Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Facial Recognition and Privacy: Constitutional Limits on State Surveillance in India

Priyal Agrawal[a]

[a]Symbiosis Law School, Noida, India

Received 02 October 2026; *Accepted* 02 November 2026; *Published* 06 November 2026

The increasing deployment of Facial Recognition Technology (FRT) by Indian law enforcement agencies raises significant concerns regarding the constitutional protection of privacy, personal liberty and civil freedoms. This paper examines whether State use of FRT complies with the requirements of legality, necessity and proportionality under Article 21 of the Constitution of India, particularly in light of the landmark judgment in Justice K.S. Puttaswamy v Union of India. Adopting a doctrinal research methodology, the study analyses constitutional provisions, statutory frameworks, judicial precedents and comparative legal developments. It evaluates the regulatory limitations of the Digital Personal Data Protection Act, 2023, and the Criminal Procedure (Identification) Act, 2022, alongside concerns relating to algorithmic bias, mass surveillance, function creep and the chilling effect on fundamental freedoms. The paper argues that existing legal safeguards are inadequate and that unrestricted deployment risks arbitrary State surveillance. It recommends dedicated legislation, independent oversight, judicial authorisation and proportionate safeguards to ensure constitutionally compliant use of FRT.

Keywords: *facial recognition, privacy, surveillance.*

INTRODUCTION

In 2019, the National Crime Records Bureau invited bids for a National Automated Facial Recognition System, a central platform against which any face captured on camera could be

matched to a database of images.[1] State police forces, including in Telangana, have also deployed similar tools, and their use has been challenged in court.[2] Each camera becomes a checkpoint where people are identified without being stopped, questioned or suspected of anything. A face differs from a password or a card. It is displayed constantly, captured from a distance and cannot be changed if misused. Yet India has no statute that expressly authorises or regulates police use of facial recognition technology (FRT). The problem is therefore constitutional: the State is building surveillance capacity through executive decision alone, after the Supreme Court held privacy to be a fundamental right.[3]

This paper asks whether, and to what extent, State use of FRT meets the legality, necessity and proportionality requirements of Article 21.[4] It argues that, without a specific law and independent safeguards, present deployment is unlikely to satisfy them, although narrow and regulated uses can be justified.

OBJECTIVES

The paper has four objectives:

- To examine the constitutional basis of the right to privacy and the test for restricting it;
- To analyse whether current State use of FRT meets that test;
- To evaluate whether the Digital Personal Data Protection Act 2023[5] and related laws adequately regulate it;
- To recommend safeguards.

RESEARCH QUESTION

Does the use of facial recognition technology by Indian law enforcement satisfy the legality, necessity and proportionality requirements that Article 21 of the Constitution imposes on State intrusions into privacy?

[1] *Request for Proposal for the National Automated Facial Recognition System* (NCRB, 2019)
[2] *S Q Masood v State of Telangana & Ors* (2022) Special Leave to Appeal (C) No(s) 12926/2021
[3] *Justice K S Puttaswamy & Anr (Retd) v Union of India & Ors* (2017) 10 SCC 1
[4] The Constitution of India 1950, art 21
[5] Digital Personal Data Protection Act 2023

RESEARCH METHODOLOGY

The methodology is doctrinal. Primary sources are the Constitution, statutes and judgments of Indian courts. Secondary sources are journal articles and reports. Materials from the United Kingdom, the United States and the European Union are used only for comparison and do not displace Indian law. The paper is limited to State use of FRT by law enforcement; private-sector uses, such as access control in offices, raise different questions and are not examined. It also relies on published sources, so claims about the extent of deployment are necessarily cautious.

APPLICABLE LEGAL FRAMEWORK

The Constitution: Article 21 protects life and personal liberty except according to procedure established by law, and since *Maneka Gandhi*, that procedure must be fair, just and reasonable.[6] Articles 19(1)(a) and 19(1)(b) protect free speech and peaceful assembly, and may be restricted only by reasonable restrictions under Articles 19(2) and 19(3).[7] Article 14 guarantees equality, which matters if a system performs worse for some groups, because unequal error rates can amount to unequal treatment by the State. These provisions operate together, so a measure that burdens one right must be examined against the others as well.

