

The Right to Privacy in the Age of Algorithmic Surveillance: Is Puttaswamy Future-Proof?

Dr. Malay Kumar Behera¹, Gunnam Bhaskar Rao²

¹Recognized as ‘Star’ & ‘Domain Scholar’ in “Patents and IPR” by NPTEL IIT Madras

²Research Scholar, PG Dept. of law, Sambalpur University

Abstract

The proliferation of artificial intelligence (AI), facial recognition, predictive analytics, biometric identification, and automated profiling is fundamentally transforming the nature of State surveillance. In India, the constitutional right to privacy is principally grounded in the Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), which recognised privacy as a fundamental right intrinsic to dignity, autonomy, liberty, and informational self-determination. This article examines whether the constitutional framework developed in Puttaswamy remains adequate in an environment where surveillance is increasingly automated, predictive, pervasive, and capable of generating information through algorithmic inference.

Using a doctrinal and comparative legal methodology, the article examines Puttaswamy, K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2019), Maneka Gandhi v. Union of India (1978), Anuradha Bhasin v. Union of India (2020), the Digital Personal Data Protection Act, 2023, and contemporary scholarship on algorithmic governance and surveillance. The article argues that Puttaswamy is **normatively future-proof but operationally incomplete**. Its principles of legality, legitimate State purpose, necessity, proportionality, and procedural safeguards provide a durable constitutional foundation. However, AI-enabled surveillance introduces distinctive challenges involving metadata, inferential privacy, mass profiling, algorithmic bias, opacity, function creep, and automated decision-making. The article consequently proposes an expanded Puttaswamy framework incorporating algorithmic impact assessments, independent auditing, meaningful transparency, human oversight, equality-based review, strict purpose limitation, and effective remedies. It concludes that Puttaswamy should not be replaced but constitutionally developed into the foundation of an Indian framework of algorithmic constitutionalism.

Keywords: Right to Privacy, Puttaswamy, Algorithmic Surveillance, Artificial Intelligence, Informational Privacy, Article 21, Proportionality, Facial Recognition, Algorithmic Governance, India.

1. Introduction

The digital transformation of governance has created unprecedented opportunities for the State to collect and analyse information concerning individuals. Artificial intelligence now permits governments and law-enforcement agencies to process biometric data, location information, communications metadata, images, social-media information, and other digital traces at a scale that was previously unimaginable. Surveillance is consequently undergoing a qualitative transformation. Traditional surveillance generally involved observing a particular person or event. Algorithmic surveillance, by contrast, can involve the

continuous collection and automated analysis of information concerning entire populations.

The constitutional implications are significant.

The issue is no longer merely whether the State collects personal information. Artificial intelligence can combine apparently innocuous information to generate highly sensitive inferences about an individual's identity, behaviour, associations, preferences, health, economic circumstances, or political activities. Algorithmic surveillance therefore creates a form of informational power that may affect autonomy even without direct physical intrusion.

India's constitutional response to privacy is principally founded upon Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The nine-judge Supreme Court bench unanimously recognised privacy as a fundamental right and located its constitutional foundations in Articles 14, 19, and 21.

The significance of Puttaswamy extends beyond conventional data protection. Its emphasis upon dignity, autonomy, liberty, and informational privacy provides a constitutional basis for addressing emerging technologies.

Yet an important question remains: **Is Puttaswamy sufficiently equipped to regulate algorithmic surveillance?**

This article argues that it is **future-proof at the level of constitutional principle but not self-executing at the level of institutional safeguards.**

2. Research Questions

The study addresses the following research questions:

RQ1

To what extent does the constitutional right to privacy recognised in Puttaswamy protect individuals against AI-enabled and algorithmic surveillance?

RQ2

Are the legality, necessity, and proportionality principles developed in Puttaswamy adequate to address contemporary forms of algorithmic surveillance, including facial recognition, predictive policing, biometric analytics, and metadata analysis?

