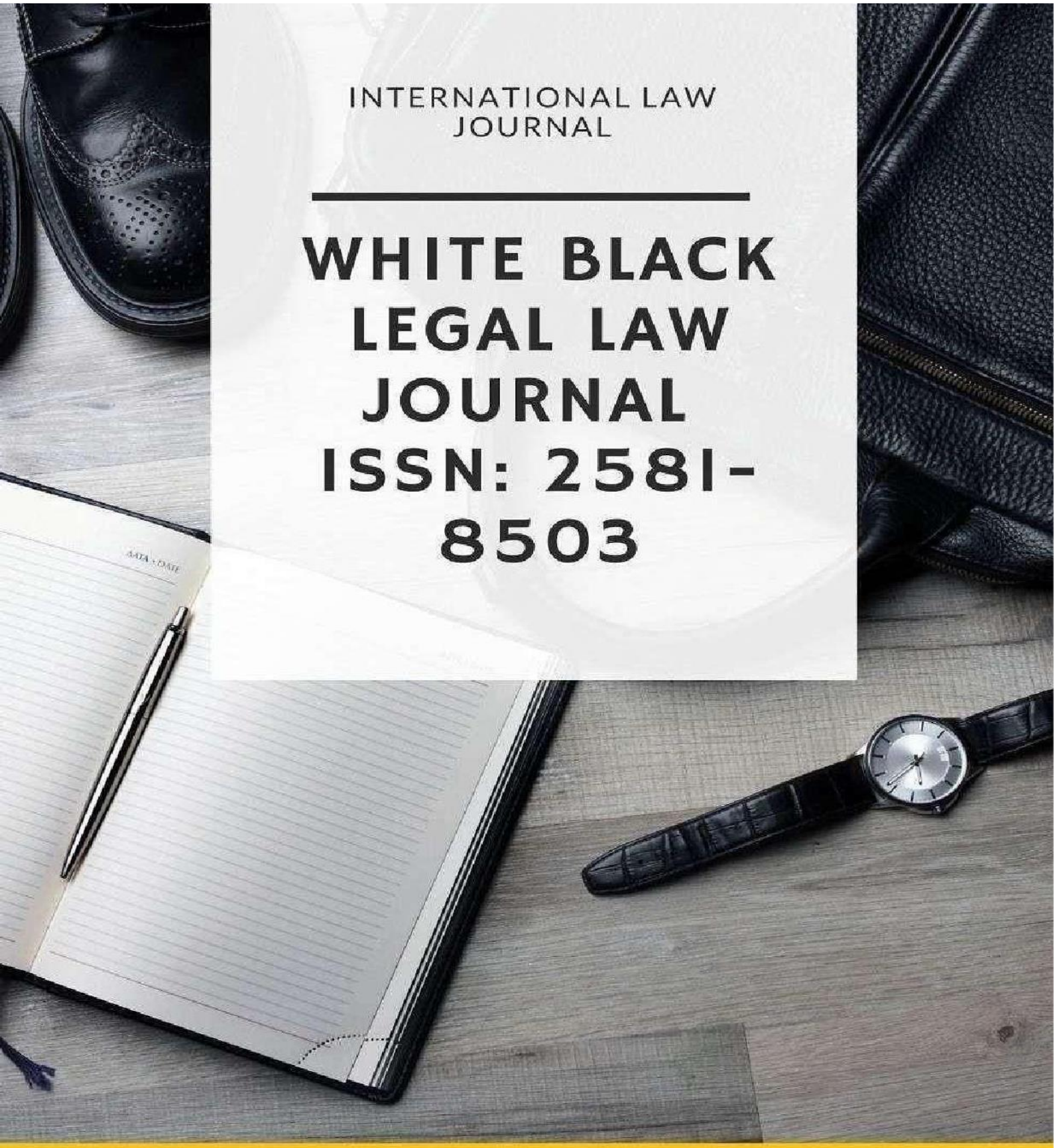


INTERNATIONAL LAW JOURNAL

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.

