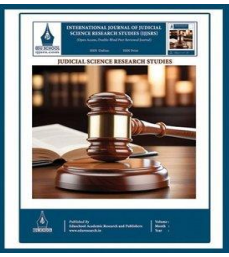
INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: 3049-0618 ISSN Print: 3108-2785



Digital Surveillance and Civil Liberties in India

Lazar T A

Manager, St. Mary's U.P. School, Vendore, Amballur, Kerala, India.

Article information

Received: 7th February 2026
Received in revised form: 6th March 2026
Accepted:10th April 2026
Available online: 21st May 2026

Volume: 3
Issue: 2
DOI: https://doi.org/10.63090/IJJSRS/3049.0618.0041

Abstract

This paper examines the evolving landscape of digital surveillance within India's legal framework and its implications for civil liberties. Following the landmark Puttaswamy judgment recognizing privacy as a fundamental right, India faces the challenge of balancing national security imperatives with constitutional protections. The study analyzes key legislative instruments including the Information Technology Act, 2000 and the Telegraph Act, 1885. Through critical examination of judicial pronouncements and statutory provisions, this paper identifies significant gaps in regulatory oversight, procedural safeguards, and transparency mechanisms. The analysis reveals tensions between state surveillance powers and citizens' rights to privacy, free speech, and due process. This research contributes to understanding how colonial-era legal frameworks intersect with contemporary digital realities, offering insights into the urgent need for comprehensive reform that reconciles security concerns with fundamental rights protection in India's digital age.

Keywords: - Digital Surveillance, Privacy Rights, Information Technology Act, Constitutional Law, Civil Liberties, India

I. INTRODUCTION

The digital revolution has fundamentally transformed the relationship between citizens and the state in India. As technological capabilities expand, so too does the state's capacity for surveillance, raising profound questions about the preservation of civil liberties in an increasingly monitored society. The tension between security imperatives and individual freedoms has intensified in the digital age, where vast amounts of personal data flow through networks subject to governmental scrutiny.

India's legal framework for digital surveillance remains rooted in legislation predating the digital era. The Telegraph Act of 1885, enacted during British colonial rule, continues to govern communications interception, while the Information Technology Act, 2000, attempts to address contemporary digital challenges. This legislative patchwork has created what scholars term a complex surveillance apparatus that operates with limited oversight and accountability.

The Supreme Court's unanimous decision in Justice K.S. Puttaswamy v. Union of India (2017) marked a watershed moment by recognizing privacy as a fundamental right under Article 21 of the Constitution. This judgment established that any surveillance measure must satisfy a three-pronged test of legality, legitimate aim, and proportionality. However, the translation of this constitutional protection into effective legislative safeguards remains incomplete.

This paper examines the architecture of India's digital surveillance legal framework, analyzing its constitutional foundations, statutory provisions, and practical implementation. Through critical engagement with legal scholarship and judicial pronouncements, it explores how India navigates the complex terrain between security and liberty in the digital age.

II. LEGAL AND CONSTITUTIONAL FRAMEWORK

2.1. Constitutional Foundations: The Right to Privacy

The nine-judge bench decision in Puttaswamy fundamentally altered India's constitutional landscape by recognizing privacy as intrinsic to life and personal liberty under Article 21 (Justice K.S. Puttaswamy v. Union of India, 2017). Justice D.Y. Chandrachud's lead opinion traced privacy's genealogy through international jurisprudence, emphasizing its role as the constitutional core of human dignity.

The judgment established a rigorous proportionality framework requiring that any privacy infringement must:

- Be authorized by law,
- Serve a legitimate state interest, and
- Be proportionate to the objective sought.

This standard drew explicitly from the European Court of Human Rights and Canadian constitutional jurisprudence, signaling India's alignment with global privacy norms (Bhatia, 2019).

However, the Court acknowledged privacy's non-absolute nature, recognizing competing interests in national security, public order, and crime prevention. This qualification has created interpretive space for expansive surveillance powers, as subsequent jurisprudence has demonstrated considerable deference to executive determinations of security necessity.