RQ3

What doctrinal gaps arise from algorithmic inference, profiling, opacity, and automated decision-making that are not adequately addressed by conventional privacy jurisprudence?

RQ4

How can Indian constitutional jurisprudence and statutory regulation be developed to create an effective rights-based framework for algorithmic surveillance?

RQ5

What lessons can India draw from comparative regulatory developments, particularly the European Union's data-protection and AI-governance frameworks, without compromising India's constitutional and developmental context?

3. Research Objectives

The principal objectives of this research are:

1. To critically examine the constitutional foundations of privacy following Puttaswamy.
2. To analyse the application of proportionality to AI-enabled surveillance.
3. To identify emerging threats to informational privacy created by algorithmic inference and profiling.

4. To evaluate the adequacy of India's existing statutory framework, particularly the Digital Personal Data Protection Act, 2023.
5. To examine the relationship between privacy, equality, liberty, and freedom of expression in algorithmic surveillance.
6. To propose an expanded constitutional framework for AI-enabled surveillance in India.

4. Literature Review

The literature concerning privacy and artificial intelligence in India can broadly be divided into four interconnected strands.

4.1 Constitutional privacy and Puttaswamy

The first body of scholarship examines the constitutional significance of Puttaswamy. The judgment fundamentally altered Indian privacy jurisprudence by treating privacy as intrinsic to dignity and autonomy rather than as a narrow derivative right.

The literature particularly emphasises the Court's recognition of **informational privacy** and its proportionality-based approach to State interference. Bhandari and Bailey (2025), for example, identify Puttaswamy as a major turning point in Indian privacy jurisprudence and examine its continuing influence on questions involving data and State power.

The strength of this literature is its demonstration that Indian constitutional law possesses a strong foundation for protecting informational autonomy. However, much of the traditional privacy literature predates the widespread deployment of generative AI, large-scale facial recognition, and sophisticated algorithmic inference.

4.2 Surveillance, metadata, and proportionality

A second strand examines State surveillance and the difficulty of applying proportionality to technologically sophisticated monitoring.

Lakra and Shrivastava (2024) argue that metadata should not automatically be regarded as constitutionally insignificant simply because it does not contain communication content. Aggregated metadata can reveal intimate information concerning relationships, movements, beliefs, and behavioural patterns.

This scholarship is particularly important for AI surveillance because machine-learning systems derive value precisely by correlating large quantities of apparently unrelated information.

The implication is that privacy analysis must become **contextual and cumulative**, rather than examining each item of data independently.

4.3 AI, facial recognition, and algorithmic governance

A growing body of recent scholarship focuses specifically on AI surveillance. Omar et al. (2025) examine the tension between AI-enabled surveillance and fundamental rights in India, identifying facial recognition, predictive policing, and welfare technologies as areas requiring constitutional scrutiny.

Similarly, Sarankumar (2025) connects constitutional principles with emerging forms of AI governance, particularly algorithmic bias, biometric technologies, and surveillance.

Recent work by Sharma (2026) on algorithmic policing argues that the Puttaswamy framework has considerable relevance to AI-based facial recognition and automated policing but also highlights the need for stronger accountability mechanisms.

This literature demonstrates that the problem has moved beyond traditional "data privacy." AI can transform collected data into predictions and classifications, producing consequences even where the ori

ginal collection was lawful.

4.4 From data privacy to inference privacy

The most recent scholarship increasingly identifies **inference** as a distinct privacy problem.

Rathi and Tyagi (2026) conceptualise AI as an "inference infrastructure" capable of producing information about individuals through surveillance, profiling, and generative systems.

This is an important conceptual development.

Traditional privacy law asks:

What information has been collected?

Algorithmic governance requires an additional question:

What information has been inferred, and what consequences flow from that inference?

The literature consequently suggests a transition from data-centric privacy toward **inference-centric privacy**.

Recent scholarship also identifies Puttaswamy as foundational but incomplete for governing algorithmic power and digital constitutionalism (Saha, 2026).

