 6, 2014), <https://timesofindia.indiatimes.com/tech-news/govt-to-launch-internet-spy-system-netra-soon/articleshow/28456222.cms>.
13. TOI City Desk, *Case Filed Against Kerala MLA P.V. Anvar for Allegedly Tapping Senior Officials' Phones*, TIMES OF INDIA (Sept. 29, 2024), <https://timesofindia.indiatimes.com/city/kochi/case-filed-against-kerala-mla-pv-anvar-for-allegedly-tapping-senior-officials-phones/articleshow/113783040.cms>.
14. *India Targets Apple Over Its Phone Hacking Notifications*, WASHINGTON POST (Dec. 28, 2023).