IMPACT OF SURVEILLANCE LAWS ON PRIVACY RIGHTS IN INDIA

Manjari Vaishnav, BA LLB, Bharati Vidyapeeth (Deemed to be University), New Law College, Pune.

ABSTRACT

This paper examines how the legal regime of surveillance is transforming worldwide and encroaching upon the very foundation of the right to privacy in India. The spread and increasing reach of digital technologies and surveillance have exposed the weaknesses and challenges of the Indian legal system. Using three major statutory instruments, namely the Indian Telegraph Act 1885, Information Technology Act 2000, Aadhaar Act 2016, and Digital Personal Data Protection Act 2023, this article analyzes the conflict between state interests in national security and individuals' right to privacy, as established in Justice K.S. Puttaswamy v. Union of India. It discusses operational practices, judicial interventions, upcoming technologies like "spyware" and face recognition, and the current lack of effective regulation. Additionally, it provides an international perspective, comparing values with other foreign laws and India's practices. The panel also highlights critical areas requiring urgent attention. It offers several recommendations, including revising statutes, establishing independent regulatory agencies, and empowering the judiciary to exercise greater oversight. Furthermore, it emphasizes the importance of comprehensive public consultation before rights guaranteed in the constitution are upheld in the digital era.

Keywords: Surveillance, Privacy Rights, India, Legislation, Digital Governance.

I. INTRODUCTION

India's current pace of digital transformation is remarkable, marked by unprecedented technological growth and large-scale government initiatives like Aadhaar, Digital India, and extensive e-governance efforts that serve people across different socio-economic backgrounds. As big data analytics, artificial intelligence, and widespread internet connectivity develop, the collection and processing of personal data have reached levels previously unimaginable for both government and non-government entities. However, this digital revolution has also heightened threats to privacy and civil liberties. Modern surveillance tools, including biometric databases, facial recognition systems, and invasive spyware, enable the state to monitor, track, and influence individuals in ways that go beyond physical and legal boundaries of the past. While maintaining order and national security has always been a key role of the government, current laws, many dating back to colonial times like the Indian Telegraph Act of 1885 — which restricts the use of telegraphs without legal permission and recent digital personal data protection laws of 2023, often grant the authorities broad and poorly defined surveillance powers with minimal oversight. These expansive powers clash with the fundamental right to privacy, which has been a cornerstone of Indian constitutional democracy since the Supreme Court recognized it in the Puttaswamy judgment. In this article, the author critically examines how surveillance laws have evolved and their impact on privacy rights, highlighting the urgent need to establish stronger safeguards and independent accountability to define the limits of state power and individual freedoms amid the many technological challenges today.

II. LEGAL FRAMEWORK GOVERNING SURVEILLANCE IN INDIA

Indian Telegraph Act, 1885

The Indian Telegraph Act is the oldest and most fundamental surveillance law in India, granting both the Central and State Governments broad powers to intercept communications. It includes a provision (5(2)) allowing interception or detention of messages during a public emergency or in the interest of public safety, especially when necessary to protect India's sovereignty and integrity, maintain public order, or prevent crimes.[1] The Act's definition of telegraph is extensive, covering any signaling or imaging mechanism via electromagnetic or other means,

[1] Indian Telegraph Act, 1885, § 5(2) (India).

which means it could potentially apply to many modern technologies.

Key concerns about the Act include:

1. Colonial Legacy: It was enacted under British rule, and its broad, non-specific provisions have largely remained unchanged, often with little modernization.

2. Vague Terminology: Words like "public emergency" and "public safety" are not clearly defined, leading to subjective interpretation by authorities and potential misuse of power.

3. Lack of Control: The executive authority predominantly grants interception permissions, with limited procedural safeguards or independent judicial oversight, mostly documented through notifications and review committees. This raises significant risks of abuse.

The Information Technology Act, 2000 (IT Act)

As digital communications grow, the reach of surveillance has been extended to other forms of traditional telegraphs through the IT Act. Section 69 gives powers to the Central and State Governments to judge and give directions on interception, monitoring, and decryption of any information that is received or sent through computer means.[2] These powers can be used to ensure the interests of sovereignty, defence, security of the state, the maintenance of the state order, friendship relations between states, the prevention of crimes, or the investigation of crimes.

Major concerns:

1. Broader Scope: The IT Act, on the other hand, targets any communication and data in digital form as compared to the Telegraph Act, which only states that permission was necessary to intercept. The Telegraph Act only extended surveillance to print media but had no or very little control over any other form of communication.