Literature gap

Although the existing literature establishes strong connections between Puttaswamy, privacy, AI, and surveillance, there remains a need for a systematic constitutional framework that integrates:

- informational privacy;
- algorithmic inference;
- proportionality;
- Article 14 equality;
- administrative-law fairness;
- algorithmic transparency;
- independent auditing; and
- effective remedies.

This article addresses that gap by arguing that Puttaswamy should evolve from a general privacy doctrine into a framework of **algorithmic constitutionalism**.

5. Research Methodology

This research adopts a **doctrinal and comparative legal methodology**.

5.1 Doctrinal analysis

The doctrinal component analyses primary legal sources, including:

- the Constitution of India;
- Supreme Court judgments;
- the Digital Personal Data Protection Act, 2023;
- relevant subordinate regulatory developments; and
- established principles of constitutional and administrative law.

Particular attention is given to Puttaswamy, Puttaswamy (Aadhaar), Maneka Gandhi, and Anuradha Bhasin.

5.2 Comparative analysis

The study compares the Indian framework with developments in the European Union, particularly:

- the General Data Protection Regulation (GDPR); and
- the European Union Artificial Intelligence Act.

The purpose is not to transplant European law but to identify regulatory principles capable of strengthening Indian constitutional governance.

5.3 Analytical approach

The research uses a rights-based framework based on:

legality → legitimate aim → rational connection → necessity → proportionality → procedural safeguards → remedy.

The analysis also considers technological characteristics including automation, inference, scale, opacity, and predictive capacity.

6. Algorithmic Surveillance and Informational Privacy

Algorithmic surveillance differs fundamentally from conventional surveillance because it permits the State to create knowledge from data.

A facial-recognition system does not merely observe a face. It may identify an individual, compare that individual against a database, establish associations, and potentially trigger further investigative action.

Predictive systems can go further by assigning risk scores or predicting future conduct.

The resulting privacy concern is therefore not restricted to secrecy.

Privacy protects the conditions necessary for individuals to develop identities, relationships, opinions, and choices without constant informational domination.

As AI systems become capable of inference, the constitutional concept of informational privacy should consequently include protection against **unjustified inferential profiling**.

7. Puttaswamy and the Proportionality Principle

The greatest strength of Puttaswamy is its proportionality framework.

State interference with privacy cannot be justified merely by asserting administrative convenience or technological capability.

A surveillance measure should possess a lawful foundation, pursue a legitimate objective, be rationally connected to that objective, be necessary, and remain proportionate to the rights infringement.

For example, deployment of facial recognition in public spaces should require answers to several constitutional questions:

1. What law authorises the system?
2. What specific public objective does it pursue?
3. Is facial recognition demonstrably effective?
4. Are less intrusive alternatives available?
5. What safeguards limit misuse?
6. How long are biometric records retained?
7. What happens after a false identification?
8. Can the affected person challenge the decision?

Recent literature concerning AI surveillance in India increasingly recognises the importance of applying proportionality to such systems.

8. The Metadata and Aggregation Problem

AI creates a further challenge because the constitutional significance of data increases through aggregation.

Individually, a location record may reveal little. A long-term location history can reveal an individual's workplace, residence, religious practices, medical appointments, social relationships, and political activities.

AI can process these patterns automatically.

Thus, constitutional privacy should not depend solely upon whether individual data points are independently "sensitive."

The relevant question should also be:

What informational picture becomes possible through aggregation and algorithmic analysis?

This suggests the need for an **aggregate privacy principle** within Indian constitutional jurisprudence.

9. Algorithmic Bias and Article 14

AI surveillance raises not only privacy concerns but also equality concerns.

Algorithms can reproduce historical biases embedded in training datasets. Facial recognition may generate different error rates across demographic groups. Predictive policing systems may reinforce patterns of historical over-policing.

Article 14 therefore provides an additional constitutional safeguard.

An algorithm that is facially neutral may nevertheless produce discriminatory outcomes.