Table 1. Comparative Analysis of Surveillance Authorization Mechanisms

Country	**Authorization Body**	**Transparency Reporting**	**Notification to Targets**
India	Executive (Home Secretary)	None	No provision
United States	FISA Court (Judicial)	Annual statistical reports	Post-investigation (limited)
Germany	Judicial warrant required	Parliamentary oversight reports	Mandatory post-surveillance
United Kingdom	Secretary of State + Judicial Commissioner	Annual transparency reports	Where operationally feasible
Canada	Federal Court authorization	Public Safety Canada annual reports	After conclusion of investigation

Note. Compiled from Donohue (2016) and national legislation.

Table 1 demonstrates India's divergence from democratic norms in surveillance governance. While peer democracies require judicial authorization or at minimum dual authorization (executive plus judicial oversight), India relies exclusively on executive discretion. Similarly, India's complete absence of transparency reporting contrasts sharply with international practice, where public accountability mechanisms are standard.

2.2. The Information Technology Act, 2000

The Information Technology Act represents India's primary legislative response to digital governance challenges. Section 69 grants the central and state governments sweeping powers to intercept, monitor, or decrypt any information through any computer resource in the interests of sovereignty, security, public order, or investigation of offenses (Information Technology Act, 2000).

The procedural safeguards in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, require authorized orders from the Home Secretary or equivalent officials. Yet these rules have been criticized for lacking meaningful judicial oversight. Interception orders are reviewed by a committee rather than courts, and no independent mechanism exists to challenge surveillance targeting (Bhatia, 2019).

Section 69B further empowers the government to authorize monitoring and collection of traffic data or information through any computer resource for cybersecurity purposes. The vagueness of cybersecurity and absence of temporal limitations create potential for pervasive, indiscriminate surveillance. Academic criticism has focused on the Act's failure to require demonstrable necessity, establish retention limits, or mandate transparency reporting.

Section 69A's provisions for blocking public access to online content have generated particular controversy. The government may direct blocking of content in the interest of sovereignty, public order, or other specified grounds, with decisions reviewed by an executive committee rather than courts. This administrative censorship mechanism has been challenged as incompatible with free speech guarantees under Article 19(1)(a) (Shreya Singhal v. Union of India, 2015).

2.3. The Telegraph Act, 1885 and Communications Surveillance

The Indian Telegraph Act, enacted during colonial administration, governs telephone interception. Section 5(2) permits the government to intercept messages in the interests of sovereignty, public safety, public order, or emergency circumstances. The Telegraph (Amendment) Rules, 2007, establish procedural requirements including Home Secretary authorization and review committee oversight.

In People's Union for Civil Liberties v. Union of India (1997), the Supreme Court recognized the constitutional implications of telephone tapping, holding that conversations over telephone constitute private communication protected under Article 21. The Court mandated procedural safeguards including reasons in writing, periodic review, and destruction of intercepted material irrelevant to investigations. However, compliance mechanisms remain weak, with no effective remedy for illegal surveillance.

The convergence of telecommunications and internet technologies has created jurisdictional ambiguities between the Telegraph Act and IT Act frameworks. Service providers often face contradictory obligations, while citizens lack clarity on applicable legal standards and redress mechanisms. This regulatory fragmentation undermines both accountability and rights protection.

Table 2. Key Surveillance Provisions in Indian Law: Safeguards and Gaps

Legislation	Surveillance Powers	Procedural Safeguards	Critical Gaps
IT Act §69	Interception, monitoring, decryption of information through any computer resource	Home Secretary authorization; Review Committee (executive officials only)	No judicial oversight; No target notification; Broad grounds (sovereignty, security, public order)
IT Act §69A	Blocking public access to online information	Committee for Examination of Requests (executive)	No prior judicial review; Content creator not heard before blocking; Limited appeal mechanisms
IT Act §69B	Monitoring and collection of traffic data for cybersecurity	Government agency authorization; Cybersecurity agency designation	Undefined cybersecurity; No temporal limits; Potential for bulk surveillance
Telegraph Act §5(2)	Interception of telephone messages in emergencies or interests of public safety	Home Secretary approval; Review Committee; Material destruction requirement (PUCL judgment)	Colonial-era statute; Weak compliance mechanisms; No independent oversight body

Note. Analysis based on statutory provisions and implementing rules. PUCL = People's Union for Civil Liberties v. Union of India (1997).

