DIGITAL SURVEILLANCE VS. PRIVACY RIGHTS: CONSTITUTIONAL LIMITS POST-PUTTASWAMY

Manish Kumar, Research Scholar, School of Law, Bennett University, Greater Noida[1]

ABSTRACT

The landmark judgement of Justice KS Puttaswamy (Retd) v Union of India (2017) by the honourable Supreme Court of India has revamped the constitutional jurisprudence in the country by elevating the right to privacy to a fundamental right guaranteed under Part III of the Indian Constitution. However, the rapid growth of digital surveillance, strengthen by the Information Technology Act 2000 and the Digital Personal Data Protection (DPDP) Act 2023, has created a conflict between state security and individual autonomy. The present paper seeks to examine the "proportionality test" as the definitive constitutional limit on state surveillance, arguing that while the legal framework exists, executive exemptions and a lack of judicial oversight continue to threaten the "privacy of the soul."

Keywords: Right to Privacy, Proportionality test, DPDP Act 2023, IT Act 2000.

[1] Research Scholar, School of Law, Bennett University, Greater Noida

1. Introduction

The digital age has fundamentally impacted the relationship between the citizens and the state. Surveillance is now accomplished through "digital footprints"—seamlessly gathered, stored, and analyzed—instead of physical intrusion. The Supreme Court of India ruled in *Justice KS Puttaswamy (Retd) v. Union of India*[2] that privacy is a "intrinsic part of the right to life and personal liberty" under Article 21. However, the state regularly uses "national security" as a general defense for widespread digital surveillance. This essay investigates whether the DPDP Act 2023 and other current laws uphold the constitutional limits established by the Puttaswamy court.

2. The *Puttaswamy* Paradigm: A New Constitutional Standard

Indian privacy legislation was a patchwork of contradictory decisions before to 2017. According to cases like *MP Sharma v. Satish Chandra*[3] and *Kharak Singh v. State of UP*[4], privacy was not expressly protected by the Constitution. These rulings were overturned by Puttaswamy, who established that privacy is an inherent right rather than a "gift of the state".

2.1 The Four-Pronged Proportionality Test

The plurality opinion in *Puttaswamy* established that any state interference with privacy must satisfy a four-fold test:[5]

1. **Legality:** The action must be sanctioned by a law (Legislative mandate).
2. **Legitimate Aim:** The state must have a valid purpose (e.g., national security).
3. **Necessity/Suitability:** The means must be necessary and there must be a rational nexus between the aim and the measure.
4. **Proportionality *stricto sensu*:** The state must use the "least restrictive" method to achieve its goal.

[2] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
[3] *MP Sharma v Satish Chandra* [1954] SCR 1077.
[4] *Kharak Singh v State of UP* [1964] 1 SCR 332.
[5] *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1.

3. Digital Surveillance and the Legislative Framework

In India, Section 5(2) of the Indian Telegraph Act 1885 and Section 69 of the Information Technology Act 2000 continue to be the major instruments for state surveillance.

3.1 The Expansion of Section 69 IT Act

Information created or maintained in any computer resource may be intercepted, monitored, or decrypted by the government under Section 69. In contrast to the Telegraph Act, which mandates the presence of a "public emergency," the IT Act permits monitoring for "investigation of any offence."[6] This lower threshold is arguably a violation of the "necessity" prong of the *Puttaswamy* test.

3.2 Deep Dive: The DPDP Act 2023 – A Post-Puttaswamy Critique

India's main legislative response to the Supreme Court's order for a thorough data protection system is the DPDP Act 2023. Its structure, however, presents a number of controversial "exemptions" that call into question the fundamental proportionality principles set forth in Puttaswamy.

3.2.1 The Mechanism of State Exemptions (Section 17)

Section 17(2)(a) of the Act raises the most important constitutional issue. This clause gives the Central Government the authority to exempt any "instrumentality of the State" from the Act's requirements in order to:

- Sovereignty and integrity of India;
- Security of the State;
- Friendly relations with foreign States;
- Maintenance of public order.

The Puttaswamy verdict mandates that any such restriction be proportionate, even though these grounds are similar to the "reasonable restrictions" under Article 19(2). According to

[6] *Information Technology Act 2000 s.69 & The Indian Telegram Act 1885 s.5(2)*

academics, Section 17 offers a "blanket exemption" as opposed to a "targeted" one. The Act creates a legal void where the state can process large amounts of data without the safeguards of accountability by permitting state agencies to evade notice, consent, and data minimization rules.[7]

3.2.2 The "Legitimate Use" Exception (Section 7)

The Act presents the idea of "certain legitimate uses" under Section 7, which permits processing of personal data without the Data Principal's consent. In particular, Section 7(b) empowers the State to handle information in order to grant licenses, permits, certifications, subsidies, benefits, and services. Although administrative efficiency is the goal, there is a chance that the "coercive consent" controversy from Puttaswamy II (Aadhaar) will resurface.[8]

The "choice" is illusory and may violate the informational self-determination principle if a person must give up their privacy in order to obtain necessary governmental services.

