
BALANCING SURVEILLANCE AND PRIVACY: A COMPARATIVE STUDY OF FACIAL RECOGNITION TECHNOLOGY REGULATION WITH EUROPEAN UNION

Shreyash Singhal, LLM (Criminal Law), Amity Institute of Advanced Legal Studies, Noida

ABSTRACT

Facial Recognition Technology (FRT) is now becoming an ever more important tool for state surveillance, with the possibility of providing benefits in the prevention of crime while at the same time giving rise to serious worries about privacy, equality, freedom of expression and the right to peaceful assembly. These concerns are especially pressing when the technology is used during public protests. The Delhi Police's use of AI-assisted facial recognition at Jantar Mantar serves as a current example upon which to examine the constitutional and legal boundaries of state biometric surveillance.

This paper critically examines whether India's existing constitutional and statutory Agency mapwork adequately regulates State use of FRT, particularly in protest settings. It analyses Articles 14, 19 and 21 of the Constitution, the Digital Personal Data Protection Act, 2023, the Criminal Procedure (Identification) Act, 2022 and relevant police powers. The study comparatively examines the European Union's rights-based framework under the EU Charter of Fundamental Rights, GDPR, Law Enforcement Directive and EU Artificial Intelligence Act, with particular attention to biometric identification and real-time remote biometric identification.

Employing a qualitative, doctrinal, comparative and analytical methodology, the study identifies significant gaps in India's framework concerning legal authority, necessity, proportionality, accuracy, transparency, accountability and effective remedies. The analysis finds that legitimate public-security objectives alone cannot justify broad or indiscriminate biometric surveillance. It argues for a clearer and more proportionate regulatory framework, informed by relevant EU safeguards while remaining grounded in India's constitutional commitment to privacy, liberty, equality and democratic participation.

Keywords: Facial Recognition Technology (FRT), Right to Privacy, Biometric Identification, Data Protection, GDPR, Algorithmic Bias & Public Surveillance.

Introduction:

The use of Facial Recognition Technology (FRT) by modern law enforcement has fundamentally changed the nature of state surveillance and has therefore given rise to important discussions at the point where public security, criminal law, and constitutional rights meet. In recent years, democratic countries have become more and more likely to employ biometric systems in order to keep the public in order, control crowds, and identify people with a criminal record. Yet this move towards algorithmic policing brings with it certain risks to basic freedoms, particularly the right to privacy, the freedom of expression, and the right to equality. In India the application of FRT by state authorities has expanded quickly without there being a specific and thorough legal framework, the system instead relying on general police powers.

On 20 June 2026, a student-led agitation over successive examination-paper leaks gathered at Jantar Mantar in New Delhi. Within weeks, the protest had drawn not only thousands of demonstrators but also Delhi Police surveillance vehicle the "Ikshana" van, whose eight cameras fed live footage through facial recognition software that drew boxes around individual faces and checked them against police databases. According to which 2,873 people were identified through matches with existing records¹. An investigation subsequently found that at least twenty-five of those "matches" were, at the material time, in judicial custody elsewhere physically incapable of having been at Jantar Mantar at all. The Delhi Police's own threshold for a "positive" match, disclosed in a 2022 RTI response, was an 80 per cent similarity score a figure that says nothing about the system's real-world accuracy and everything about how readily error can be mistaken for identification.² The Jantar Mantar episode did not target named suspects wanted for specific offences, it processed the biometric data of tens of thousands of persons protesters, bystanders, journalists, the injured seeking medical aid as an incident of their presence at that place. These systemic flaws underscore the risks of mass surveillance and highlight an urgent need to scrutinize the regulatory limits, accuracy, and legal safeguards surrounding state-sponsored biometric tracking in India.

Conversely, the European Union has adopted a stringent, rights-based approach to regulating biometric and artificial intelligence technologies. Through frameworks like the General Data

¹ Ananthakrishnan G., "How Facial Recognition Was Used for CJP Protest: Delhi Police to Supreme Court", *The Indian Express*, August 18, 2026.

² Mahender Singh Manral, "Police Say Cameras 'Caught' Murder, Rape Accused at CJP Protest – Some Were Actually in Jail", *The Indian Express*, September 4, 2026.

Protection Regulation (GDPR),³ the Law Enforcement Directive, and the pioneering EU Artificial Intelligence Act⁴, the EU has established strict operational baselines governed by principles of necessity, proportionality, and transparency. A comparative analysis between

India's relatively unchecked deployment of FRT and the EU's comprehensive legislative model offers critical insights into how democratic societies can harness technological advancements without eroding fundamental human rights.