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.

WHITE BLACK LEGAL

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.

www.whiteblacklegal.co.in
Volume 4 Issue 2 | Oct 2026 ISSN: 2581-8503

FACIAL RECOGNITION, STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL ANALYSIS WITH REFERENCE TO THE EU AI ACT

AUTHORED BY - SAUMYA AGGARWAL
L.L.M(IP)
SECTION-A
Amity Law School, Noida

Abstract

"Delhi Police told the Supreme Court its facial recognition system flagged 2,873 people with criminal records at protest, assured no action without verification. An Express verification shows at least 25 on that list, facing serious charges, were in jail."

As echoed by *The Indian Express* on 4 September 2026, this incident highlights the constitutional challenges posed by facial recognition technology and unchecked state surveillance. The increasing use of real-time biometric surveillance in India raises concerns regarding wrongful identification, mass monitoring, and violations of Article 21 of the Constitution. This paper examines India's legal framework in light of the landmark *K.S. Puttaswamy v. Union of India* judgment and compares it with the European Union's AI Act. It argues that public safety cannot justify unrestricted biometric monitoring and proposes clear statutory rules, judicial authorisation for intrusive surveillance, independent oversight, and effective remedies to protect privacy and individual liberty.

WHITE BLACK LEGAL

Keywords: State Surveillance, Article 21, Right to Privacy, Facial Recognition Technology, Constitutional Proportionality, EU AI Act.

1. Introduction

The use of artificial intelligence in policing has changed the perception of the citizens to the state. The camera, which was initially used for documentation and investigation purposes, is now capable of scanning the faces of the people and comparing them with a digital database, thus finding a possible match. While the use of facial recognition technology (FRT) can help the police identify criminals, locate missing persons, and protect the country from potential threats, such mass surveillance can turn out to be a tool for controlling civilians.

However, not only the ethics of using such a controversial instrument but also its legality is under debate. In India, people are concerned not only whether the police can use FRT but question whether there are enough legal guarantees that such surveillance will not violate the rights of citizens. One should not be considered guilty until proven guilty, and a person going to a rally, shopping, or taking a train should not be viewed with suspicion just because of that.

The controversy around the use of FRT in India was stirred in late September 2026, when The Indian Express published an article [1]based on information obtained from the Delhi Police. As per the report, police showed up at a protest, where the FRT system had identified 2,873 people with criminal records. According to the verification of the newspaper's staff, at least 25 people on that list of 2,873 were in prison at the time of the rally, having serious charges brought against them. Therefore, what does it mean for those 2,873 people who were not in prison at the moment of the rally?[2]

Article 21 of the Constitution of India protects the right to life and personal liberty of citizens, and the Supreme Court has interpreted this article to include a range of rights, including privacy, dignity, and freedom of choice. Thus, state surveillance must be evaluated not only by its ability to stop crime or protect citizens but also by the costs it imposes on the exercise of these rights.

This paper will explore the constitutional limitations of FRT in India and compare them with the European Union AI Act, which includes restrictions and prohibitions on real-time remote biometric identification. It will argue that India needs a thorough legal assessment of whether such surveillance can be used only when it is necessary, proportionate, transparent, and accountable.

2. Research Problem

The critical question is raised regarding the lack of legal protection of citizens from the use of biometric data in India. Modern Indian policing and law enforcement face the challenge of the increasing capabilities of technological equipment to identify and collect personal data of citizens. A facial recognition system, even when positively verified, may generate a false match

[1] 'Police say cameras "caught" murder, rape accused at CJP protest – some were actually in jail', The Indian Express, 4 September 2026.
[2] Justice K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.

that would require additional investigative steps. This issue is complicated by human error, which could lead to a person being placed on a wanted list or face-to-face checks in cases of false matching of biometric data with a known criminal.

