Swami Vivekananda Advanced Journal for Research and Studies
Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X **Pg. 21-33**

Evolving Standards of Electronic Surveillance and the Right to Privacy in India: A Critical Analysis

Dr. Mohammad Rashid
Assistant Professor,
Department of Law, K.G.K.(P.G.) College Moradabad UP

Accepted: 09/09/2025
Published: 14/09/2025 ***DOI: http://doi.org/10.5281/zenodo.17346401***

Abstract

The fast-evolving world of digital technology has joined the world of surveillance and privacy, posing some urgent questions on the proportions between the interests of the state security and the rights of the individual. Critically, the paper will review the changing standard of electronic surveillance and how it has impacted the right to privacy in India. Privacy as an essential right was recognized by the constitution in the case, Justice K.S. Puttaswamy v. The case of Union of India (2017) was a significant milestone in the Indian jurisprudence that allows the legal and policy frameworks that regulate surveillance to remain active based on the colonial-era legislation i.e. the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. The current research paper will follow a doctrinal and analytical methodology in revealing the history of surveillance tools, analyzing modern digital mechanisms of surveillance, such as the use of Aadhaar in identification, the Central Monitoring System (CMS), and spyware usage, and evaluating them against the constitutional protection assurances.

The paper also makes a comparative study to world systems of surveillance, especially the United States and the European Union in the context of the importance of judicial oversight, transparency, and proportionality to uphold a democratic balance. It claims that the current system in India is not well equipped to discourage arbitrary intrusion as it has no independent body to regulate it, and the populace does not have much accountability. The recent adoption of the Digital Personal Data Protection Act, 2023, though a good move, does not cover the surveillance architecture and its abuse in detail

The paper has concluded that the changing principles of electronic surveillance in India require a coherent and rights-based legal framework that is based on the principles of transparency, necessity, and proportionality. It also supports the creation of an external supervisory body, judicial sanction of interception, and stringent standards of data protection to protect the privacy of citizens. These reforms are necessary so that technological governance in India is possible under the constitutional morality and international human rights.

Keywords: *Electronic Surveillance; Right to Privacy; Puttaswamy Judgment*

1. Introduction

The current digital age has transformed the manner in which governments, institutions and citizens interact due to technological breakthroughs. As the digital communication evolves, surveillance has emerged as a critical tool that the State can use to uphold national security, curb crime, and governance more effectively (Singh and Bhattacharya, 2021). Nevertheless, the intensive growth of electronic surveillance has brought up grave legal and ethical issues concerning the privacy of an individual being. Tension in India has risen to a center of focus in constitutional and policy discussions in regard to the surveillance capabilities of the State and the right of the citizen to his/her privacy (Rao, 2020).

A broad spectrum of practices, which include telephone tapping, internet monitoring, facial recognition, and mass-scale data gathering via the use of digital identity systems such as Aadhaar are all encompassed by the current field of electronic surveillance in India (Narain, 2019). The government justifies such measures as necessary for maintaining internal security and public order *(Kumar & Sharma, 2022)*. While the State's objectives may be legitimate, the absence of a transparent, statutory oversight mechanism often transforms these systems into tools of potential abuse *(Bhattacharya, 2020)*.

India's surveillance framework traces back to the colonial era. The Indian Telegraph Act of 1885, enacted under British rule, empowered the government to intercept communications in cases of "public emergency" or "public safety" *(Mehta, 2018)*. Even after independence, these provisions continued with minimal change. With the rise of digital communication, the Information Technology Act, 2000 expanded government authority into cyberspace, allowing interception, monitoring, and decryption of electronic information *(Nair, 2021)*. In the last two decades, several large-scale surveillance systems—such as the Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and NATGRID—have been developed to centralize data collection and monitoring *(Choudhury, 2023)*. These developments reflect an expanding surveillance infrastructure that often operates beyond the scrutiny of the public or the judiciary.

The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) marked a turning point in Indian constitutional law. The Supreme Court recognized the Right to Privacy as a fundamental right under Article 21 of the Constitution, emphasizing that any restriction on privacy must meet the tests of legality, necessity, and proportionality *(Supreme Court of India, 2017)*. This ruling aligned India's constitutional jurisprudence with international human rights principles *(Ramanathan, 2018)*. Yet, despite this judicial clarity, India still lacks a comprehensive surveillance law that ensures transparency, judicial authorization, and citizen protection *(Sharma, 2023)*.

Furthermore, the increasing use of biometric and facial recognition technologies and revelations regarding Pegasus spyware have heightened concerns about mass surveillance and unauthorized data interception *(Bhatia, 2021)*. While India's Digital Personal Data Protection Act, 2023, represents progress in defining data rights, it notably exempts government agencies from many of its key provisions *(Kumar, 2023)*. This exemption perpetuates the imbalance between state power and individual liberty, creating a paradox where privacy is constitutionally protected but remains practically vulnerable.

Globally, democratic jurisdictions such as the United States and the European Union have sought to reconcile surveillance with privacy through mechanisms like judicial warrants, independent data protection authorities, and public transparency reports *(European Data Protection Board, 2020; Richards, 2019)*. Comparative analysis of these models reveals that India's framework still lacks institutional safeguards that ensure proportionality and accountability.