2. Fewer Safeguards: The enabling rules (2009) confer the authorisation, review entirely to the executive branch with no compulsory requirement that it should be reviewed by the judiciary

[2] Information Technology Act, 2000, § 69 (India).

first.[3]

3. Intermediary obligations: Internet service providers and other intermediaries are obliged to help intercepting agencies and therefore must provide decrypted information or technical support, which poses additional privacy issues.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

The introduction of the Aadhaar Act envisioned effective distribution of government welfare to citizens by means of harnessing the identification of the residents in terms of biometric and demographic data.[4] Although its purpose is administrative effectiveness and selective benefits, the Act holds grave consequences in terms of privacy and spyware since:

1. Centralized Database Dangers: Pooling the biometric (fingerprints, iris scans) as well as demographic data in one massive database, increases the chances of misuse and data demographic data in one massive database increases the chances of misuse and data breaches, as well as unauthorized profiling.

2. Potential of Mass Surveillance: With several databases of the government and the private sector (banking, telecom, healthcare, etc.) feeding data to Aadhaar, the government gains the ability to increase surveillance and profile of people in various spheres.

3. Inadequate Protection of Privacy: Many drawbacks to the Aadhaar Act are rooted in the lack of sufficient protection of privacy. Many critics point to the insufficiency of the robust, independent institutional supervision of the Aadhaar Act and bode over the concentration of governance power to the Unique Identification Authority of India (UIDAI), whose independence has been questioned. Although the Supreme Court judgments of 2018 did not mandate Aadhaar in some cases, some people still feel there are a lot of security risks and infringement of their privacy.[5]

[3] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).
[4] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).
[5] J*ustice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2019) 1 SCC 1 (India).

Digital Personal Data Protection Act, 2023 (DPDPA)

The DPDPA may be considered the first extensive legal framework in India that seeks to protect personal data and lay down rules on legal processing. But its efficacy is seriously dented by wide-ranging exemptions granted to the government, particularly under Section 17.[6]

Important Characteristics and Issues:

1. Section 17 Exemptions: This section enables the Central Government to exempt any government agency or instrumentality of the government from the greater part of the Act if the government decides that such processing is required in the cause of sovereignty, integrity, security of the state, good relations with foreign states, public order, and controlling crime. The exemption range is very broad and can be invoked for quite uncertain reasons as the protection of a public order.

2. Lack of obligatory Independent/Judicial oversight: there is no mandatory independent or judicial oversight of such exemptions or data processing about surveillance-related activities, leaving government surveillance practices with minimal to no oversight.

3. Exemption and Consent and Notification Waivers: With the exemption in place, the data can be collected, processed, and even stored without the consent or notification of the user, and many of the more standard rights of a citizen, including the right to erasure and correction, can remain suspended with these agencies.

4. Unlimited Data Retention: The DPDPA does not contain any clear obligation by government agencies to delete or limit the storage of data performing exempted processing. Data that has been gathered can be put to wide-reaching profiling and monitoring without the customary data minimisation rules. The GDPR (European Union) Introduced to ensure that exceptions to processing national security are always proportional and necessary, the policy of the DPDPA, contrary to the GDPR (European Union) which provides the independence of oversight and the restriction of exemptions on national security, is to adopt an approach that gives discretion to the executive and instead considers individual safeguards. This creates a huge legal ambiguity

[6] Digital Personal Data Protection Act, 2023, § 17 (India).

and exposure to privacy violations of Indian citizens, as there are no proper counter-balances in terms of remedying the situation or otherwise providing transparency to the citizens of India.

III. CONSTITUTIONAL AND JUDICIAL EVOLUTION OF THE RIGHT TO PRIVACY

Early Jurisprudence

During the initial years of Indian independence in the 1950s, the Supreme Court was conservative in applying the concept of privacy as a legal right. In case M.P. Sharma v. Satish Chandra (1954),[7] the Court held in Satish Chandra that there was no right to privacy in the Constitution, which may be spelt out in Article 20 (3) or any other provision of the Constitution, and such rights needed to be spelt out in an express provision. In Kharak Singh v. State of U.P. (1963), this precedent was supported.[8] The majority once again refused to make privacy a fundamental right, describing it as a kind of right which could not be discussed in isolation, and where the interest of the State in investigation and law enforcement could be upheld as precedence over the interest of the citizen in privacy of personal life. These rulings largely exposed personal privacy to State infringement, as it was being safeguarded only by legislative or administrative measures, which subsequently were not found adequate to numerous methods of increased surveillance.

