International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Privacy as a Fundamental Right After *Puttaswamy*: Limits on State Surveillance in India

Rajendra

Assistant Professor
Dayanand College of Law, Kanpur
Affiliated With: Chhatrapati Shahu Ji Maharaj University, Kanpur
rajendralaw4249@gmail.com

Abstract:
The ruling of the Supreme Court in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017) strongly asserted that the right to privacy was inherent to Articles 14, 19 and 21 of the Constitution. This case decision reversed previous precedents (e.g. M.P. Sharma, Kharak Singh) that had rejected a general right to privacy. After Puttaswamy, any state surveillance program should pass the proportionality test of the Court: it should have a legitimate purpose, use reasonable methods, be necessary and least intrusive. We consider the performance of the laws and programs in India. The current laws, such as the Indian Telegraph Act 1885 (Sec.5(2)) and the IT Act 2000 (Sec.69), evidence laws, etc., allow extensive interception under generalized conditions (e.g. public safety or state security). Practically, such programmes as the Central Monitoring System (CMS, released 2013) and the National Intelligence Grid (NATGRID, designed 2009) allow security agencies to have access to virtually all the data. The Aadhaar ecosystem (2016 onwards) has also been channeling personal information (biometrics, financial transactions, social benefits) into a central database. We examine some of the major cases (e.g. Rajagopal v.). Tamil Nadu, PUCL v. UOI, Selvi v. Karnataka), laws and policies according to the proportionality doctrine of Puttaswamy. The comparative jurisdictions and international law (ICCPR Art.17) support the idea that the intrusion of privacy should be legal, necessary, and proportionate. Results: The interception laws in India are mostly pre-Puttaswamy and do not have particular proportionality protection. CMS and Aadhaar are surveillance programs that were introduced without proper parliamentary discussion or privacy checks, which created a constitutional strain. No all-encompassing privacy or data protection legislation (as of 2019) exists to place judicial control or redress. Recommendations: To address the issue of codification of the test of Puttaswamy, legislative changes should be made to enforce clear legal foundations and judicial warrants on surveillance, enhance independent review (e.g. a standing Interception Review Commission), and provide remedy in case of abuse. Gaps should be filled with a strong privacy/data-protection law (as proposed by the 2018 Srikrishna Committee). Legal change should be accompanied by policy protection (high data retention thresholds, auditability, transparency reports), and technical protection (end-to-end encryption, privacy-by-design).

Keywords: Right to Privacy; Constitutional Law; State Surveillance; Puttaswamy Judgment; Proportionality Doctrine; Informational Privacy; Fundamental Rights; Article 21.

1. PRIVACY AND CONSTITUTIONAL JURISPRUDENCE IN INDIA

Indian jurisprudence has long been very reluctant to accord privacy any recognition. In M.P. Sharma v. Satish Chandra (1954) v. Kharak Singh. The Court, which referred to the lack of a Fourth Amendment-type provision in the U.S. Constitution, stated that neither Article 21 nor any other rights implied the right

to privacy (UP, 1963).[1] Govind v. State of M.P. (1975)[2] was the first to challenge this negative view, which stressed on personal dignity, and subsequent R. Rajagopal v. In Tamil Nadu (1994) a nine-judge bench ruled that privacy was implicit in Article 21. In PUCL v. UOI (1997)[3] The Court ruled that warrantless phone tapping was unconstitutional, said that the right to privacy is an extension of the right to life and personal liberty. More recently, Selvi v. Karnataka (2010)[4] identified a mental privacy and prohibited involuntary narcoanalysis, strengthening Article 20(3) (self-incrimination) and Article 21. Nevertheless, there was no general framework that was to regulate mass surveillance.

