

Right to Privacy vs State Surveillance in the Digital Age: A Constitutional Analysis of India

Sayali Dangare

Chhatrapati Shivaji Maharaj University Department of Law

Abstract- *The emergence of pervasive digital surveillance infrastructure has placed the constitutional right to privacy in direct and sustained tension with state security imperatives in India. This article examines that tension through a constitutional lens, tracing the doctrinal evolution of privacy as a fundamental right under Article 21 of the Constitution of India from Kharak Singh v. State of Uttar Pradesh (1963) to the landmark nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India (2017). Against this doctrinal backdrop, the article critically evaluates the surveillance powers conferred by the Information Technology Act, 2000, and the Indian Telegraph Act, 1885, applying the tripartite constitutional tests of legality, necessity, and proportionality. It argues that existing surveillance legislation fails these tests by conferring overbroad executive discretion without meaningful judicial or parliamentary oversight. The article further identifies structural challenges posed by artificial intelligence-driven surveillance, facial recognition technologies, and the nascent data-protection regime under the Digital Personal Data Protection Act, 2023. It concludes with targeted reform recommendations, including an independent surveillance oversight authority, sunset-clause legislation, and the operationalisation of a robust data-protection framework.*

Keywords: *Privacy; Surveillance; Article 21; Constitution of India; Data Protection; Proportionality*

I. INTRODUCTION

The digital revolution has fundamentally reconfigured the relationship between the individual and the state. Where mid-twentieth century surveillance required physical intrusion, contemporary states can harvest, aggregate, and analyse vast quantities of personal data without crossing a threshold. In India, this structural shift has created acute constitutional friction: Article 21 of the Constitution guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law, a guarantee the

Supreme Court has progressively expanded to shelter the right to privacy. Yet the same constitutional order authorises executive-controlled surveillance regimes that operate with minimal procedural constraint and limited judicial review.

This article addresses two central research questions. First, do India's primary surveillance statutes satisfy the constitutional requirements of legality, necessity, and proportionality as articulated in *Puttaswamy*?ⁱ Second, do the structural features of digital-age surveillance, including algorithmic decision-making and biometric identification, expose a regulatory lacuna that the current legislative framework is ill-equipped to address? The article proceeds by tracing the constitutional jurisprudence of privacy (Part II), mapping the statutory surveillance architecture (Part III), applying the constitutional tests (Part IV), identifying emergent digital challenges (Part V), and offering reform recommendations (Part VI).

II. EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

The constitutional status of privacy has undergone considerable transformation in India. In *Kharak Singh v. State of Uttar Pradesh*,ⁱⁱ the Supreme Court, in a divided opinion, held that domiciliary visits constituted an infringement of Article 21, yet refused to recognise a standalone fundamental right to privacy. The majority's restrictive approach reflected an originalist tendency to confine constitutional rights within the explicit text.

A decade later, in *Gobind v. State of Madhya Pradesh*,ⁱⁱⁱ a three-judge bench, relying on American penumbral reasoning, acknowledged that privacy "must itself be subject to the overriding public interest" but nonetheless treated it as an implicit constitutional value emanating from Articles 19 and 21. While doctrinal progress was modest, *Gobind*

planted the conceptual seed that privacy retained constitutional relevance even absent explicit textual recognition.

The decisive constitutional moment arrived with *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which a nine-judge bench of the Supreme Court unanimously declared privacy to be a fundamental right intrinsic to Articles 14, 19, and 21. The Court held that privacy is not merely an absence of intrusion but encompasses informational self-determination, the right to be forgotten, and the right to control personal data. Critically, the majority articulated a proportionality framework: any state limitation on privacy must be sanctioned by law, must be necessary for a legitimate state aim, and must be proportionate to that aim. These three limbs now constitute the operative constitutional standard against which surveillance laws must be assessed.