Statement of Problem:

The greater the use by state authorities of facial recognition technology, the more it raises a basic legal question as to how far public security can justify interference with an individual's liberty and privacy. In India, the absence of a comprehensive FRT-specific legal framework creates uncertainty regarding legality, proportionality and accountability, particularly during protests. The problem is to determine whether existing constitutional and statutory safeguards adequately reconcile State surveillance with individual rights and democratic freedoms.

Research question:

1. How does FRT affect the rights under Articles 14, 19 and 21?
2. Does Indian law adequately regulate the State's use of FRT?
3. How does the EU regulate FRT under the GDPR and EU AI Act?
4. What privacy and constitutional concerns arise from FRT use at Jantar Mantar?
5. What safeguards can India adopt from the EU framework?

Research Objective:

1. To examine the constitutional implications of State use of FRT under Articles 14, 19 and 21 of the Constitution of India.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act)" Official Journal of the European Union, L, 2024/1689, July 12, 2024

2. To assess the adequacy of India's existing legal framework in regulating State deployment of FRT.
3. To analyse the legal and constitutional concerns arising from the reported use of FRT during the Jantar Mantar protests.
4. To comparatively examine the European Union's regulatory approach to FRT under the GDPR, Law Enforcement Directive and EU Artificial Intelligence Act.
5. To identify appropriate safeguards and regulatory measures that India may adopt from the EU framework to ensure that the use of FRT remains lawful, necessary and proportionate.

Research Methodology:

This study uses comparative and qualitative methods. The doctrinal method looks at rules, laws and court decisions that control how the State uses FRT in India and the European Union. The comparative approach evaluates both frameworks in relation to privacy, biometric data, proportionality, necessity and procedural safeguards. The qualitative analysis examines the constitutional implications of FRT during the Jantar Mantar protests, drawing on legislation, judicial decisions, government materials, regulatory reports and scholarly literature.

Research Hypothesis:

India's existing framework is insufficient to regulate State use of FRT in a manner consistent with fundamental rights, and the EU regulatory approach can provide useful safeguards for developing a more lawful, necessary and proportionate framework in India.

Literature Review:

The existing literature on Facial Recognition Technology (FRT) has developed along three closely related lines: constitutional and human-rights concerns, regulation of biometric data and law-enforcement surveillance, and comparative approaches to emerging AI regulation. A review of these strands shows that the central concerns surrounding FRT are well established, but their application to the contemporary Indian context of facial surveillance at public protests, particularly under India's post-DPDP Act framework and in light of the EU AI Act, remains

comparatively underdeveloped.

A foundational contribution is Ameen Jauhar's *Facing up to the Risks of Automated Facial Recognition Technologies in Indian Law Enforcement*. Jauhar examines automated FRT through Article 21 and due-process principles and argues that its increasing use by law enforcement agencies requires stronger statutory controls. His analysis is significant because it treats the absence of clear legal authority as a constitutional problem rather than merely a regulatory deficiency. It also considers European and United States approaches as possible sources for Indian regulation. However, the article predates both the Digital Personal Data Protection Act⁵ and the EU Artificial Intelligence Act, and therefore cannot address their contemporary legal significance.⁶

Smriti Parsheera's *Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?*⁷ moves the analysis from the existence of surveillance power to the constitutional conditions governing its exercise. By examining privacy, transparency, accuracy, effectiveness and algorithmic bias in relation to India's proposed National Automated Facial Recognition System, Parsheera connects technological design with the proportionality framework developed in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)⁸. Her analysis indicates that a legitimate law-enforcement objective is not sufficient by itself; the State must also justify the necessity, design and consequences of the technological measure.

The comparative literature develops this argument across jurisdictions. Bag and Pradhan's study, *Who Monitors the Monitors? Analysing the Legal Intricacies of Digital Forensic-based Facial Recognition Technology in Law Enforcement*⁹, examines “India and the EU through privacy, due process, proportionality and fundamental rights. It is particularly significant because it demonstrates that the India-EU comparison is already present in scholarship. The present study therefore does not claim novelty from jurisdictional comparison alone. Its contribution lies in applying that comparison to a more specific constitutional problem: State use of FRT in public protests and public spaces, where biometric surveillance may

⁵ Digital Personal Data Protection Act, 2023 (22 of 2023)

⁶ Ameen Jauhar, “Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement” 16(1) *Indian Journal of Law and Technology* 1 (2020).