3.2.3 Dilution of the Right to Information (RTI)

Section 44(3) of the DPDP Act, which modifies Section 8(1)(j) of the RTI Act 2005, contains a minor but important restriction on transparency. In the past, disclosure of personal data was permitted provided it served a "larger public interest." This balancing test is eliminated by the DPDP Act, which essentially forbids the release of any personal information about public officials. This goes against Justice Chandrachud's "culture of justification" by making it harder for citizens to hold the government responsible for its data processing operations.[9]

3.2.4 Institutional Independence: The Data Protection Board (DPBI)

A data protection framework needs an independent oversight mechanism, as the Puttaswamy ruling made clear. As per the DPDP Act:

- The Central Government appoints all members of the Data Protection Board (DPBI) (Section 19).

[7] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [310].
[8] *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1.
[9] *Digital Personal Data Protection Act 2023, s 44(3).*

- The executive sets the terms and conditions of service.

Prong of Test	DPDP Act Compliance Status	Analysis
Legality	**Passed**	The Act provides a clear statutory basis for data processing.
Legitimate Aim	**Passed**	National security and public order are recognized legitimate aims.
Necessity	**Contested**	Broad exemptions for state agencies may lead to collection of data beyond what is strictly necessary.
Proportionality	**Contested**	Lack of judicial warrants for surveillance and lack of an independent regulator suggests a failure to use the "least restrictive" means.

Critics contend that the adjudicatory body fails the proportionality test's "procedural safeguards" requirement since it is unable to properly check state-sponsored surveillance if it is not shielded from executive control.[10]

4. Synthesis: Does the Act Pass the Proportionality Test?

5. Analysis of Constitutional Limits: The Proportionality Doctrine in the Digital Age

Instead of granting an unqualified right to privacy, the Puttaswamy ruling created a strict "culture of justification." Determining whether the state's digital surveillance tools, such as the Central Monitoring System (CMS) and facial recognition technology (FRT), adhere to the parameters of the four-pronged test is crucial for research scholars.[11]

5.1 The Legality Prong: Beyond Mere Statutory Existence

Legality is the first restriction. Following Puttaswamy, it is no longer adequate to conduct

[10] Gautam Bhatia, 'The Data Protection Act: A Constitutional Perspective' (Indian Constitutional Law and Philosophy, 15 August 2023) https://indconlawphil.wordpress.com accessed 8 January 2026.
[11]Columbia Global Freedom of Expression, 'Puttaswamy v. Union of India (I)' https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/ accessed 8 January 2026

surveillance using executive directives or private "standard operating procedures." It necessitates a law that is predictable, understandable, and obvious.

Section 5(2) of the Telegraph Act and Section 69 of the IT Act now regulate monitoring in India. Constitutional scholars contend that these do not meet the "predictability" criterion. The 2007 and 2009 Rules, which govern these parts, provide the government the authority to approve its own requests for monitoring without external supervision. Instead of leaving it up to the Home Secretary's haphazard discretion, the "legality" prong in a digital democracy should arguably mandate that the law explicitly specify the categories of people exposed to monitoring and the nature of the violations.[12]

5.2 Legitimate Aim and the "National Security" Quagmire

The presence of a legitimate state goal is the second restriction. Although "national security" is a widely recognized justification for limiting rights, the Puttaswamy criterion mandates that this goal be precise.

The state frequently confuses "national security" in the digital sphere with "law and order" or "investigation of any offense." There are constitutional concerns with this growth. The restriction here is that political profiling or the repression of dissent under the pretense of security cannot be accomplished through surveillance. This was reaffirmed by the court in *Vinit Kumar v. CBI*[13], which invalidated interception orders that failed to show a "public emergency" or "public safety" concern, demonstrating that even a justifiable goal must be based on an urgent need.

5.3 Suitability and the Myth of "Bulk Collection"

The state must demonstrate that the chosen surveillance measure will genuinely accomplish the stated purpose in order to pass the Suitability (or Rational Nexus) prong. This is the most difficult constitutional obstacle for mass surveillance.

The "suitability" of the bulk collection is called into question if the state gathers the metadata of millions of people in order to apprehend a single offender. The shift from targeted surveillance, which is constitutional, to dragnet surveillance, which is unconstitutional,

[12] *Information Technology Act 2000 s.69 & The Indian Telegram Act 1885 s.5(2)*
[13] *Vinit Kumar v Central Bureau of Investigation and Others* [2019] Bom CR (Cri) 613

represents the constitutional limit in this case. Bulk collecting frequently results in "false positives" and the suppression of free speech in the digital sphere. The state must demonstrate that a less invasive, focused strategy would not have been adequate within the Puttaswamy framework.[14]

5.4 Necessity and the "Least Restrictive Means"

Possibly the most important limit is the third prong, need. It requires the state to select the option that compromises privacy the least when there are several alternatives to accomplish a goal.