Puttaswamy (2017) and the new standard: In Justice K.S. Puttaswamy (Retd.). v. In a unanimous ruling, Union of India (2017) comprised of nine judges who determined that privacy is a constitutional right under the Indian Constitution. The Court specifically reversed M.P. Sharma and the narrow interpretation of Kharak Singh and stated that privacy is inherent in Articles 14, 19 and 21. Dr. The lead opinion of D.Y. Chandrachud defined privacy as inherent to the right to life and personal liberty, which includes bodily integrity, family and marital decisions, informational self-determination, and home. Most importantly, the Court has stated a four-part proportionality test: any state action that violates privacy must (i) serve a legitimate state purpose, (ii) be founded on a just/fair/rational law, (iii) be necessary, and (iv) be minimally intrusive (i.e. proportionate). Therefore, following Puttaswamy, broad surveillance must be explicitly authorized by statute, supported by purpose, and limited.

Influence on doctrine: Puttaswamy has doctrinally changed the Indian law by transforming the formal test of procedure established by law to substantive due process. Any law that allows surveillance has now to pass through minimalism review. The Court stressed the judicial control, responsibility and accuracy in any violation of privacy. This new regime puts constitutional constraints: ambiguous terms such as public safety can no longer be used to justify blanket taps or data collection without further explanation. Another point that Puttaswamy makes is that privacy is not an elite concept but the key to dignity among all people, and vulnerable groups in particular. This, in practice, implies that the current surveillance authorities (in telecom, cyber, Aadhaar schemes, etc.) should be re-evaluated in accordance with this proportionality standard.

2. SURVEILLANCE STATUTORY AND POLICY FRAMEWORK

The Indian legal system of surveillance is based on the outdated legislation that is complemented by executive regulations:

- Indian Telegraph Act, 1885: Sec. 5(2) gives the Home Secretary (Union or State) the power to direct interception of telephone, telegraph or data in case they feel it necessary or expedient in the interests of public safety or public emergency. These general reasons (public safety) are not defined and can be subject to arbitrariness. Following PUCL v. The Court interpreted the wording of the statute to provide stringent protection: all interceptions should be pre-approved by senior officials, reported to an independent review committee, and that the intercepted individuals must be of necessary good character (UOI, 1997). However, there is still ambiguity in legislation: the Act is not technologically up-to-date and does not present a specific proportionality test.
- Information Technology Act, 2000: In 2008, amended, Sec.69 permits the central government to request any agency or intermediary to intercept/monitor/decrypt computer data in the interests of sovereignty, security, public order etc. Rules (IT Interception Rules 2009) regulate the procedure, but, as with the Telegraph Act, they confer wide executive discretion. The reasons (sovereignty, public order) are similar to those in Sec.5(2) and are once again not defined precisely. Importantly, the AP Shah Committee of experts (2012) noted that the thresholds and retention rules in Sec.5(2) and Sec.69 are inconsistent.

[1] AIR 1954 SC 300.
[2] AIR 1975 SC 1378; (1975) 2 SCC 148.
[3] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[4] Selvi v. State of Karnataka, (2010) 7 SCC 263.

Other statutes: The Indian Evidence Act, 1872 (s.27) conventionally allows confession evidence to result in discovery. It is not very relevant in this case, but the Court in Selvi observed that forced tests (narco/polygraph) are incompatible with Article 20(3) and privacy, which amends the evidentiary practice. Surveillance is permitted by the Criminal Procedure and local police rules under Section 108 CrPC (warrantless search) or Section 91 (summons), yet they were not created with digital data in mind and are not transparent. No particular legislation exists regarding the sweeping up of personal information by the state (e.g. DNA profiling, biometrics).

Rules and policies: There are government policies such as the National Privacy Policy (written 2012, finalised subsequently) and National Intelligence Grid (NATGRID) policies, which are not legally binding. The Ministry of Home Affairs and IT have published several circulars on data retention to ISPs and telcos, but these are not laws, but guidelines. The absence of a general data protection law (as of 2019) implies that the state surveillance is primarily governed by these sectoral laws and regulations.
In general, the statutory regime provides broad executive authority and little oversight by the parliament. It did not require any independent oversight tribunal (as would be the case with, say, a Russian FSB court or the Investigatory Powers Commissioner in the UK). The implication of the test by Puttaswamy is that such laws should be construed strictly and any surveillance activity closely monitored.