Table 2 illustrates the structural deficiencies pervading India's surveillance framework. Across all major provisions, judicial authorization is absent, replaced by executive-dominated review mechanisms. The identified gaps vague authorization criteria, lack of independent oversight, absence of notification requirements, and unlimited data retention collectively create conditions for surveillance overreach inconsistent with Puttaswamy's constitutional mandate.

III. ANALYSIS OF SURVEILLANCE ARCHITECTURE

3.1. Gaps in Judicial Oversight

India's surveillance framework exhibits a striking absence of judicial authorization requirements. Unlike jurisdictions such as the United States, where the Foreign Intelligence Surveillance Court reviews surveillance orders, or Germany, where judicial warrants are mandatory, Indian law vests authorization power in executive officials. The review committees established under the IT and Telegraph Rules lack independence, comprising executive branch officials with no judicial members.

This executive-dominated structure contradicts the separation of powers doctrine and the proportionality test articulated in Puttaswamy. As Bhatia (2019) observes in his constitutional analysis, when the executive acts as both investigator and judge, the very premise of due process collapses. The absence of judicial gatekeeping enables surveillance decisions based on executive convenience rather than constitutional necessity.

Furthermore, individuals subjected to surveillance lack notice and opportunity to contest orders. The secrecy surrounding surveillance programs, while sometimes operationally justified, creates insurmountable barriers to accountability. Without notification mechanisms or standing to challenge surveillance, citizens cannot vindicate their privacy rights even after surveillance concludes.

3.2. The Transparency Deficit

Indian law imposes no transparency reporting obligations on government agencies conducting surveillance. Unlike democracies such as the United Kingdom, Canada, or Australia, which publish annual statistics on surveillance activities, India maintains complete opacity regarding the scope, scale, and targets of its surveillance operations.

Requests under the Right to Information Act, 2005, seeking surveillance statistics have been routinely denied on national security grounds. This categorical exemption approach prevents any public evaluation of surveillance's scope or its compliance with constitutional standards. The lack of transparency extends to technology deployment, with programs enabling real-time communications surveillance implemented without public consultation or parliamentary debate.

Civil society organizations have documented the acquisition of sophisticated surveillance technologies including facial recognition systems and mobile location tracking capabilities, all deployed with minimal public disclosure or rights-impact assessment. This opacity fundamentally undermines democratic accountability for state surveillance powers.

3.3. Data Protection and State Access

India's efforts to establish data protection legislation have been prolonged and contentious. The Personal Data Protection Bill, introduced in various forms since 2018, has faced criticism for granting excessive powers to the state. As Kak (2018) observed in her analysis of the draft bill, it was more fully understood in the context of political challenges to Aadhaar, Europe's GDPR, and concerns about tech company dominance.

The draft law contained conflicting objectives of protecting personal data of citizens from the state while ensuring the state's ease in delivering services. Critics noted that it favored the latter objective, with broad exemptions allowing government access to personal data on grounds of sovereignty and public order. Justice B.N. Srikrishna, who chaired the committee that drafted the original bill, later criticized revisions as having the ability to turn India into an Orwellian State.

The eventual passage of the Digital Personal Data Protection Act in 2023 continued to reflect these tensions. While establishing some protections for personal data, the Act maintains significant exemptions for state access, particularly for security and public order purposes. The lack of independent oversight over such access perpetuates concerns about unchecked surveillance capabilities.

3.4. Implications for Democratic Participation

Pervasive surveillance fundamentally alters the conditions for democratic participation. The knowledge or suspicion that communications are monitored produces chilling effects on free expression, particularly for marginalized communities and dissenting voices. Research demonstrates that awareness of surveillance leads to self-censorship, homogenization of viewpoints, and withdrawal from public discourse (Penney, 2016).

