



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.356>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

FACIAL RECOGNITION, PROTEST ATTENDANCE AND INFERRED POLITICAL AFFILIATION: INFORMATIONAL PRIVACY AND STATE SURVEILLANCE IN INDIA

Aditi Raikwar¹, Rishita Kumre² and Vanshika Sharma³

I. ABSTRACT

Facial recognition has moved in India from pilot projects to routine policing without a statute that says when, against whom, and for what purpose a face may be scanned. This paper examines what that gap means when the face belongs to a person attending a political protest. Attendance at a demonstration is a public act, but the record of who attended, kept by the State and matched against police databases, becomes a durable data set from which political affiliation can be inferred, whether or not the police intend to infer it. The paper builds its argument around the events at Jantar Mantar in July 2026, when the Delhi Police deployed a facial recognition system during the student agitation led by the Cockroach Janta Party over the NEET-UG paper leak, reported that it had matched 2,873 people against its criminal records, and defended its conduct before the Delhi High Court and the Supreme Court. It traces the litigation that followed, including the surveillance petition before the Delhi High Court, the petitions against the police action of 20 July before the Supreme Court, and the Supreme Court's order of 1 September 2026, and it records what each court said and what each court left open. It then compares India with the European Union, the United Kingdom and the European Court of Human Rights, each of which has treated protest-site biometric identification as a distinct problem. The paper contends that the Indian position is not a case of unlawful technology meeting a silent Constitution, but of a settled constitutional standard under Puttaswamy meeting an administrative practice that has never been tested against it. It proposes a narrower and sequenced framework built around a dedicated statute, prior

¹ 5th year B.Sc. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: aditiraikwar.bscllb@nliu.ac.in

² 5th year B.A. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: rishitakumre.ballb@nliu.ac.in

³ 5th year B.Sc. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: vanshikasharma.bscllb@nliu.ac.in

authorisation, a bar on inference of political belief, independent oversight, auditable accuracy standards, and protest-specific rules on retention and notice.

II. KEYWORDS

Facial recognition; informational privacy; right to protest; State surveillance; inferred political affiliation; Puttaswamy; Digital Personal Data Protection Act 2023.

III. INTRODUCTION

A protest is an act of political expression that depends on being seen. Participants stand in public so that others will notice them, and the law has long treated the public character of the act as the reason it receives constitutional protection rather than as a reason it falls outside it. Facial recognition changes what being seen means. A human observer at a demonstration forgets most of what the observer sees. A camera linked to a matching engine and a police database does not forget, and it does not need the participant to be suspected of anything before it begins to record who was present.

The difficulty is sharpest where the matching is done against criminal records. When the Delhi Police reported that its facial recognition teams had identified 2,873 people with criminal antecedents at the Jantar Mantar student protests between 20 and 26 July 2026, the figure was offered as evidence of diligence.⁴ An investigation of police, prison and court records later found that at least 25 of those people were already in jail when they were supposedly identified at the protest site.⁵ The point is not that the police necessarily acted in bad faith. It is that a match produced by a system accepted as "positive" at an accuracy threshold of 80 per cent can attach a person to a place and a cause, and the person has no ordinary means of knowing that the attachment has been made, of contesting it, or of finding out what else is done with it.

⁴Analiza Pathak, '2,873 Faces Scanned at Jantar Mantar? Delhi Police Rejects Mass Surveillance Claims During CJP Protests' (India.com, 18 August 2026) <https://www.india.com/news/india/2873-faces-scanned-at-jantar-mantar-delhi-police-rejects-mass-surveillance-facial-recognition-claims-during-jantar-mantar-cjp-protests-biometric-information-8504123/> accessed 5 October 2026.

⁵Outlook News Desk, 'Jantar Mantar Protest: 25 People Flagged by Facial Recognition Were in Jail for Rape, Murder' (Outlook India, 4 September 2026) <https://www.outlookindia.com/national/jantar-mantar-protest-25-people-flagged-by-facial-recognition-were-in-jail-records-show> accessed 5 October 2026, reporting an investigation by The Indian Express.

The Supreme Court of India settled in 2017 that privacy is a fundamental right and that any State intrusion into it must satisfy the tests of legality, legitimate aim and proportionality.⁶ Since then the Court and legislature have given the standard content in some areas, notably the Aadhaar judgment and the Digital Personal Data Protection Act 2023, but neither has addressed facial recognition by the police at a political gathering. The result is that a technology capable of producing a political record of every attendee operates under an internal standard operating procedure whose content, in the Delhi High Court's own account of the proceedings before it, was still being clarified in July 2026.⁷

Research in computer science adds a further reason for concern. Work published in 2021 reported that a facial recognition algorithm could predict self-reported political orientation from facial images with an accuracy materially above chance, even after controlling for age, gender and ethnicity.⁸ The claim is contested and the paper does not rely on it as proof that any Indian system infers belief from faces. It matters for a different reason. Once facial images of attendees are stored and matched, the inferential capacity of the data does not depend on the original purpose of collection. Attendance at a particular protest, on a particular day, in company with particular other people, is itself a strong signal of affiliation, and no face-based inference is needed to read it.

The puzzle this paper takes up is therefore not whether the State may ever use facial recognition in public places. The real question is what framework should govern its use at protests, how far the existing Indian law already constrains it, and what the July 2026 litigation shows about the distance between the two. The paper proceeds in five parts. It begins with the conceptual problem of converting attendance into inference, sets out the Indian constitutional and statutory framework, develops the Jantar

⁶Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

⁷Malavika Prasad, 'Jantar Mantar Protests: Delhi High Court Suggests Filing Fresh Plea on Police Surveillance After Examining SOPs, Data Protection Act' (LiveLaw, 28 July 2026) <https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-pil-against-surveillance-of-protesters-at-jantar-mantar-543178> accessed 5 October 2026.

