



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CONSTITUTIONAL CHALLENGES OF AI-BASED SURVEILLANCE IN INDIA

Examining Facial Recognition Technology, Privacy, Judicial Precedents and Regulatory Needs

AUTHORED BY - ROHAN V, KARTHIKEYAN S & BHARATH S

Abstract

Artificial intelligence is changing the way governments and law-enforcement agencies identify people, manage information and conduct surveillance. Facial Recognition Technology (FRT) is one of the most significant examples because it can compare facial images with stored records and, in some settings, operate at scale. The technology may assist legitimate functions such as identifying suspects or missing persons, but its use also raises questions about privacy, equality, personal liberty and democratic freedoms. This paper examines the constitutional issues surrounding AI-based surveillance in India, with particular attention to Articles 14, 19 and 21 of the Constitution. It studies the development of privacy jurisprudence and considers the relevance of decisions including *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *Maneka Gandhi v. Union of India*, *Anuradha Bhasin v. Union of India* and the Delhi High Court proceedings in *Sadhan Haldar v. State (NCT of Delhi)*. The paper also considers the Criminal Procedure (Identification) Act, 2022 and the Digital Personal Data Protection Act, 2023 as parts of the wider legal environment, while recognising that neither provides a complete, technology-specific framework for every form of FRT deployment. The paper argues for a rights-centred approach in which security objectives are pursued through clear legal authority, defined purposes, proportionality, data safeguards, accuracy testing, human review and meaningful accountability. The aim is not to treat technology and constitutional rights as opposing ideas, but to identify legal conditions under which innovation can operate consistently with privacy, equality, liberty and the rule of law.

Keywords: Artificial Intelligence; Facial Recognition Technology; Surveillance; Privacy; Article 14; Article 19; Article 21; Proportionality; Algorithmic Bias; Data Protection.

1. Introduction

Artificial intelligence has moved from being a specialised technological field to becoming part of everyday governance and public administration. One of its most visible applications is Facial Recognition Technology (FRT), which uses computer vision and machine-learning techniques to identify or verify people from facial images. When connected to cameras and databases, the technology can make identification much faster and can also operate on a large scale.

In India, the use of facial recognition has developed alongside broader digital governance, policing and biometric identification initiatives. The technology has attracted attention because it can serve practical purposes, including the identification of persons of interest and efforts to locate missing persons. At the same time, the same technology can be used to observe and identify people who are not suspected of wrongdoing. That difference matters constitutionally. The central question is therefore not whether FRT is useful. The more difficult question is how the State should exercise this capability without allowing surveillance to become arbitrary, excessive or insufficiently accountable.

The Supreme Court's recognition of privacy as a fundamental right has made this question particularly important.

Any analysis of AI-based surveillance must consequently consider the relationship between technological capability and constitutional limits.

This paper focuses on FRT as a concrete example of AI-based surveillance. It examines the implications for equality under Article 14, freedoms under Article 19 and privacy and personal liberty under Article 21. It then considers judicial principles, existing statutory provisions and the need for additional safeguards.

2. Statement of the Problem

The rapid development of facial recognition creates a gap between what technology makes possible and what the law clearly regulates. A camera system can record a face, an algorithm can convert the image into a biometric template, and a database can be searched for a possible match. Each stage raises a different legal question: who may collect the data, for what purpose, under what authority, how long it may be retained, who may access it, and what happens when the system is wrong?

The problem becomes more serious when a system moves from limited identification to continuous or widespread monitoring. In such circumstances, individuals may have little

practical knowledge of the processing taking place.

They may also have difficulty challenging an incorrect match or finding out how an automated decision was reached.

The research therefore addresses the constitutional and regulatory uncertainty surrounding the use of FRT by public authorities. It does not assume that every use of facial recognition is unlawful. Instead, it asks what legal conditions and safeguards are required for such use to remain compatible with fundamental rights.

3. Objectives of the Study

The main objective of this research is to examine the constitutional challenges created by AI-based surveillance, with FRT as the principal case study. The specific objectives are:

1. To examine the relationship between FRT and Articles 14, 19 and 21 of the Constitution.
2. To explain the relevance of the constitutional right to privacy to biometric surveillance.
3. To analyse judicial principles that regulate State interference with fundamental rights.
4. To examine relevant statutory developments, including the Criminal Procedure (Identification) Act, 2022 and the Digital Personal Data Protection Act, 2023.
5. To identify concerns relating to mass surveillance, function creep, algorithmic bias and wrongful identification.
6. To suggest practical legal and institutional safeguards for responsible deployment.

