Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 15 Issue 01, 2026

A Study on Interception and Monitoring of Communications in India for Cybercrime Investigation: Legal Procedures and Safeguards

[1]Nirdesh Deb, [2*]Sharad Sekhawat, [3]Prasenjit Roy

[1]Ph.D. Scholar, School of Social Sciences & Languages, Lovely Professional University, Phagwara, Punjab, India

[2]Associate Professor, Department of Government & Public Administration, School of Social Sciences & Languages, Lovely Professional University, Phagwara, Punjab, India

[3]Triple MA, B.Ed, NET/SLET/GATE, CTET, PG Diploma in Police Administration & Investigation

Peer Review Information

Submission: 21 March 2026

Revision: 13 April 2026

Acceptance: 27 April 2026

Keywords

Interception, Surveillance, Privacy, Fundamental Rights, National Security, CMS, NATGRID, NETRA.

Abstract

The interception and monitoring of communications are crucial weapons for ensuring national security, and complex criminal investigation. In the age of Information Technology, the rapid spreading out of digital surveillance technologies has increased the tension between law enforcement agencies and privacy rights of individual. In India, use of Centralised Monitoring System (CMS), Network Traffic Analysis (NETRA) and the National Intelligence Grid (NATGRID) for the surveillance and monitoring of suspects shows the state's growing capacity for bulk interception of communications. While these mechanism of monitoring justified on grounds of sovereignty and integrity of India, security of the states, public order and public safety. But they also raise questions on constitutional rights under Article 21 and judicial recognition of privacy as fundamental right as ordered in the Justice KS Puttuswamy v. Union of India (2017). This paper examines the existing legal architecture on surveillance matter, including the Indian Telegraph Act, 1885, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, alongside judicial safeguards laid down in *People's Union for Civil Liberties (PUCL) v. Union of India* (1997). By placing India's surveillance framework within comparative contexts of other countries like United Kingdom, Russia and Australia, the study identify the structural differences, particularly the absence of independent oversight and pre-authorization of surveillance by Judicial Authority. The paper hash out for a harmonized National Surveillance Policy that balances legitimate security interests as well as maintaining constitutional guarantees of privacy of individual and proposes for institutional reforms for incorporation of accountability, transparency and proportionality into India's surveillance framework.

Introduction

With development of Information Technology, the Indian society has revolutionized in governance, commerce as well as in communication technology. At the same time, there has emerged new vulnerabilities in the domains of cyber security, terrorism and transnational crime. To counter this, India has expanded its surveillance infrastructure through different projects like CMS, NETRA and NATGRID. These technologies enabled interception of communication including internet communication, financial transactions, physical travelling details etc. This development

created questions about boundaries of state power and individual rights enshrined in the Constitution of India.

The legal framework governing interception is covered in the Telecommunication Act, 2023, and the Information Technology Act of 2000, the Digital Personal Data Protection Act, 2023,the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. These laws authorize interception on grounds such as sovereignty, integrity, security and public order, but leave substantial discretion in the hands of the executive. In PUCL v. Union of India (1997), the Supreme Court imposed procedural safeguards, requiring written authorizations and review committees for lawful interception, while in Puttaswamy v. Union of India (2017) it elevated privacy to a fundamental right subject to the proportionality standard. Despite these interventions, the absence of judicial warrants, inadequate oversight, and misty review processes leave citizens vulnerable to disproportionate surveillance.

Comparative studyprovides valuable insights. The United States' Foreign Intelligence Surveillance Court (FISC) provides judicial authorization for national security surveillance, while the United Kingdom's Investigatory Powers Act (2016) institutionalizes "double-lock" safeguards through judicial commissioners. The European Court of Justice, in Schrems II (2020), reaffirmed the centrality of proportionality and necessity in cross-border personal data flows. These models demonstrate that effective surveillance need not impede constitutional safeguards.Against this backdrop, this paper critically examines the Indian framework, identifies structural shortcomings, and proposes reforms grounded in constitutional principles and comparative best practices.

Literature Review

Bhatia (2014) characterizes India's reliance on the Telegraph Act as a "colonial hangover," arguing that executive-controlled interception undermines constitutional guarantees. However, this law is repealed and replaced by the Telecommunication Act, 2023(Telecommunications Act, 2023).

Arun (2023) notes that India's surveillance regime is a "mosaic of dovetailing laws" with little coherence, resulting in inconsistent practices and thus violation of individual privacy. Ramachandran (2014) revisits *PUCL*, underscoring that the Court's safeguards have not kept pace with technological change.