⁷ Smriti Parsheera, “Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?” vol. 28 *A conversation on AI activism* p. 28, (2021).

⁸ (2017) 10 SCC 1.

⁹ A. Bag and A. Pradhan, “Who Monitors the Monitors? Analysing the Legal Intricacies of Digital Forensicbased Facial Recognition Technology in Law Enforcement” 13 *Asian J. Legal Educ.* 79 (2026).

simultaneously affect privacy, equality, expression and peaceful assembly.”

The technological literature strengthens this doctrinal development. Srikrish's demographic effects research identifies differences in error performance across facial-recognition algorithms and distinguishes between one-to-one verification and one-to-many identification. Its findings concerning false positives are particularly relevant to policing because an erroneous one-to-many match may subject an otherwise innocent person to further scrutiny¹⁰. The European Union Agency for Fundamental Rights similarly identifies erroneous identification and differential performance as fundamental-rights concerns and notes that individuals may be unaware that their biometric information is being processed.¹¹

These findings allow the literature to be synthesised doctrinally: accuracy is connected to legality through the principle of non-arbitrariness, to proportionality through the severity of potential harm, and to due process through the need for meaningful verification and challenge. An inaccurate facial match is therefore not merely a technical failure. When relied upon by the State, it can produce unequal treatment, interfere with liberty and undermine procedural fairness. This is particularly important in protest settings, where one-to-many identification can potentially subject an entire group to scrutiny without individualised suspicion.

More recent international scholarship has moved beyond privacy alone and examined FRT as a rule-of-law and fundamental-rights problem. Qandeel's 2024 study, *“Facial Recognition Technology: Regulations, Rights and the Rule of Law”*, examines the need for legal intervention where biometric AI is used for surveillance and policing. The article frames FRT as an issue involving basic freedoms, liberties and rule-of-law values, rather than merely a matter of data processing.¹²

Similarly, a 2025 Computer Law & Security Review article, *“Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind”*, argues that FRT should be treated differently from conventional forensic analysis because it creates a new biometric layer of data through automated comparison. The authors emphasise that the legal framework should

¹⁰ Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects” *NISTIR 8280* (National Institute of Standards and Technology, U.S. Department of Commerce), (2019).

¹¹ European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in Law Enforcement* (Publications Office of the European Union, 2019).

¹² M. Qandeel, “Facial recognition technology: regulations, rights and the rule of law” vol. 7 *Front. Big Data* 1354659 (2024).

account for the different stages of FRT processing and their individual impacts on fundamental rights. Importantly, the article argues that the AI Act does not itself provide the complete legal basis required for law-enforcement deployment of FRT and that broader legal authorisation remains necessary.¹³

This literature is particularly useful for the present study because it prevents an overly simple argument that the EU AI Act by itself regulates facial recognition. Instead, the literature suggests that FRT must be understood within an interconnected framework of fundamental rights, data protection, law-enforcement law and AI regulation.

EU institutional sources reinforce this layered framework. The European Data Protection Board's Guidelines 05/2022¹⁴ require law-enforcement facial recognition to comply with the Law Enforcement Directive and the principles of necessity and proportionality under the Charter. The EU AI Act introduces rules that specifically limit the use of time remote biometric identification in public places. This is a deal because it shows a shift in how the European Union is thinking about biometric surveillance. Of just controlling how biometric data is handled after it's collected the law now sets strict conditions on when such surveillance can even begin. This means the focus is on preventing surveillance before it happens not just managing it afterward. It signals a stance, on protecting privacy and civil liberties in public spaces. Indian policy literature predating the DPDP Act¹⁵ also provides an important foundation. The Justice B.N. Srikrishna Committee's 2018¹⁶ report identified the need to balance individual interests in personal data with legitimate interests in data processing and proposed a rights-oriented data-protection framework. The report remains significant as part of the development of India's data-protection architecture, although it was produced before the present statutory regime.

The Criminal Procedure (Identification) Act¹⁷ is also relevant because Parliament expressly expanded the concept of "measurements" to include photographs, iris and retina scans, biological samples and their analysis, and empowered the National Crime Records Bureau to

¹³ Monika Simmler and Giulia Canova, "Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind" vol. 56 *Computer Law & Security Review* (2025).

¹⁴ European Data Protection Board, Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement (Final Version, 17 May 2023).

¹⁵ *Supra* note 5.

¹⁶ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (July, 2018).

¹⁷ The Criminal Procedure (Identification) Act, No. 11 of 2022.

collect, store, preserve, share and disseminate such records. The Act provides for long-term retention of records, subject to specified exceptions.