The Puttaswamy Test: A nine-judge bench held privacy to be intrinsic to Article 21. The plurality opinion of Chandrachud J requires any State intrusion to satisfy three conditions: legality (a law must authorise it), a legitimate State aim, and proportionality between the means chosen and the aim pursued. Kaul J added that informational privacy must be protected against profiling and surveillance.[8]

Statutes: The Digital Personal Data Protection Act 2023 regulates digital personal data, but section 17(2)(a) allows the Central Government to exempt State instrumentalities by notification, on grounds such as security and public order.[9] The Information Technology Act 2000 and the 2011 Rules treat biometric data as sensitive, but the Rules bind body corporates, not the police.[10] The Criminal Procedure (Identification) Act 2022 permits collection of

[6] *Maneka Gandhi v Union of India* (1978) 1 SCC 248
[7] The Constitution of India 1950, arts 19 and 21
[8] *Justice K S Puttaswamy & Anr (Retd) v Union of India & Ors* (2017) 10 SCC 1
[9] Digital Personal Data Protection Act 2023, s 17(2)(a)
[10] Information Technology Act 2000; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

photographs and other measurements from convicts and arrested persons and allows retention for up to 75 years, but it does not address matching live camera feeds of ordinary people against databases.[11]

CASE LAWS

Kharak Singh[12] is the early surveillance case. The Court struck down night-time domiciliary visits but declined to recognise a general fundamental right to privacy. *Puttaswamy* overruled it on that point and now anchors the analysis.

Puttaswamy itself was decided in 2017 on a reference arising from the Aadhaar challenge. The Court held that privacy covers bodily integrity, personal autonomy and informational self-determination, and that it is not lost merely because a person is in a public place. Biometric identifiers fall squarely within informational privacy, so a State programme that captures and matches faces must justify itself under the three-part test.

PUCL v Union of India concerned telephone tapping under the Telegraph Act.[13] Because the power was unguided, the Court laid down safeguards: authorisation at a senior executive level, limits on duration and a review committee. This is a useful model for FRT, which is equally intrusive and equally unregulated.

Modern Dental College set out the Indian proportionality test, and *Puttaswamy (Aadhaar)* applied it: the measure must pursue a legitimate goal, be suitable to that goal, be necessary because no less restrictive alternative is equally effective, and strike a fair balance with the right affected.[14] *Anuradha Bhasin* confirmed that restrictions on fundamental rights must be proportionate, reasoned, published and open to review.[15]

No Supreme Court judgment has yet decided the lawfulness of police FRT. Comparative decisions help. In *Bridges*, the English Court of Appeal held that police use of live facial recognition breached Article 8 of the European Convention because the legal framework left

[11] Criminal Procedure (Identification) Act 2022
[12] *Kharak Singh v State of U P & Ors* (1964) 2 SCJ 107
[13] *People's Union for Civil Liberties v Union of India & Anr* (1997) 1 SCC 301; Indian Telegraph Act 1885
[14] *Modern Dental College & Res Ctr & Ors v State of Madhya Pradesh & Ors* (2016) 7 SCC 353; *Justice K S Puttaswamy (Retd) v Union of India* (2019) 10 SCC 1
[15] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637

too much discretion to individual officers.[16] In *Carpenter*, the US Supreme Court held that aggregated location tracking was a search despite taking place in public.[17]

ANALYSIS AND DISCUSSION

This Part applies the method of rule, application and evaluation to each requirement of the *Puttaswamy* test. It first presents the case against State use of FRT, which forms the main thesis of the paper, and then the case in favour, so that the strongest State arguments are tested openly in Part 6 rather than ignored. Throughout, the aim is to remain analytical and to keep the tone neutral, since the question is one of constitutional limits and not of whether the technology is good or bad in itself.

Arguments against State use of FRT –

Legality: The rule is that a law must authorise the intrusion. In application, NAFRS and State deployments rest on administrative decisions and procurement, with no statute defining who may be scanned, for which offences, on whose authority, or for how long data is kept. A power that is not accessible or foreseeable is not a law in the sense *Puttaswamy* requires. The position is weaker than in *Bridges*, where at least some statutory and common law framework existed.[18] The EU has gone further and generally prohibits real-time remote biometric identification in public spaces for law enforcement, subject to narrow exceptions.[19]

Proportionality: The rule requires necessity: no less restrictive means equally effective. Public-space FRT scans everyone to find a few, so most of those processed are innocent. Matching a face against a list of identified suspects under prior authorisation is far less intrusive than blanket scanning. Nothing comparable to the *PUCL* safeguards currently exists, so the balancing limb cannot be shown to be satisfied.

Accuracy and Bias: Research on commercial systems found markedly higher error rates for darker-skinned women than for lighter-skinned men.[20] A false match can lead to wrongful

[16] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA (Civ) 1058
[17] *Carpenter v United States* [2018] 138 S Ct 2206
[18] *Justice K S Puttaswamy & Anr (Retd) v Union of India & Ors* (2017) 10 SCC 1
[19] Harmonised Rules on Artificial Intelligence 2024
[20] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research <https://proceedings.mlr.press/v81/buolamwini18a.html> accessed 01 October 2026

questioning or arrest, engaging Articles 14 and 21. Indian deployments publish little independent accuracy data.