Research Problem

The central issue this study addresses is the inconsistency between India's constitutional recognition of privacy and its fragmented, executive-controlled surveillance framework. While the State justifies electronic monitoring on grounds of national security, the absence of judicial oversight and statutory checks poses significant threats to civil liberties *(Narain, 2020)*.

Research Questions

1. How have electronic surveillance mechanisms and standards evolved in India?
2. To what extent do existing laws protect the constitutional right to privacy under Article 21?
3. What are the main challenges and loopholes in India's surveillance framework concerning oversight and accountability?
4. How do global surveillance and privacy standards compare with India's current system?
5. What reforms are needed to balance national security and privacy in the digital age?

Research Objectives

1. To trace the historical and legal development of electronic surveillance in India.

2. To examine how the Indian judiciary has interpreted the right to privacy in the context of surveillance.
3. To evaluate the adequacy of existing surveillance laws and identify key deficiencies.
4. To compare India's surveillance standards with international best practices.
5. To suggest solutions to a rights-based and open surveillance system.

Significance of the Study

The study is relevant since it seeks to examine one of the hottest issues of democratic governance the balance of security and freedom. In an environment that is quickly becoming digitized, such as India, surveillance can be regarded as a source of protection and at the same time as a tool of control (Rao, 2020). This study will demonstrate that a transparent and accountable surveillance regime is urgently needed by studying the development of surveillance laws, judicial interventions, and international best practices in this area. The results will assist the policymakers, legal experts and the judicial system in establishing more balanced policies that will not only consider the interest of national security but also take into consideration the constitutional right of the individual who has a right to their privacy. Finally, the paper is also of the opinion that protecting privacy is not a question of opposition to technological advancement, but rather a matter of making sure that the technological management is consistent with the values of justice, dignity, and freedom that are inherent in the Indian Constitution (Sen, 2022).

2. Literature Review

Electronic surveillance and the right to privacy relationship has been a subject of numerous debates in legal, philosophical, and technological literature. The effect of digital surveillance on civil liberties and the degree to which the legal frameworks can protect the rights of citizens in the age of data governance have been discussed by scholars. The current literature review focuses on important sources that have influenced the scholarly and policy discourse on surveillance and privacy in India, and the world at large.

2.1 Conceptual Foundations of Surveillance and Privacy

The term in its widest conception is surveillance, the systematic gathering, regulation, and control of information regarding people or groups, especially by the government or companies. One of the first conceptualizations regarding the idea of surveillance as a way of power and social control was the Panopticon theory suggested by Michel Foucault (1977). His analogy of being watched all the time describes the survival of surveillance by the person, which results in self-control of actions. This theoretical basis is applicable in the digital era where extensive data gathering forms an unseen but effective process of control (Foucault, 1977).

Privacy on the contrary has evolved as an ethical and legal term. Privacy was conceptualized as the right to be left alone (Warren and Brandeis 1890) and people were said to have the rights and dignity of being left alone In contemporary democracies, it was argued that privacy had been extended to the informational privacy the right to control personal information and its utilization. According to Solove (2008), privacy is not just about secrecy but it is about guarding people against power imbalances that information control has established. These are the theoretical concepts that help to explain the concept of privacy as a dynamic human right especially in the digital societies.

2.2 Surveillance and Privacy in the Indian Context

On the Indian side, the historical and legal evolution of surveillance systems has been critiqued by a number of scholars. Mehta (2018) follows the history of surveillance legislation in India back to the colonial era, claiming that the Indian Telegraph Act, 1885, formalized a culture of executive discretion that remains active in the contemporary systems. She observes that there has been no legislative or judicial check to the powers of the State to have wide interception powers. Equally important, Bhattacharya (2020) points out that the surveillance system in India has been mainly driven by executive orders and departmental circulars, as opposed to parliamentary law, which compromises accountability to the populace. In his book Digital Surveillance and the Indian State.

Rao (2020) explains that national security issues that emerged following the 2008 attacks in Mumbai hastened the development of digital surveillance systems, including the Central Monitoring System (CMS) and NATGRID. According to Rao, these systems are a change of target surveillance to mass surveillance, where the data is gathered randomly and is stored permanently. This author proposes more rigorous transparency policies and judicial permission prior to interception, which is congruous with the proportionality principle, which was developed in the Puttaswamy ruling (2017).

Bhatia (2021) offers constitutional insight, highlighting the difference between the recognition of privacy as a basic right in India and the lack of legal protections. He states that, although Puttaswamy v. The notable case of Union of India (2017) did not allow a thorough system of privacy protection to be adopted. Bhatia suggests the creation of an independent oversight authority that would control the

requests to the surveillance and could provide accountability of the executive authorities.

Narain (2019) also makes another great contribution to the topic, discussing how technologies like Aadhaar and face recognition have reinvented the world of surveillance. She explains that the Aadhaar system poses new vulnerability because the gathering of biometric and demographic data has not given citizens much control over how their data is used and disclosed. Narain argues that the Indian legal system does not have evident data retention boundaries and thus there is no easy way of ensuring that surveillance has proportionality and necessity.

2.3 Comparative and Global Perspectives

The surveillance and privacy debate has also taken a new form internationally by both in the courts and policy. Richards (2019) talks about how the Fourth Amendment is applied in the United States as a way of balancing between privacy and security and this discussion is after the USA PATRIOT Act (2001). He notes that even though U.S. courts have sometimes supported surveillance programs based on the grounds of national security, they have also strengthened the requirement of warrants and judicial checks on the same.

