SHIKSHA SAMVAD
International Journal of Multidisciplinary Research
ISSN: 2584-0983 (Online)
© Shiksha Samvad|Volume-03| Issue-04| June- 2026
Available online at: https://shikshasamvad.com/
DOI:- https://doi.org/10.64880/shikshasamvad.v3i4.31

Facial Recognition Technology and the Right to Privacy in India

Asha Maria
Research Scholar, Vikrant University, Gwalior, Madhya Pradesh
Principal I/C, Ambookkan Ittoop Memorial (AIM) College of Law, Thrissur (Dt.), Kerala, India.
Email: ashamarialawaim@gmail.com
ORCID ID: 0009-0003-1070-7683

Abstract:

Facial recognition technology (FRT) has entered into various sectors of government, law enforcement, banking and public infrastructure in India but lacks a specialized regulatory framework for operation. This article discusses the constitutional and statutory aspects of the conflict between FRT and the privacy right, which has been considered as the fundamental right in the case of Justice K.S. Puttaswamy. This article covers doctrinal legal analysis and comparative study of European Union, the United Kingdom and the United States. This article advances the suggestion that Article 21 of the Constitution, the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, are inadequate to address the specific privacy threats posed by biometric surveillance. The paper notes the key deficiencies, including the absence of an independent supervision system, the absence of a requirement for judicial authorization prior to deployment of law enforcement and weak measures concerning algorithmic bias and the chilling effect on constitutionally guaranteed freedoms. It ends with a series of actual legislative and institutional proposals adjusted to India's democratic and developmental circumstances.

Keywords: Facial Recognition Technology, Right to Privacy, Biometric Surveillance, Digital Personal Data Protection Act 2023, Puttaswamy judgment, Algorithmic Bias, Fundamental Rights

Introduction

The growing popularity of facial recognition technology (FRT) across the globe has generated one of the significant jurisprudential questions of the twenty-first century that when can the use of biometric surveillance by the State become constitutionally impermissible. The subject is relevant, especially in India considering the pace and scale of FRT adoption. The National Automated Facial Recognition System (NAFRS) established by the National Crime

Records Bureau (NCRB) is meant to provide a centralized data base to identify people from pictures and CCTV footage across the country. FRT has been embedded in urban surveillance infrastructure for smart cities initiatives in Hyderabad, Bengaluru and Delhi, while Airports Authority of India controlled airports with installed DigiYatra, a biometric boarding system functioning at many airports.

There are major constitutional risks in these operations. In Justice K.S. Puttaswamy (Retd.) v. Union of India, it was concluded that privacy right is an integral element of the right to life and personal liberty protected by Article 21of the Constitution of India. It was clarified by the court that informational privacy, including control over personal data, is a unique and important aspect of this basic right. FRT captures facial geometry, which is possibly the most sensitive type of personal information: it is immutable, outwardly apparent and if compromised, irrecoverable.

However, India does not have a statutory structure particularly governing FRT. The Digital Personal Data Protection Act, 2023 (DPDPA) being a broad law on personal data processing fails to impose sector-specific duties on biometric surveillance by the state. The Information Technology Act, 2000 (ITA) precedes modern FRT and offers only minor protections. The gap in regulation makes it necessary to set conditions for widespread mass monitoring, data abuse and infringement of civil freedoms. This paper aims at mapping this legal terrain, offering a comparative perspective and proposing a normative framework sufficient to the task.

Literature Review

Since the mid-2010s, study on FRT and privacy has developed dramatically, paralleling the rapid spread of the technology. Bhatia places FRT within the larger architecture of the Aadhaar biometric identity system in India, saying that the Indian zeal for biometric governance is reflective of a developmental logic that constantly sacrifices privacy for administrative efficiency. Khosla addresses the consequences of the Puttaswamy ruling for surveillance legislation, concluding that the proportionality test laid out by the Court is the most promising doctrinal tool for curbing the utilisation of FRT. Prasad reviews municipal FRT procurement processes and notes the lack of privacy effect assessments, public input or legal authority in some high-profile installations.