3. SIGNIFICANT SURVEILLANCE SCHEMES AND PROGRAMS

Indian state surveillance is both official and quasi-official. The following is a comparative outline of major programs until 2019.:

Program	Year Launched	Scope & Data Collected	Legal Basis & Concerns
Central Monitoring System (CMS)	2013 (roll-out); announced 2011	Real-time "centralized" tapping: all telecom calls, SMS, internet metadata/content for up to 900 million mobile, 160 million internet users	Implemented via executive orders; no specific parliamentary sanction. Based on Telegraph & IT Acts but blurs lines between types of data. Little public transparency; oversight procedures (PUCL Guidelines) exist but effectiveness unknown.
NATGRID (National Intelligence Grid)	Proposed 2009; funding approved 2012; partial rollout ~2017	Integrated intelligence database: collects/pools data (credit/debit card transactions, telephone/mobile data, travel records, PAN/TAN, immigration records, police FIRs via CCTNS, etc) from 21 agencies	No stand-alone law; approved by Cabinet. Concerns about privacy (AP Shah report noted lack of data policy). Parliamentary reports and civil society have criticized absence of legal oversight or review. Full capabilities not tested.
Crime & Criminal Tracking Network and Systems (CCTNS)	2009–present	National police database linking ~14,000 police stations; stores FIRs,	Statutory backing via CrPC amendments; aims to streamline

		crime history, biometric IDs, etc.	policing. Privacy issues: government often shares CCTNS data with other agencies (e.g. for Aadhaar/KYC) without judicial check.
Aadhaar (UIDAI)	Pilot 2010; Aadhaar Act 2016	Biometric/demographic ID system for all residents. Links identity to subsidies (food, LPG, pensions), bank accounts, mobile SIMs. Authentication logs (time, location) amassed for transactions.	Aadhaar Act (2016) governs UID data. *Puttaswamy II* (2019) upheld Aadhaar for welfare purposes but struck down misuse provisions (e.g. Section 33(2) allowing security-based data sharing). Continued concerns: Act lacks robust privacy safeguards for data sharing with private/public entities; mass collection without explicit consent is borderline "mandatory", and data breaches have occurred.
Video Surveillance (CCTV)	2000s–present	Millions of CCTV cameras in public spaces (metros, streets, buildings). Some cities (Smart Cities) integrate video analytics.	No centralized law; governed by local police/urban policy. Face recognition trials raise privacy alarms. Very little legal control or oversight of camera data.
Other Digital Programs: Government schemes (DIGIT programs, e-Governance databases), cellphone location tracking for law enforcement, and intelligence tools (e.g. IMSI catchers)	Various (2010s)	Data from social media monitoring, internet usage (Deep Packet Inspection rules were proposed but stayed). Emerging tech experiments (DNA database draft bill 2018, predictive policing pilots).	Largely ad hoc or proposed; no robust legal regime. Raises *Puttaswamy*-style questions: absence of statutory checks, lack of notice or remedy for targeted individuals.

There are few comprehensive statistics on state surveillance. According to HRW, CMS has access to all phones and Internet in country, but the official data (e.g. number of intercept orders) is not published. By 2018, Aadhaar had enrolled more than 1.1 billion residents, or more than 90 percent of adults, and by 2019

it was de facto mandatory in most services. Internet shutdowns (state-imposed blackouts) although not surveillance as such, counted 223 in 2019 (according to Internet Democracy project), a measure of state control over communications. Nevertheless, such details as the percentage of intercepted calls or the number of CCTV units used are not disclosed publicly or are unspecified.

India did not have a general privacy statute prior to 2020, as the Fourth Amendment to the US Constitution or the Charter of the EU did. The ICCPR Art.17 (to which India is a party) international norms forbid arbitrary or unlawful interference with privacy. Puttaswamy brings India closer to jurisdictions that demand legislation and proportionality (e.g. decisions of the European Court of Human Rights such as Zakharov v. Russia, 2015)[5]. The lack of transparency and oversight in India is the opposite of such countries (e.g. Investigatory Powers Act 2016 of the UK, which enforces a warrant regime).