Privacy protection, especially in the area of transparency, accountability, and data minimization, is a high standard in the General Data Protection Regulation (GDPR) of the European Union. The European Data Protection Board (2020) states that the surveillance that is conducted in accordance with GDPR should pass strict legality and proportionality tests. These international standards underscore the need to have procedural protections which can be customized by India to enhance its own model of data governance.

2.4 Emerging Themes in the Literature

Through the literature, a number of themes are similar. To begin with, the majority of the scholars are in agreement that surveillance in India is executive-based with little legislative scrutiny. Second, the increasing opinion is that judicial oversight and independent review mechanisms are necessary to avert the abuse of power (Bhatia, 2021; Rao, 2020). Third, the Digital Personal Data Protection Act, 2023, although a positive step, has been criticized because of extensive exemptions of government agencies (Kumar, 2023). It is an indication of a long-standing disproportion between the interests of the state and the rights of citizens.

Fourth, another way in which the literature supports the interim report is the existence of a technological gap between law and practice. With the ever-evolving digital systems that are quicker than the current law, surveillance processes are taking place within a grey zone of the law. Lastly, a new understanding that privacy is not a one-sided right but rather should be weighed to valid societal interests is developing. Nevertheless, according to scholars, such a balance should be established by legal restrictions and proportions, as well as accountability, instead of executive discretion, which is not regulated (Narain, 2019; Bhattacharya, 2020).

2.5 Identified Research Gap

Though the available literature provides very useful information on the surveillance practices and constitutional jurisprudence in India, one can still feel a significant gap in the connection between a legal analysis and technological development. A majority of the literature is concerned with either the legal or the technical operation of the surveillance systems, yet few of them have endeavored to bridge the gap between the two. Moreover, there has not been a comparative analysis done on the standards of surveillance in India with other democratic jurisdictions.

This study seeks to fill that gap by offering an analytical, critical examination of the development of electronic surveillance standards in India and how they have adapted to constitutional privacy protection, and what the rest of the world can learn. The study will aim to contribute to the current policy discussion on how India can develop a rights-based, clear, and accountable surveillance system, which will not interfere with national security or personal liberty.

3. Research Methodology

3.1 Research Design and Approach

The research methodology that shall be adopted in this study is the doctrinal and analytical research approach which is most appropriate in the research on law and constitutional research. The methodology used by the doctrinal approach is a logically structured study of the current laws, judicial rulings, constitutional clauses, and policy statements in India concerning electronic monitoring and the right to privacy. In this manner, the study will seek to explain the development and application of the principles of the law and whether they comply with the constitutional protections of privacy and liberty.

The critical element is the assessment of the sufficiency, uniformity and efficiency of the Indian surveillance system in terms of reviewing statutory laws and judicial logic. Since the topic involves both legal interpretation and technological developments, the study integrates doctrinal legal analysis with policy and comparative perspectives, offering a multidimensional understanding of surveillance governance.

This research is qualitative in nature, emphasizing interpretation over quantification. It does not rely on

numerical data or statistical analysis but instead draws insights from legal texts, judicial reasoning, and secondary literature. The qualitative nature allows for depth, critical evaluation, and context-sensitive analysis rather than mere measurement.

3.2 Nature and Scope of the Study

The scope of this research extends to the **Indian legal and constitutional framework** governing electronic surveillance, while also examining **global benchmarks** from democratic jurisdictions such as the **United States** and the **European Union**. The study covers:

1. **Primary legal sources** such as constitutional provisions (Articles 19 and 21), legislative enactments (Indian Telegraph Act, 1885; Information Technology Act, 2000; Digital Personal Data Protection Act, 2023), and judicial pronouncements (*Kharak Singh v. State of U.P.*, *PUCL v. Union of India*, *Justice K.S. Puttaswamy v. Union of India*).
2. **Policy frameworks and institutional mechanisms** like the Central Monitoring System (CMS), NATGRID, and Aadhaar.
3. **Comparative analysis** of international standards such as the U.S. Fourth Amendment, European Union's GDPR, and case law from the European Court of Human Rights (ECHR).

The research focuses primarily on India's evolving standards and practices of surveillance post-2000, when digital communication and cyber laws became central to governance. The temporal scope thus spans roughly from 2000 to 2025.

3.3 Sources of Data

This study relies on both **primary** and **secondary** sources of data.

A. Primary Sources

1. **Statutes and Legislation:**
    - *The Constitution of India* (particularly Articles 19 and 21).
    - *The Indian Telegraph Act, 1885* and its rules.
    - *The Information Technology Act, 2000* and the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.
    - *The Digital Personal Data Protection Act, 2023*.
2. **Judicial Decisions:**
    - *Kharak Singh v. State of Uttar Pradesh* (1962).
    - *Gobind v. State of Madhya Pradesh* (1975).
    - *PUCL v. Union of India* (1997).
    - *Justice K.S. Puttaswamy v. Union of India* (2017).
3. **Policy Documents and Government Reports:**
    - Reports from the Ministry of Electronics and Information Technology (MeitY).
    - White papers on digital governance and surveillance frameworks.
    - Committee reports on data protection and privacy, including the *Justice B.N. Srikrishna Committee Report* (2018).