At the same time, the DPDP Act, 2023¹⁸ establishes India's general legal framework for processing digital personal data and recognises both individual data-protection interests and lawful data processing. The literature therefore presents an evolving Indian framework rather than a complete legal vacuum.

Research Gap in the existing literature

This study is different from India-EU comparisons that looked at FRT mainly through privacy, data protection, fairness and basic rights. This research specifically looks at how the State uses FRT during protests. The main value of this study is linking surveillance with the rights, to equality, freedom of expression and peaceful assembly instead of just focusing on privacy as the main issue. It also updates the comparison in light of India's Digital Personal Data Protection Act¹⁹, 2023 and the EU Artificial Intelligence Act, while integrating practical concerns of wrongful identification, accuracy, accountability and remedies into constitutional analysis. The study uses the Jantar Mantar protests as an example to look at whether India's current safeguards are enough to control the use of facial recognition technology during protests. It also explores safeguards, from the European Union that could be adapted to make India's system stronger.

India's Legal and Judicial Analysis of Facial Recognition Technology:

I. Constitutional framework governing State use of FRT:

India lacks a dedicated statute comprehensively regulating State use of Facial Recognition Technology (FRT). Its legality must therefore be assessed through Articles 14, 19 and 21 of Constitution of India²⁰, existing criminal and data laws, police powers and judicial safeguards. Article 14²¹ protects against arbitrary State action; Article 19(1)(a)²² and Article 19(1)(b)²³

¹⁸ *Supra* note 5.

¹⁹ *Supra* note 5.

²⁰ The Constitution of India, arts. 14, 19 & 21.

²¹ The Constitution of India, art. 14.

²² The Constitution of India, art. 19(1)(a).

²³ The Constitution of India, art. 19(1)(b).

safeguard expression and peaceful assembly; and Article 21²⁴ protects life and personal liberty.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*, the Supreme Court recognised privacy as encompassing dignity, autonomy and informational control. It held that State interference with privacy must satisfy legality, a legitimate State aim and proportionality. This framework is central to FRT because facial images, when algorithmically processed, can transform ordinary surveillance into searchable biometric identification linked to State databases.²⁵

Accordingly, the key constitutional question during protests is not merely whether the State may record public activity, but whether it has sufficient legal authority to identify individuals biometrically, and whether such identification is necessary and proportionate to a legitimate objective. In *Mazdoor Kisan Shakti Sangathan v. Union of India (2018)*²⁶, the Supreme Court recognised the need to balance public-order concerns with the rights to speech and peaceful assembly. Thus, regulation of protest surveillance must remain constitutionally justified and cannot become an unrestricted power of the State.

II. Article 14 and the problem of arbitrary and inaccurate identification:

Article 14²⁷ is interconnected with FRT in two ways. First, the State cannot exercise surveillance powers arbitrarily. Secondly, the possibility of inaccurate or discriminatory technological identification raises concerns of unequal treatment. An FRT system does not establish criminal involvement merely because it generates a match. A facial-recognition output is ordinarily a probabilistic technological assessment requiring human verification and contextual investigation. This distinction becomes particularly important during a protest, where thousands of individuals may be present and where a system may compare numerous faces against a criminal database.

III. Right to privacy and State surveillance:

The constitutional concern is greater when the system uses a relatively low similarity threshold or when the database contains historical records of individuals who have not committed any

²⁴ The Constitution of India, art. 21.

²⁵ *Supra* note 8.

²⁶ AIR 2018 SC 3476.

²⁷ *Supra* note 21

offence at the protest. In such circumstances, a person can move from being an ordinary protest participant to a "person of interest" solely because an algorithm generated a possible match. In *Manohar Lal Sharma v. Union of India*, (2021)²⁸, commonly known as the Pegasus case, the Supreme Court recognised the direct constitutional significance of surveillance and rejected the proposition that invocation of national security automatically places executive surveillance beyond meaningful judicial examination. The Court observed that privacy is directly implicated when an individual is subjected to surveillance and emphasised the need for constitutional justification of State action.

Although Pegasus involved spyware rather than facial recognition, the underlying principle is relevant. Modern surveillance technologies cannot be insulated from constitutional review merely because they are deployed for law-enforcement or security purposes. The State must identify the legal basis, purpose and safeguards surrounding the surveillance.

IV. Criminal Procedure (Identification) Act, 2022:

The Criminal Procedure (Identification) Act²⁹ provides statutory authority for collecting and processing specified "measurements", including photographs and other biometric information, and empowers the National Crime Records Bureau to store, process and share such records with law-enforcement agencies. It also contains provisions governing their retention and destruction.