Naik (2025) examines the evolution and present position of India's legal framework on lawful interception based on the laws like The Telegraph Act 1885, The Information Technology Act 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009. He also underscores the importance of judgement related to lawful interception in India like PUCL v. Union of India (1997) in balancing the protection of privacy, proportionality as well as protection of the country. Overall, the paper argues for more transparent and accountable process of lawful interception in the country so that it balance the national security imperatives with the constitutional guarantee of right to privacy of the individual.

Brownell (1954), in his work 'The Public Security and Wire Tapping' published
in Cornell Law Review, has taken an effort to find for a solution to resolve the practice of or lawful interception and the invasion of an individual right to privacy.

Ismail (2013), in his work 'A Critical Analysis on Telephone Tapping Conversation,' has analysed different provisions of taping conversation records and interceptions and its evidentiary values before the Court. He is of the view that that the Central Government must frame the guidelines so that the violation of individual right in the process of collecting information through lawful interception can be prevented.

Rubinstein, Nojeim, and Lee (2014) present a comparative study of thirteen countries, examining the different ways governments obtain access to personal data held by private entities. Their findings suggest that while legal frameworks exist, often organizations are inconsistent with actual practices, lacking transparency and clear alignment with human rights standards. The authors argue for statutory transparency, independent oversight for balancing between security interests and individual privacy rights.

Greenleaf (2019) traces how Asian jurisdictions have gradually strengthened privacy laws under the influence of General Data Protection Regulation (GDPR), yet significant divergences remain across countries. This fragmentation creates barriers for regulating cross-border surveillance and lawful interception, leaving gaps in accountability. His analysis underscores the difficulty India faces in balancing national security priorities with evolving international privacy standards.

Together, the literature suggests that while surveillance is recognized as legitimate in combating security threats, India's current framework lacks proportionality, transparency, and independent oversight mechanisms.

Procedure for Lawful Interception

- **Authorization and Competent Authority:** Lawful interception requires prior authorization. No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource except by an order issued by the competent authority. Under relevant rules, the "Competent Authority" for the Central Government is typically the Secretary in the Ministry of Home Affairs; for states or Union Territory, the Home Secretary or equivalent is the competent authority for issuing orders of interception, monitoring or decryption of information.
- **Conditions for Interception:** Statutory provisions generally allow interception in cases involving:
    1. Public emergency or public safety concerns.
    2. Sovereignty and integrity of India.
    3. Security of the State.
    4. Prevention, investigation or prosecution of offences.

The order must specify the target, communication type, reasons, and duration. Temporary or emergency orders are permissible but must be confirmed by the competent authority within a fixed period.

The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

- **Indian Legal Framework:** There are various laws in existence which deal with the subject matter of this paper. There are also safeguards enshrined in Our Great Indian Constitution. Some of the provisions are discussed below in brief.
- **Constitutional Provision**: Article 21 of the Indian Constitution is the primary article that secures the right to privacy, which includes the protection of personal information. This right covers personal data, bodily integrity, personal autonomy and protection from unauthorized state surveillance. The Hon'ble Supreme Court of India in the landmark Justice K.S.Puttuswamy (Retd.) v. Union of India(2017) case declared that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21. However, the right to privacy is not absolute and can be restricted by the State for legitimate aims such as national security, public order, or to prevent crime, provided the restrictions are fair, just and reasonable.

The Telecommunication Act, 2023

Section 20(2)(a) empowers the central and state government to intercept or block any class of messages through telecommunication network on the ground of sovereignty and integrity of India, security of the State, friendly relations with foreign states, public order, or preventing incitement of cognizable offences. Prior to enactment of this Act, the interceptions were carried out under section 5(2) of the Telegraph Act 1885. This is subject to procedure and safeguards prescribed in the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 where the competent authority, requirements parameters, review committee and norms of confidentiality of information were specifically defined. In *PUCL v. Union of India* (1997), the Supreme Court framed certain guidelines to be adopted while interception for providing safeguards to the people while empowering law enforcement agencies for protection of sovereignty and integrity of the country of the country. The guidelines are the written authorization, periodic review, and limited duration to prevent arbitrary exercise. However, the framework remains executive-driven, no judicial authorization is required.