B. Secondary Sources

- Academic books, journal articles, and commentaries on privacy law, surveillance studies, and data protection.
- Publications from think tanks and legal research institutes such as the **Centre for Internet and Society (CIS)**, **Observer Research Foundation (ORF)**, and **Internet Freedom Foundation (IFF)**.
- Comparative literature from international databases like *HeinOnline*, *SSRN*, and *JSTOR*, covering privacy and surveillance jurisprudence.

3.4 Method of Data Collection

The study uses **doctrinal data collection methods**, primarily involving desk-based research. Information was gathered from **digital law databases** such as *Manupatra*, *SCC Online*, *LexisNexis*, and *HeinOnline*, along with government websites and policy archives.

The researcher identified and reviewed judgments, statutes, and rules relating to surveillance and privacy. Academic commentaries, journal papers, and policy briefs were examined to interpret how surveillance practices have changed over time and how courts have responded to privacy challenges.

Comparative material was collected from official European Union publications (such as GDPR guidelines), U.S. government archives, and decisions of the European Court of Human Rights.

3.5 Method of Analysis

The collected data was analyzed through **doctrinal interpretation and comparative analysis**. The doctrinal method was used to:

- Interpret legal texts in light of constitutional principles.
- Identify judicial trends in privacy jurisprudence.
- Evaluate how surveillance laws have evolved historically and function today.

Comparative analysis was applied to examine how other democratic jurisdictions, particularly the U.S. and the EU, have designed oversight mechanisms and balanced state surveillance with privacy rights. This helped identify gaps in India's system and generate reform recommendations.

The analysis also followed a **thematic framework**, organizing findings into categories such as:

1. Legal evolution of surveillance laws in India.
2. Judicial interpretation of privacy.
3. Technological expansion and executive discretion.
4. Comparative international safeguards.
5. Policy gaps and reform needs.

This thematic division ensured that the research remained focused and that conclusions were grounded in structured reasoning.

4. Results and Findings

The findings of this research emerge from a detailed analysis of India's legal framework on electronic surveillance, judicial interpretations of privacy, and a comparative study of global standards. The findings show that as much as India has gone a long way in its pursuit to appreciate the right to privacy as a constitutional right, the operation and legal guidelines that govern surveillance are poorly arranged, outlived and loosely controlled. The paper finds five significant thematic results:

4.1 Evolution of Surveillance Laws in India: Continuity without Reform

Among the main conclusions of this study, there is the continuity of Indian surveillance system historically that continues to use the laws that existed during the colonial times. This Indian Telegraph Act of 1885 has remained the legal basis of communication interception even in the age of communication that is more digital. The technology that transformed the telegraph to the internet notwithstanding, the legal reasoning behind the issue is the same the State still retains wide authority to intercept messages in the name of "public safety" or in the name of a public emergency. Likewise, the Information Technology Act, 2000, and the IT (Procedure and Safeguards to Interception, Monitoring and Decryption of Information), 2009, increased these powers to digital communication. That being said, the Act does not include clear protections, including prior court permission, minimality of data, or some form of independent supervision (Rao, 2020; Mehta, 2018). This shows a gap in the law: the laws originally created to have a very limited focus (in analog communications) are being overstretched to facilitate the sophisticated surveillance of the digital world. Consequently, India has a state-centric legal architecture as opposed to a rights-based legal architecture, which permits executive agencies to conduct surveillance activities with a wide discretion.

4.2 Judicial Recognition of Privacy: A Progressive Yet Incomplete Safeguard

The second major finding concerns the judiciary's evolving stance on privacy. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017) represents a constitutional milestone. The Court emphasized that privacy is integral to dignity and liberty under Article 21 and established the three-fold test of legality, necessity, and proportionality for any restriction on privacy *(Supreme Court of India, 2017)*.

However, the findings reveal a significant gap between judicial recognition and executive implementation. Despite the Puttaswamy ruling, most surveillance programs — such as the Central Monitoring System (CMS) and NATGRID continue to operate under executive orders without parliamentary or judicial oversight *(Bhatia, 2021)*.

Further, the Court's judgments in cases like *PUCL v. Union of India* (1997) introduced limited procedural safeguards such as Review Committees, but these bodies remain internal to the executive. They do not provide independent scrutiny, thereby weakening the practical enforcement of privacy rights. The result is a situation where privacy enjoys constitutional legitimacy but not operational enforcement. Citizens, therefore, lack an effective remedy against unlawful or arbitrary surveillance.

4.3 Expansion of Surveillance Infrastructure and the Role of Technology

The third major finding highlights the rapid technological expansion of surveillance mechanisms in India. Over the last two decades, the State has developed several digital monitoring systems, including the Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and NATGRID, that enable centralized interception and analysis of communication data *(Choudhury, 2023)*.

These systems increase the ability of the investigation but they also blur the line between the target and mass surveillance. Telecommunications networks can be accessed directly through CMS without service providers knowing it, which removes a crucial level of responsibility. In the same way, biometric data such as Aadhaar-based authentication and facial recognition systems are stored in high quantities, and they can be used again to conduct surveillance without the proper consent or disclosure (Narain, 2019). The results also indicate that the policy of data storage and retention is obscure and ambiguous. Indian regimes have no codified restrictions on the length of time that surveillance data should be kept, unlike GDPR-compliant regimes, where the state should only keep data as long as it is necessary. This in turn increases the chances of abuse, unauthorised access or profiling. This is a technological aspect that shows that the surveillance regime in India is growing at a higher rate than the legal protection and there is structural imbalance between the power of the state and the autonomy of the individual.