In India's context, surveillance has demonstrably targeted human rights defenders, journalists investigating government corruption, and lawyers representing controversial clients. The asymmetry between state surveillance capabilities and citizen privacy protection threatens the deliberative foundations of democracy. As Cohen (2019) argues in her analysis of informational capitalism, surveillance produces docile subjects rather than engaged citizens.

India's surveillance architecture, lacking robust safeguards, risks creating precisely such dynamics of conformity and acquiescence. The impact extends beyond individual privacy to encompass the independent journalism, civil society activism, and political dissent essential to democratic governance.

3.5. The Path Forward: Reforming Surveillance Law

Reforming India's surveillance legal framework requires fundamental restructuring around several principles. First, judicial authorization must become mandatory for targeted surveillance. Drawing from international best practices, a specialized court or judicial panel should review surveillance requests, ensuring independent evaluation of necessity and proportionality before authorization (Donohue, 2016).

Second, legislation must narrow permissible grounds for surveillance. Vague categories like public order should be replaced with specific, demonstrable threats to life, national security, or serious crime. The necessity standard must require showing that surveillance targets are reasonably suspected of involvement in specified unlawful activities and that less intrusive measures would be inadequate.

Third, transparency mechanisms are essential. Annual reports detailing surveillance statistics, including applications made, orders granted, and individuals affected, should be published. Aggregate data disclosure, standard in many democracies, enables public accountability without compromising specific operations. Technology impact assessments should precede deployment of new surveillance capabilities, with meaningful public consultation.

Fourth, data minimization and retention limits must be mandated. Surveillance should be temporally bounded, with automatic expiration absent renewed judicial authorization. Intercepted material unrelated to the investigation's purpose must be promptly destroyed, not indefinitely warehoused.

Finally, meaningful remedies for unlawful surveillance must exist. Notification requirements, allowing surveillance targets to learn of and challenge surveillance after investigations conclude, would enable accountability. Independent oversight bodies with investigative powers and complaint mechanisms could provide forums for redress currently absent from India's legal architecture.

IV. CONCLUSION

India's digital surveillance legal framework stands at a critical juncture. The constitutional recognition of privacy in Puttaswamy established aspirational standards for rights protection, yet legislative implementation remains profoundly inadequate. Colonial-era statutes govern contemporary digital realities, while modern surveillance technologies operate with minimal legal constraint. The resulting system concentrates power in executive hands, operates behind veils of secrecy, and provides citizens with neither notice nor recourse.

This analysis has identified fundamental deficiencies in judicial oversight, transparency, and proportionality. India's approach to surveillance authorization, lacking independent judicial gatekeeping, fails to meet international human rights standards. The absence of transparency reporting prevents democratic accountability, while expansive surveillance grounds and minimal procedural safeguards enable disproportionate intrusions into privacy and free expression.

The stakes extend beyond individual privacy to encompass democracy's vitality. Surveillance without adequate safeguards threatens the independent journalism, civil society activism, and political dissent essential to democratic governance. As technological capabilities expand, the urgency of comprehensive legal reform intensifies.

The path forward requires legislative courage to subordinate surveillance powers to constitutional norms. India must transition from a framework prioritizing state information access to one that recognizes privacy protection as foundational to liberty and democracy. This transformation, while challenging, is essential if India is to realize Puttaswamy's promise of privacy as a fundamental right in the digital age. The question is not whether reform is necessary, but whether the political will exists to enact it before surveillance's corrosive effects on civil liberties become irreversible.

REFERENCES

Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.
Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Donohue, L. K. (2016). *The future of foreign intelligence: Privacy and surveillance in a digital age*. Oxford University Press.
Information Technology Act, 2000, No. 21 of 2000 (India).
Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, S.O. 2784(E) (India).
Kak, A. (2018). The emergence of the Personal Data Protection Bill, 2018: A critique. *Economic & Political Weekly*, *53*(38). https://www.epw.in/journal/2018/38/commentary/emergence-personal-data-protection-bill.html
Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117–182.
People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
Telegraph Act, 1885, No. 13 of 1885 (India).
Telegraph (Amendment) Rules, 2007, S.O. 1308(E) (India).