4. Research Questions

The study is guided by the following questions:

1. What constitutional rights are most directly affected by AI-based facial surveillance?
2. How does the right to privacy limit State use of FRT?
3. What Article 14 concerns can arise from inaccurate or discriminatory algorithmic outcomes?
4. Can widespread facial tracking affect freedoms protected by Article 19?
5. Do existing Indian laws provide sufficient safeguards for every form of FRT deployment?
6. What regulatory and institutional measures can improve transparency, accountability and protection of individual rights?

5. Research Methodology

This is a doctrinal and analytical legal study. It examines constitutional provisions, judicial decisions, legislation and policy material relating to privacy, surveillance, biometric identification and AI-based systems.

The research uses primary legal sources to identify constitutional principles and secondary literature to understand the technological and policy concerns surrounding FRT.

The study is qualitative rather than empirical. It does not claim to measure the accuracy of a particular facial recognition product or to determine the frequency of wrongful matches in India. Instead, it examines the legal questions that arise from the capability of FRT and assesses those questions against constitutional standards.

The analysis is deliberately framed around the distinction between legitimate, targeted uses and broad or continuous surveillance. This distinction is important because the constitutional assessment depends not only on the technology itself but also on the purpose, scale, safeguards and consequences of its use.

6. Understanding Facial Recognition Technology

Facial Recognition Technology is a biometric technology that uses facial characteristics to identify or verify a person. A simplified FRT process begins with image capture. Software then detects a face, identifies relevant facial features, converts them into a mathematical representation and compares that representation with images or templates in a database.

The technology can be used for one-to-one verification, where a person claims an identity, or for one-to-many identification, where a face is compared against a database to find possible matches. The second form creates more significant surveillance concerns because a person can be identified without actively presenting an identity claim.

FRT therefore has two sides. On one side, it can support investigations and help authorities work with large amounts of visual information. On the other, its scale can reduce practical anonymity in public spaces and create consequences when a system produces a false match. Legal regulation must address both sides rather than treating FRT as either inherently beneficial or inherently harmful.

7. Constitutional Framework: Articles 14, 19 and 21

7.1 Article 14 – Equality and Non-Arbitrariness

Article 14 requires the State to act consistently with equality before the law and equal

protection of the laws.

In the context of FRT, concerns can arise where an algorithm produces systematically different error rates across groups, or where authorities use the technology in a selective or arbitrary manner. A false match can also have serious consequences if it becomes the basis for further police action. These concerns make accuracy, testing, record-keeping and review important safeguards.

7.2 Article 19 – Speech and Peaceful Assembly

Article 19(1)(a) protects freedom of speech and expression, while Article 19(1)(b) protects the right to assemble peaceably and without arms, subject to constitutional restrictions. Pervasive identification at public gatherings may create a chilling effect if people reasonably believe that participation will be individually recorded and identified. The legal question is therefore not simply whether surveillance exists, but whether its purpose, method and scale are justified by law.

7.3 Article 21 – Privacy and Personal Liberty

Article 21 is central to the legal analysis because facial recognition involves the processing of information linked to an identifiable individual. The Supreme Court's privacy jurisprudence recognises privacy as part of constitutional liberty and dignity. The collection and use of facial information therefore require careful consideration of legality, purpose and proportionality.

8. Privacy and the Proportionality Framework

The nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) recognised the right to privacy as a fundamental right. The judgment placed privacy within the constitutional protection of Part III and connected it with liberty, dignity and autonomy.

The proportionality analysis developed in subsequent constitutional jurisprudence is particularly useful for surveillance questions. A rights-intrusive measure should have a lawful basis and pursue a legitimate objective.

There should be a rational connection between the measure and that objective, and the State should consider whether a less restrictive alternative is available. Finally, the impact on rights must be balanced against the importance of the public objective.

For FRT, this means that the existence of a security objective does not end the constitutional inquiry. The authority using the system should be able to identify the legal basis, the specific purpose, the categories of persons affected, the safeguards in place and the reasons why the chosen level of surveillance is necessary. This approach also helps distinguish

targeted identification from indiscriminate monitoring.

9. Judicial Precedents Relevant to AI Surveillance

9.1 Justice K.S. Puttaswamy (Retd.) v. Union of India

The 2017 privacy judgment is the constitutional starting point for analysing modern surveillance. It confirms that privacy is a fundamental right and provides the foundation for examining State action that interferes with privacy.

9.2 Maneka Gandhi v. Union of India

The judgment gave Article 21 a broad and substantive interpretation and emphasised that procedures affecting personal liberty must satisfy constitutional requirements of fairness and reasonableness. Its wider significance is that liberty cannot be separated from the quality of the procedure used by the State.