III. LEGAL FRAMEWORK OF STATE SURVEILLANCE

India's surveillance architecture is anchored principally in two statutes. The Information Technology Act, 2000,^{iv} under Section 69, empowers the Central and State Governments to issue directions for interception, monitoring, or decryption of digital information on grounds including sovereignty, security of the state, public order, or prevention of cognisable offences. Section 69B additionally authorises the government to monitor traffic data for cyber-security purposes. The procedural rules under Section 69 require written orders countersigned by senior officials but do not mandate prior judicial authorisation.

The Indian Telegraph Act, 1885,^v the colonial-era precursor to modern interception law, grants the government power under Section 5(2) to intercept messages in the interest of public safety or an emergency. Read together, these two statutes confer broad executive authority to conduct surveillance on digital and telephonic communications across the Indian population.

The procedural architecture of both statutes shares a common structural defect: oversight is internal to the executive branch.^{vi} While the Telegraph Rules require interception orders to be approved by a review committee, that committee is itself composed entirely of senior government officials.^{vii} No independent

judicial body exercises ex ante or ex post scrutiny of surveillance orders. This design stands in sharp contrast to comparative jurisdictions such as the United Kingdom, where the Investigatory Powers Tribunal provides independent adjudicatory review, and Germany, where Parliamentary oversight bodies exercise binding supervisory authority.

IV. CONSTITUTIONAL TENSIONS: PRIVACY VS. SURVEILLANCE

The *Puttaswamy* proportionality framework^{viii} requires that any limitation on the right to privacy satisfy three cumulative conditions. Applying each to India's surveillance statutes reveals serious constitutional infirmities.

As to legality, a law must be sufficiently clear, accessible, and foreseeable to enable citizens to regulate their conduct. Section 69 of the IT Act satisfies the formal criterion of being legislatively enacted; however, its grounds for interception, particularly "public order" and "friendly relations with foreign states," are drafted with a breadth that affords the executive near-unfettered discretion. The Supreme Court's observation in *People's Union for Civil Liberties* that statutory authority alone cannot redeem an unconstitutionally vague standard remains apposite.^{ix} Vague statutory standards fail the legality prong because citizens cannot foresee when the state may intercept their communications.

As to necessity, surveillance measures must be the least restrictive means available to achieve the legitimate aim. Neither the IT Act nor the Telegraph Act requires the state to demonstrate, before an independent body, that less intrusive alternatives were considered and found inadequate. The absence of such a requirement means that blanket surveillance programmes may be authorised without any comparative proportionality analysis, rendering the necessity enquiry a formal, rather than substantive, exercise.

As to proportionality *stricto sensu*, there must be a reasonable relationship between the benefit achieved and the rights infringed. Given the structural absence of judicial oversight, it is difficult to identify any ex ante or ex post mechanism through which such balancing is systematically performed. The executive order regime, unchecked by independent review, is incapable of ensuring proportionate outcomes across

individual cases. In *Anuradha Bhasin v. Union of India*, the Court confirmed that proportionality is judicially reviewable,^x yet meaningful review is frustrated where surveillance orders are neither published nor scrutinised by an independent authority.

V. CHALLENGES IN THE DIGITAL AGE

The transition from targeted wiretapping to algorithmic, population-scale surveillance introduces qualitatively new constitutional risks. Facial recognition systems deployed at public events and border crossings process biometric data in real time without individualised suspicion, enabling mass identification of persons exercising constitutionally protected rights of assembly and movement. Such technologies threaten to produce what the European Court of Human Rights has termed a "chilling effect": individuals modify lawful behaviour in anticipation of surveillance, thereby surrendering fundamental freedoms without any formal legal prohibition.

Big data analytics compound this concern. When disparate datasets, such as travel records, financial transactions, and social media activity, are aggregated and processed by machine learning models, the state acquires predictive intelligence about individual conduct that no single interception order could yield. The Committee of Experts on Non-Personal Data Governance acknowledged the potential for such aggregation to re-identify anonymised data,^{xi} yet India's current legal framework contains no prohibition on the aggregation of non-personal datasets for state intelligence purposes.