However, the Act cannot be treated as a comprehensive statutory basis for all forms of police FRT. Its scheme primarily concerns persons falling within prescribed categories in connection with arrest, conviction, investigation or judicial proceedings. It does not expressly authorise the mass or real-time biometric scanning of persons attending a peaceful public gathering. A crucial distinction therefore exists between collecting a person's biometric information under statutory authority and conducting automated one-to-many facial identification across an entire crowd. This distinction is particularly important during protests. Authority to obtain biometric material from a lawfully arrested person does not necessarily confer authority to identify every protest participant by comparing live facial images with criminal databases. Such broader surveillance must therefore be independently justified by clear legal authority and

²⁸ (2021) 6 SCC 791.

²⁹ Supra note 17.

constitutional requirements of necessity and proportionality.

V. Digital Personal Data Protection Act, 2023:

The DPDP Act³⁰ is relevant because facial images and facial templates may constitute personal data where they relate to an identifiable individual. However, the timing of the legislation is critical to the present research. The Central Government notified the DPDP Rules, 2025 in November 2025 and issued an enforcement timeline for the Act. Under that notification, the core provisions of Sections 3 to 5, Sections 6 to 17 and several related provisions were scheduled to come into force 18 months after publication of the notification. Consequently, those substantive provisions were not yet operational during the July 2026 Jantar Mantar protests. This is important because the present paper should not describe the DPDP Act³¹ as though its full substantive rights and obligations were already governing the Jantar Mantar deployment.

Even when the substantive provisions become operational, the Act is not a specialised FRT statute. Section 17 contains broad exemptions from specified obligations in situations involving, among other things, enforcement of legal rights and certain State functions. Therefore, a general data-protection statute cannot by itself answer all the constitutional questions associated with police FRT. Issues such as the legal basis for live biometric identification, permissible watchlists, accuracy thresholds, human review, retention periods, audit requirements, disclosure of vendor involvement and remedies for wrongful identification require more specific regulation.

VI. *S.Q. Masood v. State of Telangana:*

In *S.Q. Masood v. State of Telangana & Anr.*, *W.P. (PIL) No. 191 of 2021*, the Telangana High Court considered a challenge to the State's deployment of Facial Recognition Technology, raising concerns regarding privacy, equality, the rule of law and the absence of adequate safeguards. The proceeding is significant as an early Indian constitutional challenge directed specifically at governmental use of FRT.

However, its precedential value should be stated cautiously. The case has not resulted in a

³⁰ *Supra* note 5.

³¹ *Supra* note 5.

Supreme Court judgment establishing general legal standard governing police use of FRT. It is therefore more appropriately understood as an FRT-specific constitutional challenge, rather than settled authority on the legality or illegality of the technology. Its significance for the present study lies in demonstrating that concerns over the legal basis and safeguards governing State FRT predate the Jantar Mantar controversy. The latter therefore represents a continuing and increasingly important constitutional question rather than an entirely new issue.

VII. Biometric evidence and the importance of statutory authority:

In *Ritesh Sinha v. State of Uttar Pradesh*, (2019)³², the Supreme Court considered whether a Magistrate could direct an accused to provide a voice sample despite the absence of an express statutory provision. The majority permitted the direction in the circumstances of the case, relying on judicial interpretation and the Court's powers under Article 142³³. However, Article 142 should not be understood as creating a general or permanent statutory authority for the State to collect biometric information. Its role was exceptional and confined to enabling the Court to secure the ends of justice in the case before it.

The decision is therefore doctrinally relevant rather than direct authority for FRT. It underscores the importance of lawful authority when the State obtains identifying biometric information. Unlike the identified accused in *Ritesh Sinha* case, FRT at a protest may involve the biometric scanning of large numbers of unidentified persons. Such surveillance raises a substantially broader constitutional question and cannot be justified merely by invoking the Court's exceptional powers under Article 142.³⁴

Comparative Analysis of State Use of Facial Recognition Technology in India and the European Union:

The regulation of State use of Facial Recognition Technology (FRT) reveals a significant difference between India and the European Union (EU). Both recognise privacy, equality and democratic freedoms as fundamental values, but their regulatory approaches differ in specificity. India relies primarily on constitutional principles, particularly Articles 14, 19 and 21, the Criminal Procedure (Identification) Act³⁵ and the emerging data-protection framework.

³² (2019) 8 SCC 1.

³³ The Constitution of India, art. 142

³⁴ *Supra* note 33.