4.4 The Digital Personal Data Protection Act, 2023: Promise with Limitations

The study concludes that the Digital Personal Data Protection Act (DPDP), 2023, is a good move in the right direction in regulating the use of personal data. It formalizes the principles of information in data consent, limitation of purpose and accountability. Nonetheless, it has very little to play when it comes to state surveillance.

The DPDP Act gives the government exemptions under Section 17 in the name of national security, public order, or good relations with foreign states (Kumar, 2023). This broad exemption clause effectively places government surveillance outside the purview of the law. As a result, while private entities are subject to data protection obligations, state agencies are not held to the same standard.

Furthermore, the Act lacks provisions for independent data protection authorities with judicial powers. The Data Protection Board envisioned under the Act operates under executive control, undermining its independence. Therefore, while the Act enhances individual data rights in theory, it does little to address the core problem of unchecked government surveillance.

This reinforces the finding that India's approach remains asymmetrical, strict regulation for private entities but wide latitude for the State.

4.5 Comparative Insights: Lessons from Global Democracies

The comparative analysis reveals that other democratic jurisdictions have developed more transparent and accountable surveillance systems.

In the United States, judicial warrants are required for surveillance under the Fourth Amendment, and courts have limited executive powers through rulings such as *Carpenter v. United States* (2018). The Foreign Intelligence Surveillance Court (FISC) is a specialized court that offers a review and approvals of surveillance requests (Richards, 2019). The strong privacy protections in the European Union are defined by the General Data Protection Regulation (GDPR) and the ruling of the European Court of Human Rights (ECHR). The principle of proportionality of GDPR means that the surveillance should be required, lawful, and must be controlled by an independent authority (European Data Protection Board, 2020). When compared to these models, India does not have independent judicial authority and post-surveillance accountability. Transparency report, citizen notification procedures and parliamentary reviews of the surveillance orders are not published. What follows is a structural opaqueness that is a contradiction of the democratic checks and balances elsewhere.

4.6 Summary of Key Findings

Finding Area	*Observation*	*Implication*
Legal Framework	Outdated laws like Telegraph Act still govern modern surveillance.	State-centric control with limited rights protection.
Judicial Safeguards	Privacy recognized constitutionally but not institutionally enforced.	Weak practical protection for citizens.
Technological Expansion	Rapid growth of digital surveillance systems.	Potential for mass data misuse and privacy erosion.
Data Protection Law	DPDP Act excludes state agencies.	Regulatory asymmetry between citizens and government.
Comparative Standards	EU and U.S. have stronger oversight mechanisms.	India needs judicial and legislative reforms.

4.7 Overall Interpretation

As the general conclusion, the surveillance regime in India is not changing in ways enough to be constitutionally aligned. Although the legal and

institutional frameworks have not progressed to the same level as the judicial recognition of privacy since 2017, legislative improvements in this area have not been as significant. There is still a lack of balance between privacy and security as the State still has an expansive power with few checks. Essentially, India is at a crossroad; one is the direction of democratic accountability and rights-based governance and the other is the direction of unregulated executive surveillance. The study indicates that until India changes its surveillance legislation in line with the requirements of legality, necessity and proportionality, the constitutional promise of privacy will be mere symbols without actual content.

5. Discussion

As the general conclusion, the surveillance regime in India is not changing in ways enough to be constitutionally aligned. Although the legal and institutional frameworks have not progressed to the same level as the judicial recognition of privacy since 2017, legislative improvements in this area have not been as significant. There is still a lack of balance between privacy and security, as the State still has expansive power with few checks. Essentially, India is at a crossroads; one is the direction of democratic accountability and rights-based governance, and the other is the direction of unregulated executive surveillance. The study indicates that until India changes its surveillance legislation in line with the requirements of legality, necessity, and proportionality, the constitutional promise of privacy will be mere symbols without actual content.

5.1 Privacy as a Constitutional Value: Between Recognition and Realization

Justice K.S. Puttaswamy v. the acknowledgement of the right to privacy. Union of India (2017) was a milestone towards harmonization of the Indian constitutional law to the international human rights standards. The judgment pointed to the fact that privacy is not a right that is personal but rather a crucial part of human dignity, freedom and autonomy. It determined the legality of the three-part proportionality test, necessity and proportionality to be the standard of any state intrusion into privacy. Nevertheless, the results of the presented research point to the fact that the realization of this constitutional vision is not fully accomplished. The fact that the Indian Telegraph Act (1885), and the Information Technology Act (2000) remain operative, speaks of a greater structural issue: the jurisprudence of privacy in India has developed far outpacing its statutory and institutional provisions. The lack of connection generates a paradox in the constitution where people are a right on paper but have ineffective means to exercise or defend it in practice. The constitutional morality principle as stated by Navtej Singh Johar v. Union of India (2018), is an enforcement of state institutions to pursue constitutional values, and not majoritarian or political considerations. However, as demonstrated by the surveillance practices in India there is a bias towards executive comfort instead of constitutional responsibility. Therefore, privacy has not only been identified in courts, it is institutionally weak.