4. CASE LAW REVIEW AND DOCTRINAL EFFECT

Privacy has been progressively anticipated by Indian courts, and Puttaswamy is the result. Key cases include:

- R. Rajagopal v. Tamil Nadu (1994)[6]: The Supreme Court accepted privacy as implicit in Article 21, quashing a government order permitting the publication of police records, and declaring privacy as a right to be left alone.
- People's Union for Civil Liberties (PUCL) v. Union of India (1997)[7]: Raised the issue of state phone tapping under the telegraph act of Sec.5(2). The Court interpreted wiretapping as a violation of Article 21 and interpreted Sec.5(2) narrowly, setting up guidelines (review committees, senior sanction). It clearly believed that the right to privacy is an extension of the right to life and personal liberty.
- State of Maharashtra v. Bharati Ben[8] (Aadhaar parentage claim, 2014): Supreme Court stated that issuing Aadhaar did not infringe fundamental rights, and it was voluntary. (Subsequently, Puttaswamy II made clarifications on the use of Aadhaar, which supported certain provisions.)
- Selvi v. Karnataka (2010)[9]: A landmark case of 3 judges that involuntary narcoanalysis, brain mapping and polygraph tests are against Article 20(3) and Article 21. It confirmed that a person has a right to privacy of his own mind, and that bodily and mental privacy are sacrosanct under the Constitution.
- S. P. Gupta v. President (1981)[10] & Other Administrative Cases: Not specifically on privacy but established precedents on administrative secrecy. Puttaswamy expressly restricted S.P. Gupta (in which the publication of the bank account of Ashok Chavan by Parliament was affirmed), as privacy was more important than unnecessary political investigation.
- Justice K.S. Puttaswamy v. Union of India (2019)[11]: Since Puttaswamy I, the Court (5-judge) heard arguments against the Aadhaar Act. It affirmed the majority of the Act but invalidated Section 33(2) (data sharing on the basis of national security without a hearing) and Section 57 (data sharing by private bodies requiring Aadhaar). The Court restated the proportionality test and acknowledged that mass data collection (biometrics, location/time stamps in Aadhaar authentication) is a privacy concern, but weighed it against the welfare interests. It warned that privacy cannot be sold in bulk in exchange of gain. Puttaswamy II therefore reiterated privacy as issues that one has a reasonable expectation of privacy, and interpreted the Aadhaar law in a limited way to safeguard dignity.

[5] Roman Zakharov v. Russia, App. No. 47143/06 (ECtHR, Grand Chamber, 4 Dec. 2015).
[6] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[7] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[8] State of Maharashtra v. Bharati Ben, (2008) 8 SCC 713.
[9] Selvi v. State of Karnataka, (2010) 7 SCC 263; AIR 2010 SC 1974.
[10] S. P. Gupta v. Union of India, AIR 1982 SC 149; (1981) Supp SCC 87.
[11] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1.

Interpreting Precedents under Puttaswamy: Previous cases such as Rajagopal and PUCL are now interpreted as precursors of Puttaswamy. The Court specifically incorporated these in its jurisprudence in Puttaswamy. As an example, the phone tap guidelines of PUCL are still the law of the land, but they can be challenged in 2017 under the new standard as to their adequacy. Any ambiguous exceptions (such as that of public safety) now face the scrutiny of Puttaswamy. With the introduction of proportionality, the lower courts and agencies ought to reconsider the previous case law regarding evidence and privacy: e.g. Navjot Sandhu v. In the spirit of Puttaswamy, NDTV (2019) reiterated that the illegally intercepted calls cannot be admitted.