JUSTICE K.S. PUTTASWAMY (Retd.) v. UNION OF INDIA (2017)

With the path-breaking verdict on Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).[9] A paradigm shift occurred when a unanimous decision was passed by a bench consisting of nine judges of the Supreme Court, the right to privacy had been held to be an intrinsic part of the right to life and personality liberty under Article 21 of the Constitution, and in the liberties guaranteed by Part III of the Constitution. The Court upheld the position that privacy cannot be viewed separately from other integral elements of human rights (such as dignity, autonomy, and democratic freedoms), nor the protection against State action, but also unreasonable interference by individuals and private organizations.

[7] *M. P. Sharma v. Satish Chandra*, [1954] SCR 1077 (India).
[8] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).
[9] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

Above all, the "proportionality test" was determined by the judgment which, taken together, required the restriction on privacy to at least:

1. be based on a clear legal basis

2. seek a legitimate aim of the State

3. be necessary and the least restrictive means

4. be proportional to the intended objective

Also, the Court emphasized the necessity of procedural protection, openness, and effective judicial checks in order to avert the capriciousness of executive authority. This historic decision has overturned Indian constitutional jurisprudence on privacy and brought a new wave of challenges to acts and acts of surveillance, and led to the construction of a body of principles on data protection and digital rights.

IV. SURVEILLANCE PRACTICES: TENSIONS WITH PRIVACY RIGHTS

Operational realities

Although in India, the Puttaswamy judgment established the constitutional right to privacy, surveillance in India is a part of the executive-oriented system that is thoroughly ingrained there. Rather than having a monumental reform, daily surveillance operations are mostly conducted by means of executive order, notification, and behind-the-scenes government actions. And in reality, such mechanisms are not subject to any significant external scrutiny. Major surveillance laws contain statutory ambiguity: they are usually written in broad language, using words with vague meaning, e.g., to "public order" or to "national security," meaning that governments have much leeway to interpret and exercise their interception powers. The transparency architecture is restricted: the processes that contemplate surveillance of data are, to a large extent, super-secret, and disclosures/reporting to the population / Parliament are practically non-existent. Chances of judicial pre-authorization or review in real-time are minimal, which results in the surface that ensures keeping the matter within control of government agencies, and, by association, not independently performed. Remedy systems in place in case of unlawful or excessive surveillance are very few and are hardly exercised, and continued free handing of state power. This constant skew between executive dominance and

external control is diminishing the proportionality, necessity, and procedural strictness required by the Supreme Court, and is also making it tough to categorize which functions are justifiable national security, and which are just simple overreach by the State.

Mass Surveillance and Case Studies

1. Aadhaar:

The Aadhaar system was also crucial to social welfare and e-governance, but its use has also been illustrative of the dangers of such large, centralised databases in the context of surveillance. Despite the decision by the Supreme Court known as Puttaswamy II that happened in the year 2018, which permitted Aadhaar to be constitutional, it imposed restrictions on its application, especially the loss of agency to make it mandatory to be linked to the use of private services.[10] The blanket adoption of Aadhaar, however, has brought incremental function creep, i.e., using it in ways never imagined, like say law enforcement, banking KYC, and mobile SIM registration. This, together with the frequent news of data leaks, unwarranted distribution, and insufficient remedy grievance, has left the doubt unanswered on the surveillance, profiling, and the threat of state and third-party access to the personal lives of citizens.[11]

2. The Pegasus Spyware Reveals:

The 2021 revelation that the spyware telephone Pegasus of the Israeli company Group NSO had reportedly been used by certain entities against Indian journalists, lawyers, human rights activists, and even politicians of the opposition highlights the grave consequences of unregulated surveillance through digital means.[12] These disclosures shed light on gaping shortcomings in both legislative control and state accountability. Though internationally and in the country, there was alarm, the reaction of the government was largely secretive, depending largely on national security exemptions, and thus prompting it to reject any serious discussions with the parliamentary or court oversight. The case of Pegasus eloquently demonstrates how the legal systems are not functioning effectively to curb the weaponization of surveillance as a

[10] J*ustice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, (2019) 1 SCC 1 (India).
[11] Ramanathan, U. (2019). The Aadhaar judgement: A critique. *Economic and Political Weekly*, *54*(1), 10–13.
[12] Centre for Internet and Society. (2021, August 2). *Pegasus in India: A legal explainer*. CIS-India. https://cis-india.org/internet-governance/pegasus-in-india-a-legal-explainer

tool to quell any dissent, and how democratic essentials have never had the protection they should.