5.2 The Security Privacy Paradox: The State's Expanding Role

One of the key themes that stands out in the literature and findings is the security-privacy paradox, the role of the State in ensuring that the citizens are not threatened by the outside forces is in conflict with the role of ensuring that the State does not invade the privacy of its citizens. Electronic surveillance, as a policy by the Indian government, is based on the reasons of national security, terrorism and public safety. This is why these reasons are most definitely valid. Nevertheless, we have to remember that, although Foucault (1977) in his theory of the Panopticon suggests that the power of surveillance is an easy concept to transform into protection rather than control. Examples of this two-fold system are the Central Monitoring System (CMS) and NATGRID. On the one hand, they contribute to the efficiency of law enforcement; on the other, they lead to transparent mass surveillance. There is no legal permission to conduct surveillance, and no parliamentary checkpoint, which implies that surveillance is mostly in the discretion of the executive (Rao, 2020; Bhattacharya, 2020). However, in contrast, the global democracies such as the United States and the European Union provide checks via judicial warrants, separate oversight bodies, and regulators of data protection. The absence of such mechanisms in India represents the trust-based framework of surveillance, wherein the population is supposed to put their trust in the discretion of the State instead of having enforceable protection. This system, though effective during a state of crisis, is contrary to the spirit of the constitutional democracy in which the authority of the state should never be out of legal reach.

5.3 Technological Governance and the Risk of Mass Surveillance

The increase in technology has transformed the concept of surveillance into proactive and preventative surveillance rather than the focused investigation. Technologies such as Aadhaar, facial recognition applications or data analytics applications enable the State to accumulate extremely high levels of personal data, which is often not the intended use of that data collection (Narain, 2019). This is a trend that is described as the so-called function creep phenomenon by scholars who believe that the data gathered to serve a certain purpose (welfare delivery) is used against them (surveillance or profiling). The results indicate that India has no purpose limitation and data

minimization principles, which are the fundamental principles of international data protection, such as the GDPR (European Data Protection Board, 2020). In as much as the Digital Personal Data Protection Act, 2023 proposes the introduction of the rights of the individual data, it still does not address the exemption of government surveillance operations. Such exemption justifies a chain of privacy: the data of the citizens should be controlled when utilized by corporations and not when collected by the State. Practically, the data protection regime in India empowers, and not affects, the surveillance state (Kumar, 2023). The implication that is more general is the fact that unchecked technological governance can turn India into a surveillance society that is data-driven, where individual agency is lost to the power of algorithms and unseen surveillance.

5.4 Comparative Constitutional Learning: Toward a Rights-Based Model

The international comparison of structures offers valuable lessons for Indian reform. Despite its extensive national security infrastructure, the United States has judicial checks and balances, including the Foreign Intelligence Surveillance Court (FISC) and the requirement for a warrant to intercept data (Richards, 2019). In the same vein, the European Union GDPR and ECHR jurisprudence require the surveillance to be highly subject to the tests of legality, proportionality, and necessity (European Data Protection Board, 2020). The examples indicate that democratic surveillance can only exist in an institutional system of checks and balances. The accountability is ensured by independent data protection authorities, voluntary reports about transparency, as well as post-surveillance notifications. There are no such institutions in India, and this makes people reliant on judicial redresses that are mostly not preventive but reactive. The comparative understanding also shows that privacy is not anti-security right; rather, it is a system of restraint that makes the state power fall within the constitutional considerations. Therefore, a rights-based approach to surveillance is not a threat to security but an enhancement of democracy.

5.5 Institutional and Legislative Gaps

The results highlight structures of profound institutional flaws in the surveillance governance in India. To begin with, there exists no unified law that brings together all types of electronic surveillance in a single set of laws. Rather, the Telegraph Act, the IT Act, and different rules and regulations have provisions that are not unified, which leads to ambiguity. Second, there is no independent oversight body, which means that the surveillance requests are checked only by the executive committees, which are frequently chaired by the senior bureaucrats. This brings a conflict of interest, since the same body approves and checks on its actions. Third, surveillance orders are not subject to the pre-judicial approval. Most liberal democracies, on the contrary, consider judicial pre-authorization a non-negotiable protection. Lastly, there is no legal requirement of transparency citizens do not know when they are being watched, and no statistics of surveillance are being given by the government on an annual basis. Such institutional lapses demonstrate a culture of non-transparent government, in which surveillance has become the new administrative role instead of an exceptional intrusion subject to legal scrutiny.

5.6 The Need for Constitutional Accountability

Fundamentally the discussion of the issue of surveillance and privacy is not just a legal issue but also a constitutional and philosophical issue. The Indian Constitution envision the harmony between the liberty of a person and the safety of the group. The results show that now this balance is inclined much toward the latter. Privacy should comply with institutional accountability in order to make it meaningful. Surveillance activities of the State must also be constrained by constitutional morality, whereby the security goals must not dominate the liberty and dignity. Just like the Supreme Court in Maneka Gandhi v. Union of India (1978), "procedure laid down by law" should be correct, equitable, and sensible. The application of this criterion to the surveillance would mean that any limit to privacy has to be supported by open procedures and external checks and balances. To ensure that the constitutional democracy in India still works in the digital era, it needs to shift the principles of the constitutional democracy on surveillance to a rights-based form of surveillance, which is based on the law, informed by necessity, and is open to review at all times.