This dilemma turns into a paradox if protests or other activities protected by the constitution take place. By collecting and using personal information of participants in rallies, the police can discourage people from holding views different from those of the state. In this way, surveillance can affect not only privacy but also the right to freedom of speech and assembly enshrined in Article 19(1)(a) and (b) of the Indian Constitution.

The research problem is seen in the fact that India's constitutionality and legislative base do not currently provide sufficient guarantees against the continuous use of facial recognition systems by the police in real time. The critical question is whether the European Union's approach to regulating bioptic supervision can serve as a model for solving this problem.

3. Research Objectives

The principal objectives of this research are:

- ✓ To examine the constitutional protection of privacy under Article 21 in relation to state surveillance.
- ✓ To analyse the legal and practical concerns associated with facial recognition technology in policing.
- ✓ To study the safeguards introduced by the European Union's AI Act.
- ✓ To compare the Indian and European approaches to biometric surveillance.
- ✓ To recommend legal reforms that balance public safety with constitutional liberty.

4. Research Methodology

In the modern world, full of high-tech innovations, artificial intelligence is an essential element of any business. In particular, note that companies using such technologies are usually more productive and efficient. On the one hand, the introduction of automated technologies makes it possible to optimize the existing work processes. On the other hand, the actual implementation of artificial intelligence involves changes in the organization and planning of employees' activities. Nevertheless, it should be emphasized that technology by itself is not a universal solution for increasing productivity. Therefore, companies must develop new

progressive methods and techniques and form the necessary skills and abilities in employees to learn to use new high-tech tools correctly.

5. Constitutional Framework in India

5.1 Article 21 and the Right to Privacy[3]

Article 21, as the main shield against unjustified interference with life and liberty, does not mention privacy explicitly but the Supreme Court has held that this right is an intrinsic part of the freedoms that the Constitution enshrines.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, decided by a nine-judge Bench of the Supreme Court, held that the right to privacy is protected as a fundamental right. This right protects autonomy, dignity and the ability to make decisions on one's own.

This ruling is of direct relevance to the use of facial recognition. A single camera scanning an event may seem innocuous, but the ability to identify an individual across multiple locations can reveal that person's associations and behaviour at those public places. What matters to the Constitution is not only the issue of whether an individual is visible at a gathering but how the information linking them to where they have been is collected, collated, stored and used by the state.

The requirements set out in Puttaswamy, including that restrictions must be imposed by law, pursuit of a legitimate state aim and that they must be proportionate, provide a helpful touchstone for assessing whether the use of facial recognition should be considered in a particular context.

5.2 The Proportionality Test

The proportionality principle is meant to ensure that the state does not impose overly restrictive or limiting measures on individuals, unless such a restriction is strictly necessary to achieve a legitimate aim. Preventing crime is a legitimate aim but this does not mean that the surveillance of all attendees of a given public gathering is also permissible.[4]

A proportionality analysis requires consideration of at least four intertwined questions. Does a valid law allow the surveillance that is being proposed? Is the aim legitimate? Is the use of facial recognition to gather evidence appropriate and necessary in order to achieve that objective? And do the aim and necessity considerations outweigh the interference with

[3] Justice K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.
[4] Modern Dental College v State of Madhya Pradesh, (2016) 7 SCC 353.

fundamental rights such as privacy?

It is possible that finding a specific person wanted for questioning in connection with an imminent serious crime would be easier to justify than scanning everybody at a protest against a government policy. What matters in both cases is the difference between targeting and mass surveillance as well as the other measures that the police can take to serve their aim.

A proportionality analysis will also entail looking at less invasive and therefore more privacy-protective alternatives to biometric surveillance. If it is possible for conventional investigative steps to identify or narrow down a list of suspected individuals, indiscriminate use of facial recognition to target them may be harder to justify.