Internationally, Browne gives a powerful account of the racialised history of surveillance technology, showing that facial recognition is the latest in a long line of biometric classification that has traditionally been deployed against underprivileged people. Garvie, Bedoya, and Frankle of the Georgetown Law Center on Privacy & Technology, located broad deployment of FRT in the United States, without legislative authorization or accuracy criteria. On the legal front, Rosen advocates for categorizing facial recognition as a 'category-three' search that requires a warrant. Schwartz says that the existing Fourth Amendment concept is structurally ill-suited to control ambient biometric monitoring. Veale and Borgesius discuss the biometric data regulation under the General Data Protection Regulation (GDPR) in Europe and identify shortcomings that the proposed EU AI Act aims to remedy. Indian literature has not yet

generated a coherent doctrinal account incorporating constitutional law, data protection legislation and comparative analysis, although it is expanding. This paper aims to fill that gap.

Methodology

This paper combines a legal doctrinal technique with comparative analysis. Primary legal documents include constitutional provisions, legislative instruments, judicial decisions and subordinate rules, are evaluated using traditional methodologies of legal interpretation, including textual, purposive and structural approaches. The comparative study is based on the regulatory systems of the United Kingdom, the United States and the European Union on the basis of their sophisticated FRT governance systems and their proven relevance to Indian legislative deliberations.

Legal findings are contextualised through the use of secondary sources such as peer-reviewed publications, policy reports and human rights documentation to examine the practical implementation of legal standards. The paper does not use empirical social science methodologies. Its contribution is normative and analytic, not descriptive or quantitative. Factual assertions about FRT systems are taken from official government documents, technological audits.

Result and Discussion

i. Facial Recognition Technology: Architecture and Applications

FRT is a biometric modality based on artificial intelligence that recognizes or authenticates an individual by studying the spatial geometry of facial features. Contemporary systems operate via a four-stage pipeline: (i) face detection, where the system identifies faces in an image or video frame; (ii) feature extraction, where a mathematical representation ('faceprint') is created; (iii) template comparison, where the faceprint is compared to a database of enrolled templates; and (iv) decision output, where a match score is produced and a threshold applied to give an identification or verification result.

It is necessary to distinguish two modes of operation, Verification systems (one-to-one matching) are used to verify that an individual is who they say they are, such as the DigiYatra airport boarding system. Identification systems (one-to-many matching) search a faceprint against an entire database to determine the identity of an unknown person (as in the NAFRS). The latter is analytically and constitutionally different, because it is based on persons who have not consented to be enrolled, nor submitted their biometric data for the purpose at issue, and because its error rates increase substantially with the size of the database.

FRT is currently deployed across various domains in India: Law enforcement and criminal investigation (NAFRS); Border control and immigration (e-gate systems at international airports); Airport passenger processing (DigiYatra); Banking and financial services (Know Your Customer verification) and Urban governance (smart city CCTV networks). Each domain has its own privacy risk profile, of course, but they share the commonality that the data subject is often unaware of the data collection and has no meaningful opportunity to object.

ii. The Privacy Rights: Constitutional Foundations and Doctrinal Development

The development of the privacy rights in India is architecturally complex. For several decades, the Supreme Court hesitated between acceptance and uncertainty. The eight-judge bench in M.P. Sharma v. Satish Chandra and the bench of six-judge in Kharak Singh v. State of Uttar Pradesh came to different and inconsistent conclusions. The constitutional bench of nine-judge in Justice K.S. Puttaswamy (Retd.) v. Union of India authoritatively resolved this issue by overruling the earlier decisions and unanimously holding that privacy right is a fundamental right and is protected under the Indian Constitution.

The Puttaswamy Judgment pronounced a multidimensional idea of privacy that included bodily integrity, decisional autonomy and informational self-determination. It was held by the Apex Court of India that any action of state encroaching on privacy must satisfy the three-fold test as laid down in Modern Dental College v. State of Madhya Pradesh: (i) it must be legally authorised; (ii) it must possess a lawful state purpose and (iii) it must be essential and proportional to the end sought to be achieved. This proportionality framework was elaborated by the Court in Anuradha Bhasin v. Union of India and Maneka Gandhi v. Union of India and it provides the major constitutional standard against which FRT operations are to be tried.