Consequently, judicial review should consider both:

- discriminatory design; and
- discriminatory effect.

High-risk government AI systems should be subject to periodic **algorithmic impact assessments** examining privacy, accuracy, equality, and fundamental-rights consequences.

10. Surveillance and the Chilling Effect

Algorithmic surveillance also threatens Article 19.

Continuous observation may influence individuals' willingness to speak, associate, protest, or participate in political activities.

This creates a chilling effect even when no immediate legal sanction follows.

The constitutional significance of privacy therefore extends beyond individual secrecy. Privacy provides a protected sphere in which citizens can formulate beliefs and exercise democratic freedoms.

Algorithmic surveillance risks converting this sphere into a condition of permanent visibility.

11. The DPDP Act, 2023 and Its Limitations

The Digital Personal Data Protection Act, 2023 represents an important development in India's data-governance framework.

However, data protection and algorithmic governance are not synonymous.

The Act addresses processing of digital personal data, but AI surveillance raises additional questions:

- What information can be inferred?
- How should automated classification be regulated?
- What level of transparency should high-impact AI require?
- How should algorithmic bias be tested?
- What human oversight is necessary?
- What independent auditing should occur?

Consequently, the DPDP Act should be understood as an important component of privacy protection rather than a complete framework for AI surveillance.

12. Comparative Perspective: European Union

The EU provides useful comparative lessons through the GDPR and AI Act.

The GDPR establishes principles including purpose limitation, data minimisation, transparency, and safeguards relating to automated decision-making.

The AI Act adds a risk-based approach to AI governance.

The central lesson for India is that regulation should be **risk-sensitive**.

A low-risk recommendation system should not be subject to the same regulatory requirements as an AI system used for policing, biometric identification, welfare eligibility, employment, or criminal justice.

India can therefore develop a proportionate regulatory structure while preserving space for innovation.

13. Towards an Expanded Puttaswamy Framework

The following framework would strengthen the constitutional regulation of algorithmic surveillance.

13.1 Constitutional legality

High-impact government surveillance should have clear statutory authorisation.

13.2 Purpose limitation

Data and AI systems should not be repurposed beyond the legitimate objective for which they were authorised without renewed legal justification.

13.3 Algorithmic necessity

The State should demonstrate that AI is necessary rather than simply convenient.

13.4 Algorithmic proportionality

The magnitude and probability of privacy infringement should be balanced against demonstrable public benefits.

13.5 Transparency

Affected individuals should receive meaningful information about consequential AI surveillance.

13.6 Independent auditing

High-risk systems should undergo technical and rights-based audits.

13.7 Human oversight

Consequential automated decisions should be reviewable by an appropriately empowered human decision-maker.

13.8 Effective remedies

Individuals should have accessible mechanisms to challenge unlawful surveillance, inaccurate identification, discriminatory profiling, and harmful algorithmic decisions.

14. Is Puttaswamy Future-Proof?

The evidence supports a nuanced answer.

It is future-proof constitutionally.

The judgment's grounding of privacy in dignity, autonomy, liberty, and informational control allows its principles to apply to technologies that did not exist when the case was decided.

It is not completely future-proof institutionally.

The judgment does not itself provide detailed mechanisms for:

- algorithmic auditing;
- model transparency;
- bias assessment;
- automated decision-making;
- inferential privacy; or
- continuous surveillance oversight.

This distinction is crucial.

The answer is therefore not to replace Puttaswamy but to **constitutionalise its application to algorithmic systems**.

15. Conclusion

Artificial intelligence is transforming surveillance from an activity of observation into an infrastructure of prediction and inference. The State's ability to combine biometric, behavioural, locational, and metadata information creates unprecedented opportunities for public security but also unprecedented risks to individual autonomy.

Justice K.S. Puttaswamy (Retd.) v. Union of India remains the constitutional foundation for responding to these developments. Its recognition of informational privacy and its proportionality framework provide principles capable of regulating emerging surveillance technologies.