5.3 Other Constitutional Rights

Facial recognition can also implicate other fundamental rights. Article 14 protects against arbitrariness and discrimination, and facial recognition can fail this test if the system has disproportionately high error rates for a particular category of people, or is applied with no legitimate basis to a particular social group.[5]

Articles 19(1)(a) and 19(1)(b) protect free speech and the right to peacefully assemble, and it is common ground that mass surveillance of demonstrators, meetings or protests can cause people to be wary of speaking out, associating or gathering.[6]

The constitutional implications of surveillance should not be viewed solely through the lens of privacy but should consider the combined effect on all fundamental rights.

6. Facial Recognition and the Indian Express Report

The Indian Express report published on 4 September 2026 provides a useful starting point for grappling with the issues raised by the use of facial recognition. It revealed that the Delhi Police's facial recognition system had flagged 2,873 individuals with criminal records in relation to a protest and that verification by the newspaper had uncovered at least 25 individuals with serious charges who were in jail at the time.[7]

The fact that this is the case is a fundamental issue of evidence as it appears that what was actually a computer match has been presented as evidence of presence at a gathering. The report highlights that a computer-generated match cannot be viewed as conclusive proof of who is at

[5] Constitution of India, Article 14.
[6] Constitution of India, Articles 19(1)(a) and 19(1)(b).
[7] The Indian Express, 4 September 2026

a protest or any other location and that such a match should always be treated as an investigative lead that requires verification before any inference can be drawn about presence, identity or alleged criminal activity.

A computer error can cause a number of problems, many of which go beyond the issue of whether or not the police take formal action. Not only can individuals be questioned and placed in a state of suspicion, an error can also waste investigative resources and divert them away from more substantive lines of inquiry.

The very fact of the Indian Express report further illustrates why the reliability and accountability around such systems cannot be judged solely on the claims of the police. The legal framework for the use of facial recognition must contain sufficient safeguards to ensure that there are procedures for verifying a computer match to an individual, determining who can view such a match, how long it should be retained and what remedies are available to someone wrongly identified.

What the report does not show is that every single facial recognition system should be viewed as faulty or that every facial recognition usage by the police is unlawful. The value of this particular episode is far narrower but, when it comes to the rights of individuals to not be wrongly subject to state power, it demonstrates that there should be appropriate safeguards in place when the state is able to utilise such technology.

7. India's Legal and Regulatory Position

India does not currently have a comprehensive statute specifically addressing all aspects of police use of facial recognition and real-time surveillance. As such, when evaluating the legality of such conduct by law enforcement, courts must take into account the relevant constitutional and procedural statutes, the police regulation, any data-protection requirements and the context in which the facial recognition is used.

The Digital Personal Data Protection Act, 2023, provides a broad framework for processing digital personal data and recognises the rights of individuals to their data-protection as well as the state's need to process data for legitimate purposes. However, this statute cannot replace specific rules for live police facial recognition and its commencement is phased in, thus particular sections should be evaluated in the light of the commencement notifications.

A further consideration is that the general legal authority for investigating crime may not answer all the questions concerning mass biometric scanning. The creation of specific rules for facial recognition is essential to distinguish between targeted identification of suspects and the mass scanning of people who have no suspected criminal activity.

Specific rules for police use of facial recognition should delineate permissible purposes, circumstances and restrictions, provide a legal framework for accessing biometric databases, determine retention and deletion periods, and contain mechanisms for independent review and documentation of why less intrusive options would not have been available.[8]

8. The European Union's AI Act: A Comparative Perspective

Regulation (EU) 2024/1689, the European Union Artificial Intelligence Act, offers a more specific regulatory approach to certain high-risk uses of artificial intelligence. Article 5 proscribes prohibited AI practices and restricts real-time remote identification in public spaces for law-enforcement purposes to narrowly defined exceptions and safeguards.[9]

The Act makes it a condition of the use of real-time remote biometric identification in a public space for law enforcement that this satisfy stringent conditions. These include necessity and proportionality, a temporal and geographical limitation, a fundamental-rights impact assessment, and authorisation from a judicial authority or independent administrative authority with binding decision-making powers. One narrowly defined urgency exception permits the use to be initiated before authorisation, but the request must be made without undue delay and not later than 24 hours. If authorisation is declined, the use must cease and the relevant data and outputs must be deleted. The Act explicitly prevents an adverse legal decision being based solely on the system's output.