The Information Technology Act, 2000

Section 69 of IT Act authorizes interception, monitoring, and decryption of electronic communications for similar grounds mentioned in the Telecom Act. The Information Technology (procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009 operationalize this power. Here again, power of authorizations is vested with the Home Secretary at central or state level. Review Committees, composed of senior bureaucrats, provide post-facto oversight. Critics hash out that such internal review lacks independence (Ramachandran, 2014).

Again, Sections 43A and 72A of Information Technology Act, 2000 provide for compensation and punishment for the disclosure of sensitive personal data without consent.

The Digital Personal Data Protection Act, 2023

Though this Act established a data protection framework but exempts government agencies broadly because of security, sovereignty and

public order. In addition, the absence of a strong 'Data Protection Authority' undermines the meaningful oversight. The article by Arun (2023) noted that this Act is legitimizing the state surveillance rather than constricting it.

Judicial Pronouncements

- *PUCL v. Union of India* (1997): Introduced procedural safeguards for call interception, but abstained from issuing direction mandating judicial warrants for putting any number under lawful interception.
- *K.S. Puttaswamy v. Union of India* (2017): Elevated privacy to a fundamental right and established the **proportionality test**—legality, necessity, and proportionality—as the benchmark for lawful interception. This means that interception cannot be arbitrary. It must be justified, narrowly tailored and subject to safeguards of individual privacy.
- Pegasus litigation (2021): The Supreme Court appointed an expert committee to probe allegations of spyware use, reflecting judicial unease with unregulated surveillance which is a violation of fundamental right to privacy.

Thus, collectively if we see, India's framework for lawful interception is illustrating a paradox. One the one side, it is legally grounded but safeguards remain weak and fragmented since there is no judicial oversight during the process of lawful interception.

Comparative Perspectives

During research comparative study on the law related to surveillance of the following countries were conducted and analysed below:

India

In India, the legal framework governing lawful surveillance and interception is covered in The Telecommunication Act, 2023 and The Information Technology Act of 2000. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 are framed based on the above stated Acts. The Digital Personal Data Protection Act, 2023 introduced to safeguard individual data is also a reference law to be taken into consideration.

United States

The **Foreign Intelligence Surveillance Act (FISA, 1978)** established the **FISA Court (FISC)** to review and authorize national security surveillance requests. Thus, the FISC provides judicial involvement at the authorization stage. The **USA Freedom Act (2015)**, curtailed bulk metadata collection and introduced reporting obligations.

United Kingdom

The **Investigatory Powers Act (2016)** provides surveillance powers under a "double-lock" system that means such warrants mandates approval from both a 'Secretary of State' and a '**Judicial Commissioner'**. The Act also mandates transparency reports and provides redress through the '**Investigatory Powers Tribunal'**.

European Union

The **General Data Protection Regulation (GDPR)** underscoresthe necessity and proportionality in data processing, including surveillance. The **Schrems II judgment (CJEU, 2020)** invalidated the EU-US Privacy Shield, stating that bulk surveillance without safeguards violated fundamental rights under the EU Charter.

Germany

The **G10 Act** regulates restrictions on the secrecy of telecommunications. Surveillance requires approval from the **G10 Commission**, an independent body appointed by the Parliament. German constitutional jurisprudence consistently reinforces the proportionality principle.

Russia (Contrasting Model)

Russia's **Yarovaya Law (2016)** mandates data retention and government access of calls and texts for six months and metadata for three years. The Act lacks strong safeguards and ignore the individual privacy for the sake of curving terrorism and public safety. This law serving as a cautionary example of how surveillance can undermine rights when unchecked.