Biometric data involve the most serious privacy concerns. In the case of Puttaswamy, it was accepted that the first site of privacy is the body. The data sourced from bodily features is more sensitive as it is permanent, non-transferable and exclusively identifying. A password or a PIN can be changed at any time, but the face can't be changed. The hidden collection of facial geometry by the State thus demands serious justification under Article 21.

ii. The use of FRT and Privacy concerns

The basic important risk is the mass surveillance. The state has the ability to track movement of the people in public space, continuously and retrospectively with FRT, CCTV networks and real-time analytics. It differs from traditional surveillance being automated, scalable and invisible to the subject. The European Court of Human Rights has acknowledged in Big Brother Watch v. United Kingdom that bulk interception regimes violate Article 8 ECHR without regarding whether or not there is an analysis of individual data points.

Algorithmic bias is another threat. The US National Institute of Standards and Technology (NIST) by its independent audits, have found that FRT algorithms have significantly higher fault rates. It can be wrong positive and wrong negative for women, older people and people with darker skin tones. In the situation of law enforcement, a wrong positive identification can lead to wrongful arrest. The contact of marginalised communities with the police is extremely higher in India and consequences of algorithmic bias have severe constitutional implication under Articles 14 and 21.

Consent and purpose limitation are other important concerns. Collected data for one purpose may not be reused for another point and is violated when databases are brought together for one governmental scheme (such as voter rolls or passport photographs) and are

repurposed to train or query FRT systems. The individuals who offered photographs for administrative use did not consent to have their faces entered into a law enforcement identification system. The idea of meaningful consent is further challenged in public spaces where people cannot practically avoid being surveilled.

The chilling effect on constitutionally protected liberties is a separate harm and a multiplier of other harms. The knowledge that the state is watching through widespread facial recognition surveillance may discourage people from taking part in political protests, religious services or any other public event they have reason to believe is being monitored. This effect is not speculative: research by Feldstein on AI-enabled surveillance states documents the documented suppression of public dissent in contexts where citizens know that facial recognition is deployed. The same logic applies with equal force to surveillance technologies in India where the Supreme Court has recognised the chilling effect as a constitutional harm in the context of speech restrictions.

Analysis of Legal Framework

The Puttaswamy interpretation is that it extends the protection of Article 21 to privacy. However, Article 21 is a negative right: it restrains state action but does not of itself impose positive obligations to enact specific regulatory regimes. Thus, the constitutional command is one of justification, not prohibition. FRT is not per se unconstitutional, but any deployment must meet the Puttaswamy proportionality standard. Absent enabling legislation, it currently fails to meet the first limb, the requirement of legal authority.

The most recent and directly relevant statutory instrument is the Digital Personal Data Protection Act, 2023. The DPDPA provides for a consent-based regime for processing of personal data, includes biometric data within the definition of 'sensitive personal data' and establishes a Data Protection Board with adjudicatory functions. But the Act has a wide exemption in Section 17 for state processing in the interests of 'sovereignty', 'public order' and 'prevention and detection of offences', which are precisely the reasons for deploying law-enforcement FRT. The Act does not introduce prior authorisation, obligations to evaluate the impact of algorithms or audit mechanisms for biometric surveillance systems.

The Information Technology Act, 2000 (amended in 2008) provides for protection of data only vaguely by Section 43A (reasonable security practices for sensitive personal data) and Section 72A (disclosure of information in breach of a lawful contract). The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, define biometric data as personal data that is sensitive but are applicable only to 'body corporate' entities and not to government agencies. This lacuna means that state FRT systems are presently not subject to any enforceable data protection obligations under the ITA framework.

Government policy on FRT has developed through a combination of administrative circulars, tender specifications, and project-specific authorisations rather than

through legislation. The Automated Facial Recognition System of the NCRB was approved through the process of inter-ministerial, but without the approval of parliament. The absence of a dedicated FRT legal framework and complete executive-level guiding principles, means that accountability for misuse is widespread. The effective judicial review is obstructed by the lack of a well-defined legal framework to challenge.