Chilling Effect: People who know they can be identified may avoid protests and meetings. This engages Articles 19(1)(a) and 19(1)(b), and *Anuradha Bhasin*[21] shows the Court treats restrictions on these freedoms as requiring justification and review. Finally, a face cannot be reset after a breach, so large centralised databases create lasting risk.

Function Creep and Oversight: A system built to find missing children can be repurposed to identify protesters or monitor communities, because the same database and software serve both ends. Without purpose limitation in law and an independent body to audit use, citizens cannot know or challenge how their faces are used. *PUCL* shows that the Court regards review mechanisms as part of what makes a surveillance power fair.

Arguments in favour of State use of FRT –

Legitimate Aim: Preventing and detecting crime and protecting security are accepted aims. Article 19(2) itself recognises the security of the State and public order. *Puttaswamy* did not treat privacy as absolute, and the first limb of its test is plainly capable of being met.

Efficiency: Proponents point to tracing missing children, identifying suspects in crowds and reducing reliance on witness identification, which is itself error-prone. Automated matching can process footage no human team could review.

Reduced Expectation of Privacy in Public: The State may argue that a person who appears in public cannot expect anonymity, and that FRT only automates what an officer could do by sight. It may add that accuracy is improving and that technology should not be rejected merely because it can be misused.

Administrative Safeguards are Enough: The State may also contend that internal standard operating procedures, human verification of matches and limited retention periods already prevent abuse, so that a dedicated statute is unnecessary and would slow useful policing. This argument has some force for low-intrusion uses, such as matching a photograph of a missing child against a closed database.

[21] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637

COUNTER-ARGUMENT AND ALTERNATIVE PERSPECTIVE

These arguments deserve fair acknowledgement. Security needs are real, and for serious crime and missing persons the legitimate aim is clearly met. The difficulty lies elsewhere. First, a legitimate aim is only the first limb; it cannot cure the absence of law or of necessity.

Second, the public-place argument is weak. *Puttaswamy* locates privacy in the person, not the place, and *Carpenter* recognised that aggregating movements in public reveals far more than any single observation. An officer's glance and a searchable, permanent record of every face are different in scale and consequence.

Third, improved accuracy does not resolve the legality problem. A perfectly accurate system would increase surveillance power and sharpen the need for rules about who may be identified and why. The proper conclusion is not that FRT must be abandoned, but that it must be authorised and constrained by law.

Fourth, internal procedures are not a substitute for law. Standard operating procedures can be changed or withdrawn by the same authority they bind, are often unpublished, and give individuals no remedy. *Puttaswamy* and *Anuradha Bhasin* both require a standard that is public and reviewable. Safeguards of that kind are best placed in legislation, with independent oversight, rather than left to the discretion of the agency using the technology.

RESEARCH GAP AND CRITICAL FINDING

The law in this area is unclear and outdated, and several questions remain unanswered. The 2023 Act can exempt State agencies from its protections, and the Srikrishna Committee had separately noted the need for reform of surveillance law. The Identification Act 2022[22] is silent on facial matching of the general public. No FRT-specific statute, independent oversight body or mandatory impact assessment exists. No Supreme Court ruling has addressed police FRT. Courts and legislators have not answered when, if ever, real-time public identification is constitutionally permissible. The Telangana petition, the main judicial test to date, has not, to the author's knowledge, produced a final ruling. Equally unresolved is who audits accuracy, how long images may be kept, and what remedy a person has after a false match. Comparative systems show that these questions can be answered in law, which suggests the

[22] Criminal Procedure (Identification) Act 2022

Indian gap is one of legislative choice rather than technical impossibility. This is where further research and legislative attention are needed.

CONCLUSION AND RECOMMENDATIONS

State use of FRT in India does not currently satisfy Article 21[23] as interpreted in *Puttaswamy*.[24] No specific law supplies legality, blanket scanning struggles to meet necessity, and independent oversight is absent. Narrow, targeted use against serious offences can in principle be justified. Parliament should therefore enact a dedicated statute that defines permitted purposes, requires judicial or independent authorisation for non-emergency use, mandates necessity and impact assessments and accuracy testing, sets retention and deletion limits, provides audit and remedies, and prohibits blanket real-time scanning of public spaces.

[23] The Constitution of India 1950, art 21
[24] *Justice K S Puttaswamy & Anr (Retd) v Union of India & Ors* (2017) 10 SCC 1