The European approach is significant due to its acknowledgment that real-time bio-identification is not an ordinary administrative tool. Its capacity to interfere with the rights of many can, at once, affect those who have no connection with a suspected offence. Its requirement for a specific justification and independent authorisation serves to limit the discretion of law-enforcement authorities.

[8] Digital Personal Data Protection Act, 2023, Section 1(2).
[9] Regulation (EU) 2024/1689, Article 5.

The EU AI Act does not impose an absolute ban on every form of facial recognition: its restrictions apply according to the system's type, purpose, setting and applicable exceptions (safeguards). Nor should its provisions be assumed to apply directly to Indian police authorities: It is a comparative guide to show how legislation may define permitted use and establish safeguards rather than leave crucial questions to general policing discretion.

9. Comparative Analysis: India and the European Union

The most important difference between the two approaches lies in the level of specificity of regulation in relation to real-time biometric surveillance. India has a constitutional framework that protects the privacy of its citizens and requires state action to satisfy legal and proportionality standards. But these broad principles do not, themselves, afford a complete operational code for police facial recognition.

The European Union has applied a more detailed legislative model to specified uses of AI that explicitly address real-time remote biometric identification in public spaces and identify circumstances in relation to which its use may be permitted. They also provide for the requirement of prior independent authorisation and restrictions on scope and oversight mechanisms.

Another difference lies in the existence of preventive safeguards. The EU framework requires authorisation to be provided generally before a covered real-time identification operation may begin. This prevents the likelihood of surveillance first and justification later. In India, a comparable system of a specific, uniform statutory authorisation for the police's use of real-time facial recognition is an important area for legal reform.

Finally, a third difference concerns the treatment of automated results: The EU Act explicitly prevents an adverse legal decision from being based solely on the output of real-time remote biometric identification. This is particularly relevant to the Indian Express report, in which the reported matches required verification against information about the individuals' actual whereabouts.

The comparison must nevertheless be approached carefully: India and the EU have different legal systems, policing structures, constitutional arrangements, and public-security needs. India need not follow the European model word for word: It can adopt the principles most relevant

to its constitutional context, which include legal certainty, targeted use, independent authorisation, human verification, transparency, and effective remedies.[10]

10. Major Findings

The study produces five principal findings.

First: The recognition of privacy as a fundamental right under Article 21 places constitutional limits on state surveillance: the police must be able to demonstrate a lawful and proportionate basis for intrusive biometric identification.

Second: Facial recognition errors can have consequences beyond technical inaccuracy: An incorrect match may expose an individual to suspicion or investigation. It may undermine confidence in law-enforcement institutions.

Third: Surveillance at protests presents a heightened constitutional concern due to its potential to discourage exercise of freedom of speech and peaceful assembly: the absence of a formal restriction does not eliminate the possibility that pervasive monitoring may deter participation.

Fourth: General data-protection legislation and constitutional principles are important but do not eliminate the need for specific rules governing police use of facial recognition: clear standards should govern when systems may be used, how results be verified, and when information be deleted.

Fifth: The EU AI Act provides a useful comparative model due to the fact that it places defined limits on real-time biometric identification and requires safeguards for real permitted law-enforcement uses. The central lesson is that the technological capacity must not dictate the legal limits of state power.

11. Recommendations

India should enact a dedicated statutory framework governing the use of facial recognition by law-enforcement authorities. The law should clearly define the purposes to which the technology may be used and prohibit indiscriminate mass biometric surveillance, subject only to narrowly defined, legally justified exceptions.

