

	ORIGINAL RESEARCH PAPER SURVEILLANCE AND THE CONSTITUTION: PROPORTIONALITY, PRIVACY AND THE LIMITS OF STATE INTERCEPTION IN INDIA	Law KEY WORDS: Privacy, State Surveillance, Interception, Article 21, Proportionality, Constitutional Law, India
Dr.Parul Pareek	Associate Advocate and Independent Legal Researcher, Formerly Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmangarh, Rajasthan, India	
ABSTRACT	State surveillance presents a constitutional problem because the same technologies that assist crime control and national security can also penetrate communications, associations and personal autonomy. Indian law now regulates interception through more than one statutory route. Section 5(2) of the Indian Telegraph Act, 1885 continues to operate, while section 69 of the Information Technology Act, 2000 governs specified electronic information. In parallel, section 20(2) of the Telecommunications Act, 2023 and the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 provide a newer framework for telecommunication messages. Against this background, the article examines the constitutional standards emerging from Justice K.S. Puttaswamy (Retd.) v. Union of India and subsequent proportionality jurisprudence. It argues that the principal difficulty is not the existence of surveillance power as such, but the institutional structure through which that power is exercised and reviewed. Executive authorisation, limited disclosure and executive review raise questions of necessity, safeguards and effective remedy. A constitutionally durable framework therefore requires clearer targeting standards, stronger independent oversight, meaningful retention controls and a practicable mechanism for post-surveillance accountability.	
INTRODUCTION	The State has a legitimate interest in preventing crime, protecting national security and responding to serious threats. In a constitutional order, however, the existence of a legitimate objective does not by itself validate the means adopted to pursue it. Surveillance is particularly intrusive because communications may disclose relationships, political or professional associations, movements and intimate choices. The constitutional question is therefore whether the legal framework sufficiently disciplines the exercise of surveillance power. The jurisprudence on privacy has changed substantially since the early constitutional cases. <i>M.P. Sharma v. Satish Chandra</i> and the majority decision in <i>Kharak Singh v. State of Uttar Pradesh</i> did not recognise a general constitutional right to privacy. Later decisions, including <i>Gobind v. State of Madhya Pradesh</i> and <i>R. Rajagopal v. State of Tamil Nadu</i>, moved towards recognising privacy within Articles 19 and 21. The nine-judge Bench in Justice <i>K.S. Puttaswamy (Retd.) v. Union of India</i> finally settled the matter by recognising privacy as a fundamental right connected with dignity, liberty and autonomy.	
OBJECTIVES AND METHOD	The study has four objectives: to trace the constitutional basis of privacy; to examine the statutory routes to interception; to assess the adequacy of oversight and safeguards; and to identify reforms compatible with national security and fundamental rights. The methodology is doctrinal. It relies on constitutional provisions, statutes, rules, reported Supreme Court decisions and selected comparative materials. No empirical claim is made about the volume or frequency of interception because such information is not comprehensively available in the public domain. The statutory position discussed here is stated as it stands on 24 September 2026.	
RESULTS Constitutional Standards	Puttaswamy established that privacy is constitutionally protected and that State interference must have a legal basis, pursue a legitimate State aim and satisfy proportionality. The Court's reasoning must be read with <i>Maneka Gandhi v. Union of India</i>, which requires procedure under Article 21 to be fair, just and reasonable. In the Aadhaar judgment, the Court articulated proportionality through the familiar sequence of legitimate purpose, rational connection, necessity and balancing. Later decisions have also emphasised the need for safeguards against abuse. Surveillance may additionally burden Article 19 freedoms. The Supreme Court in <i>People's Union for Civil Liberties v. Union of India</i> treated telephone tapping as a serious invasion of privacy and imposed procedural safeguards on interception. The constitutional significance of PUCI is not that it created an absolute prohibition on surveillance, but that intrusive State power must operate through defined legal procedures and accountability. Present Statutory Framework Section 5(2) of the Indian Telegraph Act, 1885 permits interception on the occurrence of a public emergency or in the interest of public safety, subject to specified grounds and statutory conditions. Section 69 of the Information Technology Act, 2000 provides a separate power concerning interception, monitoring or decryption of information, supplemented by the 2009 Rules. The Telecommunications Act, 2023 introduced another route. Section 20(2), brought into force on 26 June 2024, permits interception or disclosure of messages, subject to prescribed procedure and safeguards, on specified grounds and for recorded reasons. The 2024 Interception Rules place ordinary authorisation with the Union Home Secretary or the State Home Department Secretary, while allowing specified exceptional authorisation in unavoidable circumstances and operational situations. Rule 5 establishes review committees composed of senior executive officials, with periodic review and power to set aside non-compliant orders. The 2025 amendment altered certain procedural details, including the competent-authority provision for certain inter-State requests. The legal position requires an important qualification. Section 60 of the Telecommunications Act, which provides for repeal of the Indian Telegraph Act, has not been included in the commencement notifications identified above. The statutory architecture is therefore presently transitional and plural rather than a simple replacement of the 1885 law by the 2023 Act. Oversight and Remedy The principal constitutional concern is institutional rather than merely textual. The current interception regimes rely substantially on executive decision-making. The 2024 Telecom Rules provide for review by committees composed of senior executive officers. Such review is a safeguard, but it is not equivalent to prior scrutiny by a judicial or genuinely independent authority. Nor does the framework establish a	

general statutory right of delayed notice to the subject of surveillance once secrecy ceases to be necessary. The absence of a practical route to learn of surveillance can correspondingly limit the opportunity to challenge unlawful or excessive interception.