9.3 Anuradha Bhasin v. Union of India

The Supreme Court applied proportionality principles while considering restrictions on fundamental freedoms. The case is relevant to surveillance because it demonstrates the need to examine the justification, scope and duration of rights-restrictive measures.

9.4 Sadhan Haldar v. State (NCT of Delhi)

The Delhi High Court proceedings are relevant to the use of facial recognition in the context of missing children.

The orders record discussion of the Delhi Police's facial-recognition software and the need to improve mechanisms for locating missing children. The case is better understood as an example of an identified and limited use context; it should not be cited as a general Supreme Court ruling declaring that FRT is constitutionally valid or invalid.

9.5 PUCL v. Union of India

The telephone-tapping jurisprudence of PUCL is important to the broader law of surveillance because it illustrates the constitutional importance of procedural safeguards when the State exercises intrusive monitoring powers.

10. Statutory and Regulatory Landscape

India's legal framework relevant to biometric and digital surveillance is spread across different instruments. This fragmented structure makes it important to examine each law for its actual scope rather than treating any one statute as a complete FRT law.

The Criminal Procedure (Identification) Act, 2022 expands the kinds of measurements that

may be taken for specified criminal-justice purposes and provides for collection, storage and sharing of records. It is relevant to biometric identification, but it does not amount to a comprehensive statute regulating every public-space facial recognition deployment.

The Digital Personal Data Protection Act, 2023 also forms part of the data-governance framework.

Section 17 contains specific exemptions, including provisions concerning processing for prevention, detection, investigation or prosecution of offences and certain notified State instrumentalities. These exemptions make it especially important to examine how surveillance practices are governed by other legal rules and constitutional standards.

The important point is that the existence of data-protection legislation does not, by itself, resolve every constitutional question concerning facial recognition. Issues of statutory authority, purpose, proportionality, accuracy, oversight and remedies continue to require separate consideration.

11. Constitutional Challenges in FRT Deployment

11.1 Mass or Indiscriminate Surveillance

The greatest constitutional concern arises when facial recognition changes from targeted identification into continuous monitoring. A system that attempts to identify everyone passing a camera is materially different from a system used to verify a person in a defined investigation.

11.2 Function Creep

Information collected for one purpose may later be used for another. This can undermine purpose limitation and make it difficult for individuals to know how their biometric information is being used. Purpose limitation is therefore a practical constitutional safeguard as well as a data-governance principle.

11.3 Algorithmic Bias

Facial recognition systems can produce errors, and performance can vary depending on the system, dataset and conditions in which the technology is used. Where errors have unequal effects, Article 14 concerns may arise.

Independent testing and transparent performance reporting are consequently important.

11.4 Wrongful Identification

A facial match is an investigative lead, not necessarily proof of identity or guilt. Treating an automated match as conclusive can create serious risks of mistaken police action.

Human verification and procedural safeguards are necessary before a match produces adverse consequences.

11.5 Chilling Effects

People may behave differently when they believe that their movements or participation in public activities can be identified and recorded. This concern connects privacy with the practical exercise of freedoms under Article 19.

12. Regulatory Gaps and Accountability

The main regulatory challenge is not simply that technology is developing quickly. It is that the legal framework must clearly allocate responsibility at every stage of the surveillance process.

A robust system should identify the authority responsible for deployment, define permissible purposes, establish retention periods, control access to biometric databases and record how searches are conducted. It should also provide independent mechanisms for auditing accuracy and investigating misuse.

Transparency is equally important. Individuals cannot effectively challenge a system if the government agency does not disclose basic information about its purpose, legal authority and safeguards. At the same time, legitimate security interests may require some information to remain confidential. The regulatory challenge is therefore to create meaningful accountability without unnecessarily exposing sensitive operational information. The study also finds that grievance redressal deserves greater attention. Where an individual is incorrectly identified, there should be a practical route to challenge the error and correct the record. Accountability should not begin only after serious harm has occurred.

13. Findings of the Study

The research leads to the following findings.

First, FRT can serve legitimate public purposes, but the constitutional assessment depends on how and why it is used.

Second, privacy is a central constitutional concern because facial recognition involves the collection and processing of information connected to identifiable individuals.

Third, Article 14 becomes relevant where automated systems or administrative practices produce arbitrary or discriminatory outcomes.

Fourth, Articles 19(1)(a) and 19(1)(b) may become relevant where widespread monitoring has

a chilling effect on speech or peaceful assembly.

Fifth, the proportionality framework requires more than a general claim of public safety. The State should be able to show lawful authority, a legitimate objective, a rational connection, necessity and a proportionate impact.

Sixth, existing statutes address parts of the broader biometric and data-governance environment, but they should not be described as a single, comprehensive FRT-specific regulatory framework.