3. Facial Recognition Technology:

There are broad privacy risks with the more and more deployment and utilisation of facial recognition technology by police and local governments across varied jurisdictions in the absence of specialised legislative guidelines and approval of the populace.[13] These technologies facilitate mass identification, tracking, and profiling of individuals in public and semi-public spaces, unlike targeted surveillance. This not only poses a challenge to the privacy enjoyed by information, but it also destroys the cocoon of anonymity that plays a critical role whenever people want to protest, demonstrate, or simply move around without having to worry about being profiled and/or grouped under the target list. The increasing evidence is that the implementation of such systems, especially in political times of unrest or demonstration, has a chilling effect on the citizens who want to express their dissent and debate freely.

Chilling Effect on the Civil Society

Indian democracy can feel the impact of the uncontrollable growth of the state surveillance machine. Surveillance, however, is increasingly pervasive and technically sophisticated; it creates what is called a chilling effect on civil society, such that in addition to virtual free speech, it discourages routine civic engagement, investigative reporting, human rights activism, and political activism.[14] The feeling of surveillance and profiling adjusts people and institutions to avoid stating dissenting opinions, reporters cover sensitive topics, and adopt an individual action rather than a communal one. This degree of self-regulation brings into play the very nature and perception of democratic participation and representative responsibility, where the scope of awareness and democratic dialogue is reduced. Lacking strong legislative changes, independent checks, and open protections, the growth of surveillance has the potential to endanger the very building blocks of constitutional democracy in India and silence the voices that give it its life and strength.

---

[13] Internet Freedom Foundation. (2022, June 15). *The creep of facial recognition in India*. https://internetfreedom.in/the-creep-of-facial-recognition-in-india/

[14] Amnesty International. (2022, April 28). *India: "Chilling effect" on freedoms as authorities use draconian laws to silence critics*. https://www.amnesty.org/en/latest/news/2022/04/india-chilling-effect-on-freedoms-as-authorities-use-draconian-laws-to-silence-critics/

V. OVERSIGHT DEFICITS AND ACCOUNTABILITY GAPS

One of the core weaknesses of the surveillance architecture that India operates is that it lacks strong, independent control and has no substantial accountability mechanisms. Under the existing legal framework, the executive agencies are granted broad and largely discretionary power to authorise interceptions, data monitoring, and surveillance on very general and ambiguously determined criteria, including those without particularly solid grounding, such as those of the maintenance of public safety or national security. More importantly, the system of prior judicial authorisation of an interception or surveillance request is not governed by law, a mechanism that is common across comparative constitutional systems as a means of controlling abuses of power. Rather, these authorisations are periodically reviewed by such ministerial or departmental committees and comprise only senior executive officials. This makes the process itself inherently circular, as the same branch of government pursuing the surveillance process is the branch of government that approves itself and monitors itself.

There are practically no checks and balances on these issues in parliament, and there is no transparency on this issue. A majority of executive orders, interception orders, and those activities related to surveillance are being withheld due to claims of confidentiality or sensitive information, and legislators and the general population cannot discuss the necessity or legality of such acts. Redress or challenge to those affected is a practically fanciful notion in the case of those on the receiving end of improper or in excessive surveillance; the secrecy of the process, the undisclosed nature of authorisations, the fact that targets will never know of the infringement, and will even less of the legal recourse means that those hapless enough to find themselves caught in the net are unlikely to bother to seek relief.[15]

These issues are additionally cemented under the Digital Personal Data Protection Act (DPDPA) 2023. Section 17 gives a wide berth to most of the fundamental provisions of the Act, including consent, data minimisation, and user redress when wide-ranging interests, including public order, national security, etc., are involved. Such exemptions do not get a vetting or reviewing power from any outside, judicial, or parliamentary institution. Not only does this legal design invite the concentration of surveillance and data-processing outlays into

[15] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Government of India.

the State, but buys statutory impediments to vindication or responsibility, which cumulatively serve to weaken the letter and the spirit of constitutional avenues of privacy protection.