³⁵ *Supra* note 17.

The EU has developed a more detailed structure through the EU Charter of Fundamental Rights, the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the EU Artificial Intelligence Act (AI Act). This difference is particularly significant where FRT is deployed during protests, because biometric surveillance may affect privacy, freedom of expression and peaceful assembly simultaneously.

In India, the principal constitutional foundation is *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)³⁶, in which the Supreme Court recognised privacy as a fundamental right under Article 21. State interference with privacy must satisfy legality, pursue a legitimate objective and meet the requirement of proportionality. Articles 14, 19(1)(a) and 19(1)(b) further protect against arbitrary State action and safeguard speech and peaceful assembly. The EU provides comparable protection through Articles 7, 8, 11, 12 and 21 of the Charter, which protect private life, personal data, expression, assembly and non-discrimination. The important distinction is that data protection is expressly recognised as a fundamental right in EU law, whereas informational privacy in India has developed primarily through constitutional interpretation.

The Criminal Procedure (Identification) Act³⁷ permits collection and processing of specified "measurements", including photographs and biometric information, and gives the National Crime Records Bureau powers over such records. However, it does not establish a comprehensive framework governing live or mass facial recognition. Thus, it remains uncertain whether existing statutory powers can justify automated identification of an entire protest crowd. This is significant because the legal basis for collecting biometric information from persons involved in criminal proceedings is not necessarily equivalent to authority for indiscriminate identification of protesters, journalists or bystanders.

The EU provides a more specific framework for law-enforcement processing. Article 10 of the Law Enforcement Directive³⁸, gives enhanced protection to biometric data used for uniquely identifying an individual and requires such processing to be strictly necessary and subject to appropriate safeguards. The CJEU reinforced this principle in *Comdribus case*³⁹, decided in 2026, concerning biometric identification connected with a demonstration. The Court emphasised that biometric collection cannot be systematic and must be justified by strict

³⁶ *Supra* note 8.

³⁷ *Supra* note 17.

³⁸ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, O.J. L 119/89 (2016).

³⁹ Case C-371/24, *Comdribus*, EU:C:2026:219 (CJEU, 19 March 2026).

necessity. The decision is particularly relevant because it directly connects biometric identification with the exercise of the right to demonstrate.

The biggest difference happens when it comes to time remote biometric identification in places that are open to the public. India does not have a full law that stops police from using live facial recognition technology in public areas. There is also no system that says when they can use it. So whether it is. Not has to be checked using the idea of fairness under the constitution and the rules that already exist. On the hand Article 5 of the EU AI Act says that real-time remote biometric identification in public places is generally not allowed for police work. This is true unless there are specific reasons. These reasons include finding a person who is in danger dealing with an immediate threat to someone's life or safety or looking for someone who is suspected of a serious crime. When these situations happen the use of the technology has to be focused on a specific person last, for a short time cover a small area and only involve a few people.

The EU system also offers ways to prevent problems. Using time facial recognition technology in certain cases needs a special check, for how it affects basic rights. As a general rule it must get permission first from a court or an independent group that makes decisions. Emergency use is subject to subsequent authorisation requirements, and where authorisation is refused, the use must cease and relevant data must be deleted. India currently has no equivalent FRT-specific requirement for prior judicial or independent administrative authorisation. The EU framework therefore seeks to prevent disproportionate surveillance before it occurs, whereas the Indian framework depends more heavily on constitutional review of State action.

The two systems also differ in how they operationalise necessity and proportionality. Under Indian constitutional law, surveillance must pursue a legitimate objective and must not impose a disproportionate restriction on fundamental rights. Targeted use of FRT to identify a specific wanted person may therefore be easier to justify than scanning the faces of every protester. EU law makes this distinction more explicit by requiring strict necessity and targeted use. This creates a higher threshold where authorities seek to conduct broad biometric surveillance in public spaces.

A further distinction concerns accuracy, automated decision-making and accountability. Indian law does not yet provide a comprehensive FRT-specific regime establishing accuracy standards, mandatory human verification, algorithmic auditing or procedures for challenging

false matches. This is particularly problematic because an erroneous facial match may lead to investigation, detention or other interference with liberty. The EU's LED and AI Act provide stronger safeguards against adverse consequences based solely on automated biometric outputs and place greater emphasis on human oversight and accountability.