5.7 Summary of Discussion

Theme	***Interpretation***	***Implication***
Constitutional Recognition	Privacy is legally recognized but not practically enforced.	The gap weakens constitutional accountability.
Security–Privacy Balance	State power dominates privacy protection.	Need for stronger oversight and proportionality.
Technological Expansion	Data systems enable mass surveillance.	Legal safeguards lag behind technological growth.
Comparative Standards	EU and U.S. models ensure	India must adopt similar

	independent review.	oversight institutions.
Constitutional Morality	Rights must guide governance, not convenience.	Calls for a rights-based surveillance framework.

5.8 Conclusion of Discussion

In conclusion, the discussion reaffirms that India stands at a critical juncture in its digital constitutional evolution. The country has achieved a jurisprudential victory in recognizing privacy as a fundamental right, but it has yet to achieve a practical transformation in how surveillance is conducted. The challenge lies not in abolishing surveillance but in regulating it through clear, transparent, and accountable procedures.

Electronic surveillance, when guided by legality and oversight, can coexist with privacy. But when left unchecked, it risks eroding the very democratic values that the Constitution seeks to protect. The next step for India is to translate judicial ideals into institutional design through comprehensive legislation, independent oversight, and adherence to the principles of necessity and proportionality. Only then can the evolving standards of surveillance be reconciled with the enduring promise of privacy in a constitutional democracy.

6. Conclusion and Recommendations

6.1 Conclusion

The current paper has critically analyzed the history of electronic surveillance and its overlap with the right to privacy in India. As the analysis shows, the surveillance system in India, despite the wide range and technological advancement, is legally divided and constitutionally incoherent. The main paradox that was revealed during the research is the fact that the protection of privacy, which is constitutionally guaranteed, is not yet being institutionally provided.

The Indian surveillance history shows that it is not undergoing any substantive reform. The Indian Telegraph Act, 1885, still gives an omnivorous power of interception to the State, and the Information Technology Act, 2000, adds digital communication, but fails to provide appropriate procedural protection. Though these laws have been adjusted to the new technologies, their logic, which is to emphasize the state over individual rights, has not changed (Mehta, 2018; Rao, 2020).

The judicial system has also been transformative, especially with the Justice K.S. Puttaswamy v. Union of India (2017), in which privacy was declared to be one of the fundamental rights inherent in human dignity and liberty. Nonetheless, in spite of this constitutional milestone, there have been no legislative reforms to match the judgment, which is limiting the practical implications of the judgment. In many ways, surveillance initiatives, including the Central Monitoring System (CMS), NATGRID, and facial recognition programs, are predominantly executed by executive orders without much external control (Bhatia, 2021; Choudhury, 2023).

More on this, the Digital Personal Data Protection Act, 2023, which is the progressive law regarding the protection of personal data, offers wide exemptions to government agencies based on national security (Kumar, 2023). This unequal treatment of the regulation of private and state actors sabotages the constitutional pledge of equality and accountability. The outcome is an imbalance in the structure- citizens' data is safeguarded against the misuse of the magnitude of the private, but it is not under attack by the state. The comparative analysis highlights that democratic countries such as the United States and the European Union have established effective measures in the oversight that put security and privacy into balance. The U.S. Foreign Intelligence Surveillance Court (FISC) and the GDPR policy implemented in the EU prove that legal transparency, judicial authorization, and post-surveillance accountability can be reconciled with the national security necessity (Richards, 2019; European Data Protection Board, 2020). Conversely, the Indian system is still opaque, with the executive authorities having enormous discretionary powers, to which they have neither judicial nor parliamentary scrutiny.

This paper, therefore, concludes that the evolving standards of electronic surveillance in India are not well in tandem with the constitutional values. The legal framework that is in place is that of state prerogatives as opposed to autonomy on the part of individuals as a way of governance based on administrative convenience and not democratic accountability. This imbalance may, otherwise, turn India into a surveillance democracy - a country where freedom is on paper but is violated in practice. Thus, a reform in the sphere of rights-based surveillance, which will reconcile the interests of security with the right of the individual to his/her privacy, is urgently required. The second part offers recommendations to help inform such reform.

6.2 Recommendations

1. Enact a Comprehensive Surveillance Regulation Act

India seriously requires a specific Act that puts together all the provisions concerning surveillance, interception as well as monitoring. This act on Surveillance Regulation must:

- Define key terms such as "surveillance," "monitoring," and "data interception."
- Specify the conditions under which surveillance may be authorized.
- Include procedural safeguards such as prior judicial approval, periodic review, and record-keeping.
- Ensure transparency in surveillance activities by having parliamentary reporting.

This legislation would provide a coherence to the existing haphazard laws and make the framework as close to the constitutional and international norms as possible

2. Introduce Judicial Authorization for Surveillance Orders

No surveillance should occur without **prior judicial authorization**. Presently, the power to issue interception orders lies with executive authorities, typically the Union or State Home Secretary. This arrangement violates the principle of separation of powers. Judicial authorization would ensure **independent scrutiny** and prevent arbitrary or politically motivated surveillance.

A **special surveillance bench** or an **independent judicial tribunal**, similar to the **U.S. FISC**, can be created to review and authorize requests confidentially but impartially.

3. Establish an Independent Oversight Authority

India should establish an Independent Data and Surveillance Oversight Authority to monitor compliance with privacy standards. This body should:

- Operate autonomously from the executive branch.
- Have powers to audit surveillance agencies.
- Publish annual transparency reports summarizing the number and nature of surveillance requests.
- Provide a citizen complaint mechanism for privacy violations.