Jurisdiction	Key Law(s)	Authorization / Oversight	Safeguards & Principles	Notable Features
India	Telecommunication Act, 2023; IT Act, 2000; Telecommunication Interception Rules, 2024; IT Interception Rules, 2009; Digital Personal Data Protection Act, 2023	Executive authorization (Home Secretary at Union/State level); Review Committees (executive)	Minimal judicial oversight; safeguards mostly executive; privacy recognized under Article 21	Broad grounds including public safety, national security, sovereignty, prevention of crime
United States	FISA (1978); USA Freedom Act (2015)	Judicial authorization by FISA Court (FISC)	Judicial involvement; reporting obligations introduced after 2015	Bulk metadata collection curtailed; strong national security focus
United Kingdom	Investigatory Powers Act (2016)	"Double-lock" system: Secretary of State + Judicial Commissioner	Transparency reports; redress via Investigatory Powers Tribunal	Consolidates surveillance powers; combines executive and judicial control
European Union	GDPR (2016); Schrems II Judgment (CJEU, 2020)	Judicial review at EU level; independent data protection authorities	Necessity & proportionality are core principles; strong privacy protections	Schrems II invalidated EU–US Privacy Shield over bulk surveillance concerns
Germany	G10 Act	Authorization by independent **G10 Commission** (appointed by Parliament)	Proportionality principle reinforced by Constitutional Court	Clear judicial-constitutional check; limited, targeted grounds
Russia (Contrasting)	Yarovaya Law (2016)	Government agencies (e.g., FSB) direct access; telecoms must comply	Very weak safeguards; no strong judicial or parliamentary review	Mandatory storage of calls (6 months) & metadata (3 years); undermines privacy in name of counter-terrorism

Critical Analysis of Shortcomings

Despite statutory grounding under the **Telecommunication Act (2023)**, **Information Technology Amendment Act (2008)**, and the **Digital Personal Data Protection Act (2023)**, India's surveillance regime suffers from deep structural deficiencies.

- **Executive-Centric Authorization**

Surveillance orders are approved by the Home Secretary (Union or State), with "emergency" powers delegated to senior bureaucrats of the rank Inspector General of Police or equivalent rank and above. This executive concentration of power directly contradicts the separation of powers principle. Unlike search warrants, which require judicial sanction, interception can be authorized solely within the executive, leaving scope for arbitrariness.

- **Absence of Judicial Oversight**

Judicial authorization—common in many democracies—is conspicuously absent. *PUCL* (1997) endorsed bureaucratic review committees instead of judicial warrants, a position that is increasingly untenable after *Puttaswamy* (2017), which requires surveillance restrictions to pass the test of **legality, necessity, and proportionality**.

- **Bulk and Dragnet Surveillance**

Projects likeCentralized Monitoring System (CMS), Network Traffic Analysis (NETRA) and the National Intelligence Grid (NATGRID) facilitate bulk collection of metadata and content, without sufficient limitations to targeted surveillance. This contradicts proportionality, since bulk interception affects law-abiding citizens disproportionately.

- **Transparency Deficit**

Unlike democracies that publish annual surveillance statistics, India provides little public reporting. An RTI revealed that 7,500–9,000 interception orders are issued monthly, but no aggregate data is disclosed officially (Times of India, 2018). Lack of transparency fosters suspicion and weakens democratic legitimacy.

- **Weak Remedies and Accountability**

There is no neutral body for citizens to challenge unlawful interception. Internal review committees rarely overturn orders. The absence of a strong **Data Protection Authority** compounds the accountability vacuum.

- **Technological Risks**

The Pegasus spyware controversy illustrates how state surveillance can be outsourced or misused. Without statutory regulation of spyware procurement or deployment, citizens face covert intrusions without remedy.

Thus, it is found that India's surveillance regime is **executive-heavy, opaque and disproportionate**—leaving it incompatible with constitutional requirements of accountability and proportionality.

Way Forward

India requires a recalibration of its surveillance regime to align with constitutional guarantees and international best practices. Reform should be guided by four interrelated pillars: statutory consolidation, judicial oversight, independent accountability, and technological safeguards.

1. Statutory Consolidation: A National Surveillance Policy

The current framework, dispersed across the Telecommunication Act, IT Act, and Data Protection and Privacy Act (DPDP Act), must be harmonised into a National Surveillance Policy. Such a law should codify:

- Permissible grounds for interception, limited to threats of national security and serious crime;
- Authorised agencies, explicitly listed to avoid misuse;
- Time-bound authorizations, with strict renewal procedures; and
- Data retention and deletion protocols, ensuring minimization of unnecessary collection.

This would replace colonial-era provisions with a coherent, rights-compliant framework.

2. Judicial Authorisation and Oversight

Surveillance should mirror the model of search warrants, requiring prior judicial authorisation. Judges can assess legality, necessity, and proportionality before interception commences. Post-facto review by an Independent Oversight Commission—comprising retired judges, privacy experts, and legislators—should audit implementation, review logs, and investigate complaints. This dual mechanism would ensure both ex ante and ex post accountability.

3. Parliamentary Oversight and Transparency

Periodic parliamentary review is essential for bolstering democratic legitimacy. Annual transparency reports should disclose the following key information:

- The number of interception orders issued.
- The categories of crimes or threats targeted.
- Aggregate data on approvals, rejections, and renewals.