The Digital Personal Data Protection Act, 2023, represents a legislative attempt to establish data-subject rights, yet it exempts state processing for security and law enforcement purposes in terms broad enough to swallow the rule.^{xii} The Act does not establish a truly independent Data Protection Board, and its enforcement mechanisms remain untested. As Justice Chandrachud observed in *Puttaswamy*, informational self-determination, the right to control one's personal data, is an essential dimension of privacy;^{xiii} a data-protection regime that carves out state surveillance wholesale undermines this constitutional commitment at its core.

VI. CONCLUSION AND RECOMMENDATIONS

India's constitutional jurisprudence has advanced

considerably: privacy is now a fundamental right subject to rigorous proportionality scrutiny. The legislative architecture of surveillance, however, has not kept pace. The IT Act and the Telegraph Act vest the executive with broad interception authority, hedged only by internal administrative review, and thus fail the tests of legality, necessity, and proportionality established in *Puttaswamy*. The deployment of AI-driven surveillance technologies and the absence of robust data-protection enforcement sharpen these constitutional deficiencies.

Three targeted reforms are accordingly proposed. First, Parliament should establish an independent Surveillance Oversight Authority, modelled on the United Kingdom's Investigatory Powers Commissioner's Office, with statutory power to authorise, review, and annul surveillance orders. Such a body would supply the institutional mechanism through which proportionality is assessed case by case, resolving the current structural deficit identified above.

Second, surveillance legislation should incorporate sunset clauses and mandatory parliamentary reporting. Interception orders issued under Section 69 of the IT Act should expire after a specified period absent judicial renewal, and aggregate surveillance statistics should be reported annually to a parliamentary committee. This reform operationalises the legality requirement by ensuring that surveillance powers remain democratically accountable and time-limited.

Third, the exceptions for state processing under the Digital Personal Data Protection Act, 2023, should be brought within a necessity and proportionality framework, with the Data Protection Board granted jurisdiction to review state processing decisions on complaint. India may draw productively from the proportionality-anchored model of the General Data Protection Regulation,^{xiv} adapted to the constitutional architecture of Article 21. Together, these three reforms would align India's surveillance law with its constitutional commitments and with emerging global standards for the protection of privacy in the digital age.

REFERENCES

- [1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- [2] Kharak Singh v. State of Uttar Pradesh, AIR 1963

- SC 1295 (India).
- [3] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148 (India).
 - [4] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
 - [5] Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
 - [6] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).
 - [7] Telegraph Act 1885, s 5(2) (India).
 - [8] Puttaswamy (n 1) [301] (Chandrachud J): three-limb test of legality, necessity, and proportionality.
 - [9] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
 - [10] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); Personal Data Protection Bill, 2019 (India).
 - [11] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
 - [12] Report of the Committee of Experts on Non-Personal Data Governance Framework (Ministry of Electronics and Information Technology, 2020).
 - [13] Puttaswamy (n 1) [180] (Nariman J): informational self-determination and the right to control one's data.
 - [14] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

^{ix}People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India) (finding that telephone tapping engages Article 19(1)(a) and Article 21 rights).

^xAnuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India) (proportionality applied to internet shutdowns).

^{xi}Report of the Committee of Experts on Non-Personal Data Governance Framework (Ministry of Electronics and Information Technology, 2020).

^{xii}Personal Data Protection Bill, 2019 (India); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India). ^{xiii}Puttaswamy (n 1) [180] (Nariman J): the right to privacy includes informational self-determination and the right to control one's data. ^{xiv}General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

ⁱJustice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy].

ⁱⁱKharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).

ⁱⁱⁱGobind v. State of Madhya Pradesh, (1975) 2 SCC 148 (India).

^{iv}Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act].

^vIndian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India) [hereinafter Telegraph Act].

^{vi}IT Act, s. 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).

^{vii}Telegraph Act, s. 5(2).

^{viii}Puttaswamy (n 1) [301] (Chandrachud J): the three-limb test of legality, necessity, and proportionality.