Comparative Analysis

The European Union have the most advanced legal framework. The GDPR classifies biometric data which is handled for the aim of unique identification of natural persons as a 'special category' and it is bound by enhanced protection. Processing of such data is prohibited in the absence of a clear exception. The proposed EU Artificial Intelligence Act, which entered into force in 2024, classifies real-time remote biometric identification in openly accessible spaces as 'prohibited AI' and it provides a model of layered protection.

In the United Kingdom, the use of FRT by police forces has been challenged through judicial review. In R (Bridges) v. Chief Constable of South Wales Police, the Court of Appeal held that the use of live FRT by South Wales Police infringed both the right to privacy under Article 8 ECHR and the Public Sector Equality Duty under the Equality Act 2010. The UK's approach - a combination of human rights review, data protection regulation and equality law - illustrates how multiple legal instruments can operate in combination to restrict FRT even without specific legislation.

In the United States, the constitutional framework is dissimilar but the legislative response has been enlightening. Absent a federal FRT statute, several cities - including San Francisco, Boston, and Portland - have enacted municipal ordinances prohibiting government use of FRT entirely. Illinois' Biometric Information Privacy Act (BIPA) stipulates a private right of action for biometric data violations and has generated extensive litigation that has created de facto regulatory standards for private-sector FRT. The US experience shows both the legislative creativity that can occur in the absence of federal action and the resulting fragmentation that makes national-level legislation desirable.

Challenges and Suggestions for India

India's problems are doctrinal, institutional and political all at once. The absence of a special law for FRT means that, doctrinally, the constitutional review of FRT deployments must be carried out within the general proportionality framework of Article 21. This framework may be sufficient but lacks the necessary procedural and institutional specificity to govern systematically. The Data Protection Board under the DPDPA is not independent at an institutional level (the members are appointed by the Central Government) and it does not have jurisdiction over state actors in the areas where FRT is most pervasively deployed. There are political incentives for security agencies, smart city planners and technology vendors to deploy, rather than restrain. Here are the following recommendations. First, India needs dedicated FRT legislation that goes beyond the DPDPA in several respects: it should exhaustively define

permissible use cases; require independent prior authorization for law-enforcement identification deployments; impose mandatory algorithmic impact assessments before procurement; require data minimisation and strict purpose limitation; establish a right to challenge FRT-based decisions and create a specialist oversight body with investigative and enforcement powers independent of the executive. Second, the DPDPA should be amended to eliminate or significantly narrow the Section 17 national security exemption in respect of biometric data consistent with the 'strictly necessary' standard of EU law. Third, a warrant-requisite model should be acquainted for judicial authorisation of dentification implementation in public spaces. Fourth, obligations of transparency need to be included in the legislation, requiring public disclosure of all government FRT contracts, demographic-specific correctness metrics and incident reports. Fifth, accountability measures should provide for a statutory private right of action for individuals and personal liability for public officials for the misuse of FRT data.

Conclusion

Facial recognition technology is not fundamentally contrary with constitutional democracy; its compatibility joints entirely on the legal and institutional context within which it operates. India's current regime lacks statutory support for the most interfering FRT uses. It has no independent supervision and exempts state actors from the most important data protection obligations. There is a failure to address the unique risks of algorithmic bias in a diverse society. The Puttaswamy judgment stipulates the constitutional base for regulatory reform and it is for the Parliament to achieve that direction. The comparative experience of the EU, the UK and the US indicates that strong FRT governance can be achieved through a combination of prohibition of the most invasive uses, previous authorisation requirements for law enforcement, independent oversight, transparency responsibilities and enforceable individual rights. India can learn from each of these regimes, even as it tailors the framework to its own constitutional structure, institutional capacity and development priorities. The object is not to prevent valid uses of a powerful technology but to make sure that the use of the technology does not come at the expense of the fundamental rights that define India as a constitutional republic.