- Encryption and Backdoors: The need principle is violated if the state requires "backdoors" into encrypted platforms (like WhatsApp) when there are alternative investigative methods (like metadata analysis or physical device confiscation) available.[15]

- Facial Recognition (FRT): Since FRT permanently changes the "anonymity in a crowd" that is necessary for political expression, its use in public protests fails the need test if the purpose is only identification.[16]

5.5 Proportionality *Stricto Sensu*: The Balancing Act

The balance of rights is the ultimate limit. This means that the court must balance the "intensity of the infringement" of the individual's right with the "social importance" of the state's objective.

The "intensity of infringement" rises exponentially as digital surveillance becomes more widespread and uses deep-packet inspection, AI, and predictive policing. The "Privacy of the Soul" is the constitutional restriction in this case. A 360-degree digital profile that forecasts a person's thoughts, political inclinations, or future behavior cannot be constitutionally created by the state, even while it may monitor a person's actions for a valid reason. Puttaswamy aimed

[14] H M Verhelst, A W Stannat and G Mecacci, 'Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma' (2020) 26 Sci Eng Ethics 2975.
[15] *Podchasov v Russia App no 33671/25 (ECtHR, 13 February 2024) [76]–[79]*
[16] UNHRC, 'The Right to Privacy in the Digital Age: Report of the OHCHR' (2018) UN Doc A/HRC/39/29.

to stop this "profiling" as a form of totalizing state power.[17]

6. Judicial Review and Procedural Safeguards

The need for procedural due process is a crucial constitutional restriction. Puttaswamy stressed that a surveillance act is unlawful if it lacks protections against abuse, even if it is appropriate in theory.

6.1 The Absence of Judicial Warrants

In India, the Home Secretary, who is part of the executive branch, has the authority to conduct its own surveillance. A "judge in their own cause" situation exists here. Judicial warrants are the bare minimum constitutional protection against digital intrusion, according to comparative jurisprudence (such as the US Fourth Amendment or the UK Investigatory Powers Act). One major constitutional vulnerability that has not been addressed since Puttaswamy is the absence of such a provision in the IT Act regulations.[18]

6.2 The Right to be Notified

In privacy legislation, post-surveillance notification is becoming more and more common. A person should ideally be informed if they are being surveilled and no charges are brought against them so they can pursue legal action for any unjust intrusion. The "secrecy by default" approach of the current Indian framework restricts citizens' access to Article 32 constitutional remedies.[19]

7. Conclusion

A major conclusion of this study is that rights without remedies are illusory. The DPDP Act's reliance on a government-appointed Data Protection Board creates a conflict of interest that undermines the "procedural safeguards" required by *Puttaswamy*. For a constitutional limit to be meaningful, there must be an independent "watchman."

This paper argues for the judicialization of surveillance. The executive should not be the sole arbiter of its own surveillance needs. A system of "judicial warrants" for digital interception—

[17] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [311] (Chandrachud J)
[18] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [310] (Chandrachud J)
[19] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 [311] (Chandrachud J)

similar to the requirements for physical searches under the Code of Criminal Procedure—is not just a policy recommendation; it is a constitutional necessity post-*Puttaswamy*.

In conclusion, the *Puttaswamy* judgment was not the end of the struggle for privacy, but the beginning of a new constitutional era. The limits on digital surveillance are clear in principle but diluted in practice. The DPDP Act 2023, in its current form, requires urgent judicial pruning to bring its exemption clauses in line with the proportionality standard.

Ultimately, the digital state must remember that "security" is not merely the absence of external threats, but the presence of internal liberty. A state that watches its citizens constantly may be "secure," but it is no longer "free." The constitutional limits established post-*Puttaswamy* serve as the final line of defense for the "private space" that is essential for a thriving democracy. The soul of the Constitution resides in the silence of the private room, and it is the duty of both the Court and the Legislature to ensure that the digital eyes of the state do not intrude upon that silence without a compelling, proportionate, and legally sanctioned reason.

8.The Global Context and the Way Forward

India’s path forward must be viewed through the lens of "Digital Constitutionalism." As the world’s largest democracy, India’s handling of the tension between surveillance and privacy will set a precedent for the Global South. We must move away from the "rule by law" (where the law is a tool of state control) toward the "rule of law" (where the law limits state power).

The final limit is the **"Privacy of the Soul."** As AI and big data analytics become more integrated into governance, the risk is no longer just the "leakage" of data, but the "manipulation" of the individual. The constitutional limit post-*Puttaswamy* must therefore expand to include protection against **algorithmic profiling**. The state must be prohibited from using digital surveillance to "nudge" or "predict" citizen behavior in ways that bypass conscious choice.