Nevertheless, principles alone are insufficient.

The constitutional regulation of AI surveillance requires an expanded framework incorporating algorithmic impact assessments, independent auditing, meaningful transparency, human oversight, equality-based scrutiny, purpose limitation, and effective remedies.

The central proposition of this article is therefore that Puttaswamy is **not obsolete in the age of AI; rather, it is incomplete unless its principles are operationalised for algorithmic power**.

Indian constitutionalism should move from protecting individuals merely against the collection of information to protecting them against **unjustified informational inference and algorithmic classification**.

In this sense, the future of the right to privacy lies not merely in controlling data but in controlling the constitutional conditions under which data are transformed into knowledge, predictions, and decisions about individuals.

Puttaswamy can therefore be future-proof—but only if Indian constitutional law evolves from a doctrine of informational privacy into a doctrine of algorithmic constitutionalism.

References

1. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
2. Bhandari, V., & Bailey, R. (2025). Evolution of privacy jurisprudence in the Supreme Court of India: Evaluating the impact of Puttaswamy. National Law School of India Review, 36(2). <https://repository.nls.ac.in/nlsir/vol36/iss2/7/>
3. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the

- European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
5. Haque, I. U., Jafri, S. M. A., & Rehman, T. U. (2025). Right to privacy in the age of mass surveillance by the State. In Proceedings of the International Conference on Law and Technology. Atlantis Press. <https://www.atlantispress.com/proceedings/iclt-25/126019766>
 6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
 7. K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (India).
 8. Lakra, R., & Shrivastava, A. (2024). Confronting the metadata dilemma in India: A turn to context and proportionality. International Journal of Law and Information Technology, 32(1). <https://academic.oup.com/ijlit/article-pdf/32/1/eaee012/58356599/eaee012.pdf>
 9. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
 10. Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023. Government of India.
 11. Omar, R., Kaushik, A., Kaur, H., Singh, K., & Kaur, R. (2025). AI and right to privacy: Harmonizing surveillance with fundamental rights in India. In International Conference on Springer. https://link.springer.com/chapter/10.1007/978-3-032-20318-2_47
 12. Rathi, G., & Tyagi, S. (2026). Artificial intelligence as an inference infrastructure: Recasting the right to privacy across surveillance, profiling and generative systems in India. Lex Gazette. <https://lexgazette.com/wp-content/uploads/2026/08/Manuscript-Artificial-Intelligence-As-An-Inference-Infrastructure-Gayatri-Rathi.pdf>
 13. Reddy, J., Baradwaj, A., & Pawar, S. (2025). Digital privacy and State surveillance: An Indian legal and technological perspective. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5330133
 14. Saha, K. (2026). From privacy to digital constitutionalism: Reimagining fundamental rights in India's data-driven democracy after 75 years of constitutional governance. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7009258
 15. Sarankumar, R. (2025). An analysis of the role of the Indian Constitution in protecting digital rights and AI governance. International Journal of Legal Science and Innovation. <https://ijlsi.com/article/view/an-analysis-of-the-role-of-the-indian-constitution-in-protecting-digital-rights-and-ai-governance>
 16. Sharma, K. (2026). Governing algorithmic policing in Himachal Pradesh: Artificial intelligence, privacy, and constitutional accountability. In Applications and strategic implementation of AI in IGI Global. <https://www.igi-global.com/chapter/governing-algorithmic-policing-in-himachal-pradesh/408735>
 17. Singh, A., & Srivastava, R. (2024). Challenges of legal regulation of artificial intelligence: A study with special reference to right to privacy. International Journal of Legal Science and Innovation. <https://ijlsi.com/article/view/challenges-of-legal-regulation-of-artificial-intelligence-a-study-with-special-reference-to-right-to-privacy>
 18. United Nations Educational, Scientific and Cultural Organization. (2021). Recommendation on the ethics of artificial intelligence. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
 19. United Nations General Assembly. (2024). Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (A/RES/78/265). United Nations.