VI. INTERNATIONAL AND COMPARATIVE PERSPECTIVES

The global constitutional democracies have in common principles of necessity, proportionality, legality, and independent review as the cornerstone of the regulation of surveillance. The de facto standard in privacy protection is the European Union General Data Protection Regulation (GDPR).[16] According to the GDPR, any restriction of data rights by State or private authorities has to be mandated by law, be necessary to pursue a legitimate aim, be preceded by a minimal limit, and always be under the control of an independent authority. Citizens possess the right to inform, the right to redress, as well as the right to appeal the illegal processing of information or monitoring to the courts.

In the United States, the Fourth Amendment to the Constitution embodies the idea that searches, seizures, and most forms of surveillance must be conducted by a judicial warrant issued in advance and upon probable cause.[17] The exceptions are treated very strictly and are construed against the law. Although this model is not free of controversy, central protection against executive abuse and the governance of surveillance authority not being used arbitrarily are the key safeguards provided in this model.

The resolutions of the United Nations General Assembly and the reports of the special rapporteurs confirm once again that surveillance has to meet the threshold of legality, necessity, and proportionality and that it should be complemented with redress and control by the international community.[18] In particular, the UN has demanded transparency, good control of abuse, and protection against mass surveillance operations contrary to democratic liberties.[19]

In these global standards, the Indian paradigm is deficient in content as well as procedural aspects. The lack of an independent review, the virtually limitless discretion as granted to the executive, along with a minimal provision of legal remedies to the citizens, make it a serious

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[17] U.S. Const. amend. IV.
[18] G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).
[19] Kaye, D. (2015, May 22). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (U.N. Doc. A/HRC/29/32).

threat to the constitutional fabric and to internationally recognised rights of man. Unless such accompanying safeguards are put in place, however, legal and technological modernization can only imperil the legitimacy of the dissent that is so vital to the checks that form the heart of democratic accountability.

VII. REFORM NECESSITIES: RECOMMENDATIONS

Several urgent reforms are needed to redress the balance between national security and privacy, and to bring Indian practices into line with both the constitutional and international standards:

Legislative Revision

The current surveillance legislations, particularly the Indian Telegraph Act, Information Technology Act, and the DPDPA, need to be revamped and provide clear and specific definitions of triggering conditions, limit the usage of vague and discretionary criteria, and contain sunset clauses of emergency powers that are binding and stipulated. Authorities granted by surveillance shall also be restricted to clear and narrow provisions, and blanket or mass surveillance shall be strictly prohibited.

Free-standing Regulatory Agency

An independent and adequately autonomous, resourced, and skilled Data Protection Authority ought to be established. This organ should be able to screen and check the requests of surveillance, audit the compliance, investigate the potential for abuses, and means of redress to heal the affected people with binding. It should be composed in a way that promotes diversity in opinions and immunity against the influence of the executive branch.

Judicial Safeguards

The permission to carry out surveillance should require prior judicial or quasi-judicial authorisation in advance, and frequent and intensive review by the courts or quasi-judicial tribunals should be mandatory. The reason behind such judicial oversight is necessitated by having to adhere to the principle of proportionality and protect against arbitrary or politically based surveillance.

Transparency and Participation of the People

The transparent rules, which should include publication of anonymised annual statistics of interception orders, independent audits, and open consultation with civil society on proposed surveillance measures, should be obligatory to build trust and guarantee democratic control. Where there are opportunities, notification requirements are to be included, except in narrowly tailored, veritable exigent circumstances.

Privacy by Design

The statutory and non-statutory data handling schemes in the state and the private sector should be made to imbibe the technologies and organisational habits that incorporate privacy by design and default. These comprise data minimisation, purpose limitation, default encryption, and tight access controls to reduce the surveillance footprint and minimise the chances of abuse or leaks.[20]

VIII. CONCLUSION

India is currently at a very decisive point in its digital and constitutional voyage. Although the recognition of the right to privacy as the basic one has been a landmark case in courts, the development is threatened to become still decorative unless it is supported by a comprehensive legislative and institutional reform. The presence of loopholes in the existing surveillance laws, inefficiency in the supervision, and low levels of control, almost unlimited executive authority, endangered democratic representation and civil liberties. The real need is radical changes, which must stem from autonomous checks and balances, judicially enforceable rights, and transparency to ensure India's surveillance policies are matched with constitutional protection and international corporate practices. Unless it takes action in this regard, the enjoyment of privacy, autonomy, and digital futures will be called into jeopardy because of the threat of being preempted by the spectre of an unaccountable digital surveillance state, and the principles of democracy and the rule of law would be undermined in India.

[20] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).