The Digital Personal Data Protection Act, 2023 should not be presented as an already-operative answer to this problem. Under the commencement notification of 13 November 2023, section 17, including its State-instrumentality exemptions, is scheduled to come into force eighteen months after publication. It therefore does not constitute the presently operative interception safeguard framework as of 24 September 2026.

DISCUSSION

The strongest constitutional objection to the existing architecture concerns proportionality at the level of safeguards. A power may have a legitimate aim and still be constitutionally defective if its operation is insufficiently constrained. *Gujarat Mazdoor Sabha v. State of Gujarat* emphasised that rights-infringing State action should contain safeguards against abuse. That principle is especially pertinent to secret surveillance, where the affected person cannot ordinarily contest the order when it is made.

A better framework need not prohibit surveillance. It should instead distinguish legitimate secrecy from unreviewable secrecy. First, interception should require a reasoned order identifying the person, account, device or narrowly defined class to be targeted and the statutory purpose relied upon. Second, prior authorisation should ordinarily be entrusted to a judicial officer or an independent statutory authority. Genuine emergencies may justify temporary executive action, but such action should be subject to prompt independent confirmation. Third, retention, dissemination and destruction of intercepted material should be governed by clear rules, with special protection for legally privileged or otherwise sensitive communications. Fourth, once disclosure would no longer prejudice a legitimate investigation, affected persons should have access to a delayed-notice and remedy mechanism, subject to narrowly defined exceptions.

The argument that secrecy makes independent review impracticable is not conclusive. Comparative jurisprudence recognises that secret surveillance can coexist with democratic government when legal rules are sufficiently clear and supervision is effective. In *Klass v. Germany* and *Roman Zakharov v. Russia*, the European Court of Human Rights examined the safeguards surrounding secret interception, including the quality of the law, supervision and available remedies. These decisions are persuasive rather than binding in India, but they illustrate a general constitutional principle: secrecy in the operation of surveillance does not eliminate the need for independent safeguards.

The same reasoning informs the Supreme Court's approach to national security. In *Anuradha Bhasin v. Union of India*, the Court treated proportionality and judicial review as applicable to executive restrictions affecting fundamental rights. In *Manohar Lal Sharma v. Union of India*, concerning allegations surrounding Pegasus spyware, the Court also declined to treat national security as a blanket bar to judicial scrutiny and constituted an expert committee to examine the allegations. These decisions do not create a comprehensive surveillance code, but they reinforce the proposition that national security remains a legitimate constitutional objective within, not outside, the discipline of law and judicial review.

CONCLUSION

The constitutional legitimacy of surveillance depends less on whether the State possesses the power than on the legal conditions governing its use. Indian law has developed

significant safeguards through judicial decisions and statutory rules, yet the framework remains fragmented and heavily dependent on executive authorisation and executive review. The current position is also more legally complex than the simple narrative of an old law being replaced by a new one.

The post-Puttaswamy inquiry should therefore focus on safeguards: precise statutory thresholds, independent prior authorisation, emergency review, strict retention and destruction duties, protection for privileged communications, delayed notice and an effective remedy. Such measures do not treat security and privacy as mutually exclusive. They seek to ensure that surveillance, when lawfully required, remains an instrument of constitutional government rather than an area of executive power insulated from meaningful accountability.

REFERENCES

1. Constitution of India, arts. 14, 19 and 21.
2. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
3. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
4. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
5. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
6. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
7. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
8. *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1.
9. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
10. *Gujarat Mazdoor Sabha v. State of Gujarat*, (2020) 10 SCC 459.
11. Indian Telegraph Act, 1885, s. 5(2).
12. Information Technology Act, 2000, s. 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
13. Telecommunications Act, 2023, ss. 20, 60–61; Ministry of Communications, Department of Telecommunications, S.O. 2408(E), Gazette of India, Extraordinary, 21 June 2024.
14. Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Gazette of India, Extraordinary, 6 December 2024; Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Amendment Rules, 2025, G.S.R. 625(E), Gazette of India, Extraordinary, 12 September 2025.
15. Digital Personal Data Protection Act, 2023, s. 17; Ministry of Electronics and Information Technology, G.S.R. 843(E), Gazette of India, Extraordinary, 13 November 2025 (notification bringing provisions of the Act into force in phases).
16. International Covenant on Civil and Political Rights, art. 17, 999 U.N.T.S. 171 (1966).
17. *Klass and Others v. Germany*, App. No. 5029/71, Eur. Ct. H.R., 6 September 1978.
18. *Roman Zakharov v. Russia* [GC], App. No. 47143/06, Eur. Ct. H.R., 4 December 2015.
19. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
20. *Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985 (27 October 2021).