5. GAPS, TENSIONS, AND REFORM

Gaps and Tensions: Puttaswamy has some huge gaps between his mandates and reality:

- Absence of a General Privacy/Data Law: India did not have a comprehensive law that defined personal data or controlled state intrusion until 2019. The Draft Personal Data Protection Bill (2018) is not in force (as of 2019). In the absence of a data protection framework, activities such as bulk collection by UIDAI or data retention by telcos are carried out with little restrictions.
- Judicial Oversight: Executive surveillance is permitted by law to a large extent without judicial approval. Puttaswamy suggests that warrants (or post-hoc approval by an independent body) must be obtained. However, the present day rule of Sec.5(2)/Sec.69 gives the internal government committees (not subject to judicial review) the responsibility of vetting intercepts. This puts a strain on the demand of Puttaswamy of fair, reasonable process.
- Opacity and Accountability: Surveillance programs (CMS, NATGRID) were created in secrecy of the executive. Their scope was not discussed in any parliamentary debates or consultations with the people. Virtually no transparency reports are made on the number of intercepts or accesses. Puttaswamy requires accountability (“check and balance) yet citizens are usually unaware of the time their information is gathered.
- Technology Outpacing Law: Surveillance at Scale: Technologies (mass data analytics, AI, biometrics) facilitate scale surveillance. But law is behind: the police are outsourcing cyber intelligence to private vendors, and personal data are being collected by private companies in vast amounts with minimal regulation. This nexus between the private and the public can be avoided by constitutional constraints, a tension that needs redress.

REFORM RECOMMENDATIONS:

1. Legislation: Pass a strong privacy/data protection law (e.g. the PDP Bill) that specifically includes the principles of Puttaswamy. Among the key features, one should note: (a) the existence of clear legal grounds of any state data collection (with a set of purposes), (b) the necessity of the prior judicial consent to intercepts or access to stored data, (c) the minimization of data and limitation of its purpose, and (d) the presence of independent oversight bodies with investigative powers. Such safeguards, such as special exceptions, were already suggested by the Justice Srikrishna Committee (2018) under strict conditions.
2. Judicial and Parliamentary Oversight: Amend the Telegraph Act and IT Act to change the phrase of the satisfaction of the officer to the requirement of judicial warrants, particularly in capturing content. Enhance the current Intelligence Oversight Bodies (particularly the recommendations of Justice Radha Krishna Committee) by turning them into a real body and a public one. Also, Parliament ought to examine all surveillance projects: e.g. a Joint Parliamentary Committee on privacy (as implied in media) should examine NATGRID, CMS, etc.
3. Policy and Transparency: The government policies must require transparency: release statistics on surveillance orders, data breaches and audits. Restate PUCL recommendations and publish the findings of the Interception Review Committees. Any emerging technology (such as facial recognition, AI

profiling) should be accompanied by clear regulations and effects evaluation. Law enforcement training on privacy rights (as per Puttaswamy) is also required.

4. Technical Safeguards: Promote privacy-saving technologies. As an example, make strong encryption the default and restrict the features that force service providers to develop backdoors. Implement privacy by design in government databases (e.g. tokenize Aadhaar in welfare schemes). Invest in privacy enhancing audits and data management standards of government agencies.
5. Judicial Vigilance: The lower courts ought to take the initiative to apply the Puttaswamy test to pending cases. As an illustration, they need to insist on proving necessity and minimality when hearing challenges to telephone or internet surveillance (or even informal data-gathering such as Twitter or electronic voting machines).

CONCLUSION:

Justice K.S. Puttaswamy has transformed the Indian law by making privacy a fundamental right. Its contribution to the field of surveillance is that no encroachment on privacy can be made without substantial justification and procedural fairness. Until 2019, though, the surveillance infrastructure of India, both the old colonial legislation and the new ID databases, has been mostly run on a wide executive discretion. The gap between the aspirational constitutional norm and reality on the ground will be bridged only through sweeping reforms: new laws, strict control, and transparency culture. Only in this case, the constitutional restrictions on surveillance can fulfill the desired role of protecting individual autonomy in the digital era.