[10] Justice K.S. Puttaswamy v Union of India, (2017) 10 SCC 1; Regulation (EU) 2024/1689, Article 5.

Second, intrusive real-time biometric identification should ordinarily require prior judicial authorisation. An application should identify the individual or specific threat being investigated, the purpose of the operation, its duration and geographical scope and the reasons why less intrusive alternatives would not be sufficient. Any emergency exception should be narrowly defined and subject to prompt independent review.

Third, facial recognition results should never be treated as conclusive evidence of identity, presence, or guilt: authorities should verify matches using independent evidence before taking adverse action. The system's confidence score, limitations and relevant contextual information should be considered rather than relying solely on a match.

Fourth, India should establish independent technical and legal oversight: an appropriate oversight body should examine the accuracy and performance of deployed systems, assess possible discriminatory effects, review complaints, and audit compliance with retention and access restrictions.

Fifth: clear rules should govern biometric databases: data should be collected only for specified lawful purposes, access should be restricted and logged, and information should be deleted when retention is no longer justified. Individuals who are wrongly identified should have access to an effective complaint mechanism and appropriate remedies.

Finally, surveillance practices should be subject to periodic public reporting, subject to legitimate operational confidentiality: this should disclose the number and general purpose of deployments, authorisations sought and granted, complaints received and verified instances of error. These measures will promote accountability without unnecessarily compromising genuine criminal investigations.

12. Conclusion

Facial recognition technology presents both an opportunity and a constitutional challenge for modern policing. It may enable authorities to identify suspects and respond to serious threats, but its benefits do not negate the need for legal limits. Without adequate safeguards, an investigative tool can become a mechanism of intrusive and potentially arbitrary surveillance.

The Indian Express report of 4 September 2026 illustrates why verification, accountability and procedural safeguards are essential. The reported discrepancy between facial recognition results and the actual whereabouts of certain individuals raises concerns about the consequences of relying on automated matches without sufficient independent confirmation.

The Supreme Court's decision in K.S. Puttaswamy v. Union of India provides the constitutional foundation upon which to assess these practices. Privacy is not merely a matter of secrecy; it is connected to dignity, autonomy and the freedom to participate in public life without unjustified interference. The European Union's AI Act provides a comparative example of how legislation may impose specific restrictions and permit narrowly defined use for legitimate law-enforcement objectives. India should, therefore, develop a clear, enforceable and rights-based framework for facial recognition. This should be based upon statutory authority, necessity and proportionality, prior independent authorisation, reliable verification, technical audits, and remedies for misuse. The ultimate objective should not be to choose between public safety and privacy, but to ensure it may be pursued in a manner that is consistent with constitutional liberty and the rule of law.

REFERENCES AND BIBLIOGRAPHY

A. Cases

1. *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
2. *Modern Dental College and Research Centre v State of Madhya Pradesh* (2016) 7 SCC 353.
3. *Maneka Gandhi v Union of India* (1978) 1 SCC 248.

B. Legislation and Legal Instruments

1. Constitution of India, 1950, arts 14, 19 and 21.
2. Digital Personal Data Protection Act 2023 (Act 22 of 2023).
3. Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

C. Newspaper and Online Sources

1. Manral MS, 'Police say cameras "caught" murder, rape accused at CJP protest – some were actually in jail' *The Indian Express* (4 September 2026).
2. National Institute of Standards and Technology, 'Face Recognition Technology Evaluation (FRTE)' (NIST).

D. Official and Institutional Sources

1. Supreme Court of India, *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, judgment.
2. India Code, Digital Personal Data Protection Act 2023.
3. Ministry of Electronics and Information Technology, Notification GSR 843(E), 13 November 2025.
4. EUR-Lex, Regulation (EU) 2024/1689, official text.
5. National Institute of Standards and Technology, Face Recognition Technology Evaluation programme.

WHITE BLACK
LEGAL