This institutional innovation would transform oversight from internal bureaucratic review to **independent constitutional supervision**.

4. Embed Proportionality and Necessity Tests in Law

Legislation must codify the **proportionality principle** articulated in *Puttaswamy (2017)*, requiring that surveillance be:

1. **Lawful:** based on clear legal authority;
2. **Necessary:** justified by a legitimate state objective;
3. **Proportionate:** minimally intrusive and narrowly tailored.

These criteria should be explicitly written into the law, ensuring that surveillance is not used for general monitoring but for specific, demonstrable threats. Regular judicial review must confirm whether these tests were satisfied.

5. Strengthen the Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act** must be amended to include **government surveillance activities** within its regulatory scope. Current exemptions granted to public authorities undermine its credibility. The **Data Protection Board** should be made **independent and quasi-judicial**, with powers to summon officials, review interception orders, and impose penalties for misuse.

Additionally, the Act should include:

- **Data retention limits** (automatic deletion after defined periods).
- **Purpose limitation clauses** to prevent repurposing of collected data.
- **Right to notification** once surveillance has concluded, wherever possible.

6. Promote Transparency and Accountability

Transparency does not mean disclosing operational details but ensuring **public awareness** and **legislative oversight**. The government should be mandated to:

- Publish **annual transparency reports** detailing the number of interception orders issued and their justifications.
- Enable the **Parliamentary Standing Committee on Home Affairs** to review surveillance activities annually.
- Encourage **public consultations** before introducing new technologies such as facial recognition systems.

Such measures would strengthen public trust and reduce fears of misuse.

7. Foster Privacy Literacy and Technological Ethics

Public understanding of digital rights remains limited. Government agencies, educational institutions, and civil society organizations should collaborate to promote privacy education and data ethics. Awareness campaigns can help citizens understand their rights, report abuses, and demand accountability.

In addition, law enforcement personnel and bureaucrats involved in data management must undergo mandatory training on privacy principles, legal safeguards, and responsible data handling.

References

Books and Journal Articles

1. Bhatia, G. (2021). *Privacy and Surveillance in the Age of Digital Governance.* Oxford University Press.
2. Bhattacharya, P. (2020). The surveillance state and the right to privacy in India. *Economic and Political Weekly, 55*(3), 45–52.
3. Choudhury, R. (2023). State surveillance and data protection in India: Policy and practice. *Indian Journal of Constitutional Studies, 18*(2), 23–40.
4. European Data Protection Board. (2020). *Guidelines on data protection and surveillance under GDPR.* Retrieved from https://edpb.europa.eu
5. Foucault, M. (1977). *Discipline and punish: The birth of the prison.* Vintage Books.
6. Kumar, A. (2023). The Digital Personal Data Protection Act, 2023: Promise and limitations. *Journal of Indian Law and Policy, 5*(1), 10–25.
7. Kumar, R., & Sharma, N. (2022). National security and privacy in the digital era. *Indian Journal of Law and Technology, 16*(2), 45–62.
8. Mehta, R. (2018). Colonial legacies and modern surveillance laws in India. *Indian Law Review, 4*(1), 33–48.
9. Nair, V. (2021). *Information Technology Act and the evolution of cyber law in India.* Cambridge Scholars Publishing.
10. Narain, P. (2019). Aadhaar, privacy, and the expanding state surveillance network. *Law and Society Review, 53*(4), 72–89.
11. Narain, P. (2020). Privacy in the post-Puttaswamy era: Constitutional and policy challenges. *NUJS Law Review, 13*(1), 101–119.
12. Ramanathan, U. (2018). The right to privacy: From Puttaswamy to practice. *Seminar Journal, 709*, 30–35.
13. Rao, S. (2020). *Digital surveillance and the Indian state: Law, policy, and accountability.* Routledge.
14. Richards, N. M. (2019). *Intellectual privacy: Rethinking civil liberties in the digital age.* Oxford University Press.
15. Sen, A. (2022). Technology, democracy, and the limits of state power. *Contemporary Indian Policy Review, 12*(3), 15–27.
16. Singh, R., & Bhattacharya, T. (2021). Governance, data, and surveillance: Rethinking privacy in India. *Asian Journal of Law and Policy, 9*(2), 19–37.
17. Solove, D. J. (2008). *Understanding privacy.* Harvard University Press.
18. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Judicial Decisions

1. *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (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*, AIR 1975 SC 1378 (India).
4. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).
5. *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 (India).
6. *Maneka Gandhi v. Union of India*, AIR 1978 SC 597 (India).
7. *Carpenter v. United States*, 585 U.S. (2018) (U.S. Supreme Court).

Statutes and Policy Documents

1. The Constitution of India.
2. The Indian Telegraph Act, 1885 (India).
3. The Information Technology Act, 2000 (India).
4. The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 (India).
5. The Digital Personal Data Protection Act, 2023 (India).
6. Ministry of Electronics and Information Technology (MeitY). (2018). *Report of the Committee of Experts on Data Protection (Justice B. N. Srikrishna Committee Report).* Government of India.
7. Organisation for Economic Co-operation and Development. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* OECD Publishing.
8. United Nations. (2014). *Resolution on the Right to Privacy in the Digital Age (A/RES/68/167).* United Nations General Assembly.

that might occur from the use, interpretation, or reliance upon the information, methods, instructions, or products discussed in the journal's content.

****