Path Forward

A number of questions require further scholarly attention. Firstly, as large language models and generative AI become able to reconstruct facial data from partial inputs, the regulatory perimeter of 'facial recognition' will need to be dynamically redefined. Second, empirical work is needed at the intersection of FRT with India's caste and religious diversity. Existing audit literature is largely based on North American and European demographic data and Indian-specific accuracy studies are truly needed to inform proportionate regulation. Third, the institutional design challenges of the enforcement architecture of any future FRT statute and in particular the design of an independent oversight body capable of regulating state actors are beyond the scope of this article and deserve separate treatment. Fourth, the implications of FRT

for electoral integrity will become more salient as state election commissions explore the use of biometric authentication, particularly in the context of voter verification systems.

REFERENCES

1. National Crime Records Bureau, Ministry of Home Affairs. (2019). *Automated facial recognition system: Request for proposal*. Government of India.
2. Ministry of Housing and Urban Affairs. (2022). *Smart Cities Mission: Guidelines* (Updated ed.). Government of India. (Original work published 2015)
3. Airports Authority of India. (2023). *DigiYatra: Paperless and seamless travel*. Government of India. https://www.digiyatra.in
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
5. Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts* (Ch. 9). HarperCollins.
6. Khosla, M. (2021). Surveillance law and proportionality after Puttaswamy. *Indian Law Review*, *5*(1), 45–68.
7. Prasad, V. (2022). Facial recognition in Indian smart cities: An audit of procurement and accountability. *Economic and Political Weekly*, *57*(34), 34–41.
8. Browne, S. (2015). *Dark matters: On the surveillance of Blackness*. Duke University Press.
9. Garvie, C., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law Center on Privacy & Technology.
10. Rosen, J. (2012). The deciders: The future of privacy and free speech in the age of Facebook and Google. *Fordham Law Review*, *80*(4), 1525–1538.
11. Schwartz, P. M., & Peifer, K. N. (2017). Paragraph III data protection: The German approach to protecting biometric data. *California Law Review*, *105*(2), 617–671.
12. Veale, M., & Borgesius, F. Z. (2021). Analysing the upcoming EU Artificial Intelligence Regulation. *Computer Law Review International*, *22*(4), 97–112.
13. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20.
14. Phillips, P. J., et al. (2011). An introduction to the good, the bad, and the ugly face recognition challenge problem. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 346–353.
15. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).
16. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
17. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
18. Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
19. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
20. Maneka Gandhi v. Union of India, AIR 1978 SC 597 (India).

21. Big Brother Watch v. United Kingdom, App. No. 58170/13 (Eur. Ct. H.R. Grand Chamber, 2021).
22. Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology.
23. Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
24. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
25. Internet Freedom Foundation. (2021). *Project Panoptic: Tracking facial recognition in India*. https://panoptic.in
26. Council of the European Union. (2016). General Data Protection Regulation (EU) 2016/679, art. 9. *Official Journal of the European Union*, L 119, 1–88.
27. European Parliament and Council of the European Union. (2024). Regulation on Artificial Intelligence (AI Act), Regulation 2024/1689. *Official Journal of the European Union*, L 1689.
28. R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058 (Eng.).
29. Gumbs, A. (2021). Banning facial recognition: A survey of municipal ordinances in the United States. *Harvard Journal on Legislation*, *58*(1), 165–202.
30. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (2008).

Cite this Article:

Asha Maria, "Facial Recognition Technology and the Right to Privacy in India" Shiksha Samvad International Open Access Peer-Reviewed & Refereed Journal of Multidisciplinary Research, ISSN: 2584-0983 (Online), Volume 03, Issue 04, Pp.294-302, June-2026. Journal URL: https://shikshasamvad.com/

CERTIFICATE

of Publication

This Certificate is proudly presented to

Asha Maria

For publication of research paper title

Facial Recognition Technology and the Right to Privacy in India

Published in 'Shiksha Samvad' Peer-Reviewed and Refereed Research Journal and E-ISSN: 2584-0983(Online), Volume-03, Issue-04, Month June 2026.

Dr. Neeraj Yadav
Editor-In-Chief

Dr. Lohans Kumar Kalyani
Executive-chief- Editor

Note: This E-Certificate is valid with published paper and the paper must be available online at: https://shikshasamvad.com/

DOI:- https://doi.org/10.64880/shikshasamvad.v3i4.31