Finally, legal safeguards need to be accompanied by technical safeguards. Independent testing, human review, access controls and mechanisms for correcting errors are essential if automated identification is to be used responsibly.

14. Recommendations

1. Clear statutory authority: Public deployment of FRT should have a clearly identifiable legal basis and defined limits.
2. Purpose limitation: Authorities should specify the precise purpose for which facial data and recognition systems are used. Expansion to unrelated purposes should require fresh legal justification.
3. Necessity and proportionality assessment: Before deployment, authorities should document why FRT is necessary and why less intrusive alternatives are inadequate.
4. Independent oversight: Significant surveillance programmes should be subject to independent review, auditing and periodic assessment.
5. Accuracy and bias testing: Systems should undergo independent testing using representative datasets, with results and limitations documented for accountable decision-making.
6. Human verification: A facial-recognition match should not, by itself, be treated as conclusive proof of identity.
Human review should be required before serious adverse action is taken.
7. Data minimisation and retention limits: Collection and retention should be limited to what is necessary for the specified lawful purpose, with secure deletion procedures.
8. Grievance redressal: Individuals should have an accessible mechanism to challenge incorrect identification and seek correction or other appropriate remedies.
9. Parliamentary accountability: Large-scale surveillance programmes should be subject to democratic scrutiny and clear institutional responsibility.

10. Periodic review: Surveillance systems should not be treated as permanent simply because they have been deployed.

Their necessity, effectiveness and rights impact should be reviewed periodically.

15. Discussion

The constitutional debate around AI-based surveillance is ultimately a debate about the exercise of public power.

The State may have genuine reasons to use technology for public safety, but the presence of a legitimate objective does not remove the need for legal safeguards. The more intrusive the technology, the more carefully its purpose, scope and consequences should be examined. FRT also illustrates why constitutional analysis cannot be separated completely from technical design. A legal rule requiring proportionality has little practical value if the system is inaccurate, if there is no record of how a match was generated, or if an individual has no way to challenge the result. Conversely, technical accuracy alone does not make a surveillance system constitutionally permissible. A highly accurate system can still be used for an unlawful or excessive purpose.

The appropriate approach is therefore one of accountable innovation. Security needs, technological development and individual rights do not necessarily have to be treated as mutually exclusive. They can coexist when surveillance is based on clear authority, narrowly defined purposes, reliable systems, independent oversight and effective remedies.

16. Conclusion

Facial Recognition Technology demonstrates both the possibilities and the difficulties created by AI-based surveillance. It can assist public authorities in identification and investigation, but its ability to operate at scale also creates serious questions concerning privacy, equality, liberty and democratic participation.

In India, Articles 14, 19 and 21 provide the principal constitutional framework for examining these questions.

The privacy jurisprudence beginning with *Puttaswamy*, together with the broader principles developed in *Maneka Gandhi*, *Anuradha Bhasin* and surveillance cases such as *PUCL*, requires State action to be supported by law and justified through constitutional standards.

The research does not suggest that every use of FRT should be treated in the same way. Instead, it highlights the importance of purpose, scale, necessity, safeguards and accountability. A

targeted system used for a clearly defined and lawful objective raises different questions from continuous identification of everyone in a public space.

India would benefit from a clearer rights-centred framework for AI surveillance that brings together statutory authority, proportionality, data safeguards, technical auditing, human review, independent oversight and effective remedies. Such an approach would allow technological tools to support legitimate public objectives while keeping their use within the boundaries of constitutional governance and the rule of law.

17. References

1. Constitution of India.
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
3. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
4. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
5. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
6. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
7. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
8. *Sadhan Haldar v. State (NCT of Delhi) & Ors.*, W.P. (Crl.) 1560/2017, Delhi High Court orders (2019).
9. Criminal Procedure (Identification) Act, 2022.
10. Digital Personal Data Protection Act, 2023, especially Section 17.
11. NITI Aayog, *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology*.
12. Smriti Parsheera, *Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?*, Data Governance Network Working Paper 05.
13. Faizan Mustafa & Utkarsh Leo, *On Facial Recognition and Fundamental Rights in India: A Law and Technology Perspective*.
14. Rahul Sharma & Virender Negi, *Facial Recognition Surveillance and the Indian Constitution: A Critical Analysis of Privacy, Equality & State Power*, International Journal of Law Management & Humanities, Vol. 9, Issue 2 (2026).

Publication note: This manuscript has been edited for clarity, natural academic flow and consistency. It should still be formatted according to the specific journal's author guidelines before submission, including its required citation style, word limit, plagiarism declaration, author-affiliation format and reference requirements.