These differences are particularly important in the context of protest surveillance. In India, police may invoke public order and crime prevention, but such objectives remain subject to Articles 14, 19 and 21 and the requirements of legality and proportionality. The absence of a dedicated FRT statute creates uncertainty over large-scale identification of protesters. In the EU, real-time remote biometric identification in public spaces begins from a position of general prohibition and is permitted only under narrowly defined conditions. This reflects a stronger regulatory preference for targeted surveillance over indiscriminate biometric monitoring.

Overall, both India and the EU recognise that FRT may interfere with fundamental rights, but the EU has translated these principles into more detailed statutory safeguards. India's constitutional jurisprudence, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)⁴⁰ judgement, provides a strong foundation for legality and proportionality, while existing legislation offers only partial regulation of biometric surveillance. The principal comparative lesson is therefore not that FRT should be prohibited altogether, but that India requires a dedicated legal framework establishing clear limits on targeted use, prior authorisation, necessity, fundamental-rights assessment, retention, human oversight, accuracy and remedies. Such regulation would allow legitimate law-enforcement uses of FRT while preventing its transformation into disproportionate surveillance of peaceful assemblies.

Findings:

The study finds that Facial Recognition Technology (FRT) can assist legitimate law enforcement objectives, but its use by the State creates serious concerns when it shifts from targeted identification to broader surveillance. These concerns become particularly significant during protests because FRT may affect privacy, equality, freedom of expression and peaceful assembly at the same time.

India already has a strong constitutional basis for regulating FRT. Articles 14, 19 and 21 of the

⁴⁰ Supra note 8.

Indian Constitution⁴¹, particularly after *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)⁴², require State interference with fundamental rights to satisfy legality, legitimate purpose and proportionality. However, the study finds that these principles have not yet been translated into a sufficiently detailed statutory framework for police use of FRT.

The Criminal Procedure (Identification) Act⁴³ regulates the collection of specified measurements, including photographs and biometric information, but it does not clearly establish when police may conduct mass or real-time facial recognition of persons attending a protest. Similarly, the DPDP Act⁴⁴ provides a broader data-protection framework but does not specifically regulate law-enforcement FRT. This creates uncertainty regarding the legal basis, scope, retention and oversight of biometric surveillance.

The research further finds that accuracy is a legal as well as a technological concern. An incorrect facial match may result in investigation, detention or other adverse consequences.

Consequently, an FRT match should be treated as an investigative lead requiring human verification rather than conclusive proof of identity.

The comparison with the European Union shows a more detailed regulatory structure. The EU Charter⁴⁵, Law Enforcement Directive and AI Act impose specific requirements concerning necessity, proportionality, authorisation and safeguards. The recent *Comdribus* decision of the CJEU⁴⁶ further demonstrates that biometric identification connected with demonstrations must be strictly necessary. It therefore supports the hypothesis that India's present framework is insufficiently specific and that the EU provides useful safeguards for strengthening Indian regulation.

Suggestions:

The comparative analysis suggests that India can draw several safeguards from the EU framework while adapting them to its constitutional and institutional context.

⁴¹ The Constitution of India arts. 14, 19, & 21.

⁴² *Supra* note 8.

⁴³ *Supra* note 17.

⁴⁴ *Supra* note 5.

⁴⁵ Charter of Fundamental Rights of the European Union, 2012 O.J. C 326/391.

⁴⁶ *Supra* note 39.

- I. India should enact a dedicated statutory framework for State use of FRT. As in the EU, the law should clearly distinguish between ordinary data processing, targeted facial identification and mass or real-time biometric surveillance. It should specify the authorities permitted to use FRT, the purposes for which it may be deployed and the offences that can justify its use.
- II. India should adopt the EU's strict necessity and proportionality standards. FRT should be used only where genuinely necessary and where less intrusive methods cannot achieve the same purpose. During protests, mere presence at an assembly should not justify biometric identification.
- III. For intrusive uses, particularly real-time FRT, India should require prior judicial or independent authorisation, subject to narrowly defined emergencies. A mandatory Fundamental Rights or Privacy Impact Assessment should also examine the effects on Articles 14, 19 and 21, potential discrimination, alternatives and the scale of surveillance.
- IV. India should introduce stronger safeguards for accuracy and human oversight. Systems should undergo independent testing for accuracy and demographic bias, and every facial recognition match should be independently verified by a human before any adverse action. An automated match alone should not justify arrest, detention or investigation.
- V. India should also adopt clear purpose limitation, retention and deletion rules. Biometric data collected during protests should not be retained indefinitely, particularly where individuals are not suspected of an offence. Continued retention should require specific justification and periodic review.
- VI. India should strengthen transparency, independent auditing and remedies. Authorities should document the legal basis, purpose, duration, number of matches and false positives arising from each deployment. Individuals should have an effective mechanism to challenge inaccurate identification and obtain correction or deletion of wrongly held data.