Such reporting, which is already commonplace in the United Kingdom and the United States, can foster public trust while preserving operational secrecy.

4. Rights-Based Technological Safeguards

Technical reforms should complement legal reforms. Surveillance systems should incorporate the following safeguards:

- Privacy-by-design tools, such as data minimization and anonymization.
- Secure audit trails to prevent unauthorised access.
- Encryption safeguards to avoid backdoors that compromise cyber resilience.

By aligning with the OECD Privacy Guidelines and Council of Europe's Convention 108+, India can ensure that surveillance technologies respect democratic protections (Kuner, 2021).

Conclusion

Surveillance is indispensable for safeguarding sovereignty and national security in a digital age marked by cybercrime, terrorism, and

transnational threats. However, when unchecked, it risks undermining the very constitutional freedoms it purports to defend. India's reliance on executive-driven authorizations, and opaque oversight has produced a surveillance regime that is outdated, disproportionate, and democratically fragile.

Comparative experience demonstrates that surveillance can coexist with robust safeguards. Judicial warrants in the United States, the double-lock system in the United Kingdom, and parliamentary oversight in Germany illustrate pathways for reconciling state security with fundamental rights. The European Court of Justice's jurisprudence, emphasizing proportionality, underscores the normative benchmark India must aspire to.

This paper has argued for a National Surveillance Policy, embedding judicial authorization, independent oversight, parliamentary review, and technological safeguards. Such reforms are not designed to weaken security but to constitutionalize it—ensuring that state power remains bounded by legality, necessity, and proportionality.

As a constitutional democracy, India cannot afford a surveillance regime that prioritizes expediency over accountability. Reform entails not rejecting surveillance but rather embedding it within a framework of legality, proportionality, accountability, and transparency—principles that have already been endorsed by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India,(2017)case.

Reference

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

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

Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), C-311/18.

U.S. Congress. (1978). Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511.

UK Parliament. (2016). Investigatory Powers Act 2016, c. 25. London: HMSO.

Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), C-311/18.

European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. National Law School of India Review, 26(2), 127–155.

Arun, P. (2023). A mosaic of dovetailing laws: India's communications surveillance regime. Indian Law Review, 8(2), 158–180. https://doi.org/10.1080/24730580.2023.2193931

Ramachandran, C. (2014). PUCL v. Union of India revisited: Why India's surveillance law must be redesigned for the digital age. NUJS Law Review, 7(2), 243–268.

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: A comparative analysis. International Data Privacy Law, 4(4), 346–368.

Greenleaf, Graham, Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock (August 30, 2019). (2019) No 4, Revista Uruguaya de Protección de Datos Personales (Revista PDP), August 2019, 49-73, UNSW Law Research Paper No. 19-103, Available at SSRN: https://ssrn.com/abstract=3483794

Kaye, D. (2021). The Spyware State and the Prospects for Accountability. Global Governance: A Review of Multilateralism and International Organizations, 27(4), 483-492. https://doi.org/10.1163/19426720-02704005

Vipul Kharbanda (Aug, 2015). "Policy Paper on Surveillance in India". The Centre for Internet & Society. https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india

Kamesh Shekhar & Shefali Mehta (Feb,2022)."The state of surveillance in India: National security at the cost of privacy?". Observer Research Foundation. https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/#:~:text=Under%20the%20legal%20grounds%20of,with%20international%20governments%2C%20integrating%20public

Mr. David Kaye (Feb,2019). "The Surveillance Industry and Human Rights". Software Freedom Law Centre. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/SFLC_IN.pdf

Ira S. Rubinstein, Gregory T. Nojeim, and Ronald D. Lee (2014). "Systematic government access to personal data: a comparative analysis". International Data Privacy Law. Doi: - https://doi.org/10.1093/idpl/ipu004

P. Arun (December, 2016). "Surveillance and Democracy in India: Analysing Challenges to Constitutionalism and Rule of Law". Journal of Public Affairs and Change, Vol.I No.1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=29

Sagar, S. (2025). Low-Resource Fine-Tuning of LLMs for Domain-Specific Tasks. *Universal Research Reports*.

Telecommunications Act, 2023, Act No. 44 of 2023 (India), published in The Gazette of India on December 24, 2023. URL: https://egazette.gov.in/WriteReadData/2023/250880.