Conclusion:

The present position should be understood as an emerging rather than settled FRT jurisprudence. Facial Recognition Technology offers significant possibilities for modern law enforcement, but its use also creates a serious challenge for constitutional democracy. The

central issue is not whether the State may use technology for public security, but whether such use remains lawful, necessary and proportionate when it affects fundamental rights. The absence of a comprehensive FRT-specific legal framework leaves important questions concerning legal authority, accuracy, retention, accountability and remedies insufficiently addressed.

The European Union provides a useful comparative model by translating broad rights-based principles into more specific safeguards concerning necessity, targeted use, authorisation, human oversight and accountability. India need not reproduce the EU framework in its entirety, but its experience demonstrates the importance of establishing clear limits before intrusive biometric technologies become embedded in routine policing.

Ultimately, the legitimacy of FRT should depend not on what the technology is capable of doing, but on how, why and under what legal safeguards the State chooses to use it. Public safety and technological advancement cannot justify unlimited biometric surveillance. A democratic legal order must ensure that the protection of security does not come at the cost of privacy, equality and the freedom to participate in public life.

REFERENCES:

1. Shah Alam and Bushra Ansari, "Privacy in a World of Mass Surveillance and Facial Recognition" 7 *International Journal of Legal Science and Innovation* 166 (2025).
2. Alessandro Acquisti, Ralph Gross and Fred Stutzman, "Face Recognition and Privacy in the Age of Augmented Reality" 6 *Journal of Privacy and Confidentiality* 1-20 (2014).
3. European Union Agency for Fundamental Rights, "*Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*" 9 (2019)
4. Ameen Jauhar and Jai Vipra, "Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies" *JURIST – Professional Commentary* (2022).
5. Lavanya G T and Viola Rodrigues, "Adoption of AI Facial Recognition Technology: Challenges to Indian Legal Regime during Pandemic" 3 *International Journal of Legal Science and Innovation* 1238-1247 (2021).
6. Charter of Fundamental Rights of the European Union, 2012 O.J. C 326/391.
7. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, O.J. L 119/89 (2016).
8. Case C-371/24, Comdribus, EU:C:2026:219 (CJEU, 19 March 2026).
9. M. Qandeel, "Facial recognition technology: regulations, rights and the rule of law" 7 *Front. Big Data* 1354659 (2024).
10. Monika Simmler and Giulia Canova, "Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind" 56 *Computer Law & Security Review* (2025).
11. European Data Protection Board, Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement (Final Version, 17 May 2023).

12. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, “*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*” (July, 2018).
13. European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in Law Enforcement (Publications Office of the European Union, 2019).
14. Ananthakrishnan G., "How Facial Recognition Was Used for CJP Protest: Delhi Police to Supreme Court", *The Indian Express*, August 18, 2026.
15. Mahender Singh Manral, "Police Say Cameras 'Caught' Murder, Rape Accused at CJP Protest – Some Were Actually in Jail", *The Indian Express*, September 4, 2026.
16. Ameen Jauhar, “Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement” 16(1) *Indian Journal of Law and Technology* 1 (2020).
17. Smriti Parsheera, “Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?” 28 *A conversation on AI activism* 28, (2021).
18. A. Bag and A. Pradhan, “Who Monitors the Monitors? Analysing the Legal Intricacies of Digital Forensic-based Facial Recognition Technology in Law Enforcement” 13 *Asian J. Legal Educ.* 79 (2026).
19. Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects” *NISTIR 8280 (National Institute of Standards and Technology, U.S. Department of Commerce)*, (2019).
20. European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in Law Enforcement (Publications Office of the European Union, (2019).
21. The Law Communicants, “Facial Recognition & Surveillance in India: Constitutional Issues, Privacy Rights and the Need for a Statutory Framework” *The Law Communicants*, Aug. 14, 2026.
22. Rahul Sharma and Virender Negi, “Facial Recognition Surveillance and the Indian Constitution: A Critical Analysis of Privacy, Equality & State Power” 9 *International*

Journal of Law Management & Humanities 157-172 (2026).

23. Vishal Ranaware and Rahul Mishra, “Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations: Delhi Riots Lessons on Rights and Reliability” 143 *Engineering Proceedings* 17 (2026).
24. The Constitution of India.
25. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
26. The Information Technology Act, 2000 (Act 21 of 2000).
27. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2026.