⁸Michal Kosinski, 'Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images' (2021) 11 Scientific Reports 100.

Mantar case study in detail, compares the European Union, the United Kingdom and the European Court of Human Rights, and closes with proposals for a calibrated Indian model.

A. Research Objectives

This paper pursues the following research objectives:

1. To explain how facial recognition at a protest converts a public act of attendance into a stored record from which political affiliation can be inferred.
2. To assess the adequacy of the Indian constitutional and statutory framework, including Articles 19 and 21 of the Constitution, the *Puttaswamy* proportionality standard, the Criminal Procedure (Identification) Act 2022 and the Digital Personal Data Protection Act 2023, as applied to facial recognition at protests.
3. To examine the Jantar Mantar events of July 2026 as a case study, including the surveillance and police-action petitions, the statements of the Delhi High Court and the Supreme Court on them, and the directions and suggestions that followed.
4. To compare India's position with that of the European Union, the United Kingdom and the European Court of Human Rights.
5. To propose a calibrated framework for India that protects informational privacy and the freedom of assembly without disabling legitimate policing.

B. Research Questions

The paper is guided by the following research questions:

1. Why does the use of facial recognition at a protest raise a distinct informational privacy problem, over and above the problem of ordinary public photography?
2. What does the Indian legal framework currently require of the State before it deploys facial recognition against assembled citizens?

3. What did the Delhi Police do at Jantar Mantar in July 2026, what did the petitioners allege, and what did the courts say and direct?
4. What can India learn from the European Union's prohibitions, the United Kingdom's judicial scrutiny of police facial recognition, and the European Court of Human Rights' decision on protester identification?
5. What legal and institutional design should India adopt to regulate protest-site facial recognition and to prevent the inference of political affiliation from attendance data?

C. Research Methodology

This paper adopts a doctrinal and comparative legal methodology. The primary materials are the Constitution of India, the Criminal Procedure (Identification) Act 2022, the Digital Personal Data Protection Act 2023, the decisions of the Supreme Court of India, Regulation (EU) 2024/1689, the decision of the Court of Appeal of England and Wales in *Bridges*, and the decision of the European Court of Human Rights in *Glukhin v Russia*.

The case study in Part VI relies on a different class of material, and the limits of that material should be stated plainly. The orders of the Delhi High Court in *Aishe Ghosh v Union of India* are taken from that Court's order portal, and the orders of the Supreme Court in *Shailendra Mani Tripathi v Union of India* and the matters tagged with it from the Supreme Court website; full case titles and numbers have been confirmed against the orders themselves.⁹ Observations made at a hearing but not embodied in an order are identified as oral, and statements attributed to counsel rather than to the Bench are described as such. Contemporaneous reports in LiveLaw, Bar and Bench, Deccan Herald and Outlook India are used as secondary support for matters the orders do not record. Findings about the police system, such as the number of people identified, are

⁹*Aishe Ghosh v Union of India* W.P.(C) 9639/2026 (Delhi HC, orders of 24, 27 and 28 July 2026); *Shailendra Mani Tripathi v Union of India* Diary No 44078/2026 (SC, orders of 28 and 30 July, 3 and 13 August and 1 September 2026); *Yashovardhan Azad v Union of India* W.P.(C) 917/2026 (SC). Case titles and numbers have been taken from the orders themselves.

the police's own claims unless an independent source is named. The Delhi High Court proceedings remained pending when this paper was finalised.

The comparison is confined to the European Union, the United Kingdom and the European Court of Human Rights. The European Union is examined because it is the only major jurisdiction to have prohibited, by statute, both real-time remote biometric identification in public spaces by law enforcement (subject to exceptions) and biometric categorisation that infers political opinion. The United Kingdom is examined because its courts have tested police facial recognition against privacy and equality law. The European Court of Human Rights is examined because *Glukhin* is the leading judgment on facial recognition used to identify a protester.

IV. FROM PUBLIC PRESENCE TO POLITICAL INFERENCE: THE CONCEPTUAL PROBLEM

A. Why "No Expectation of Privacy in Public" Fails

The standard answer to a privacy objection against protest surveillance is that a person who joins a demonstration in a public place cannot expect privacy. The Solicitor General made this argument to the Delhi High Court in July 2026, saying that every protest is videographed and that a claim of privacy in a public place was ironical.¹⁰ The argument treats privacy as a binary between secret and exposed.

Privacy scholarship has not worked on that basis for some time. Solove's taxonomy treats surveillance, aggregation and identification as separate harms, each of which can occur without any disclosure of a secret.¹¹ Nissenbaum's account of contextual integrity asks whether information is flowing in a way that matches the norms of the context in which it was shared.¹² A person who stands on a road at Jantar Mantar shares her presence with passers-by and fellow protesters. She does not thereby consent to its conversion into a searchable record held by the police, matched against

¹⁰Prasad (n 7).

¹¹Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.

¹²Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

a criminal database and retained for a period she cannot discover. The Supreme Court's own formulation of informational privacy in *Puttaswamy* is directed at exactly this control over the use of personal information.¹³

B. Attendance as a Proxy for Belief

Political affiliation is among the most sensitive categories of personal information, and the harm of disclosure is rarely confined to the first act of disclosure. Attendance at a protest organised by a particular movement, on a particular date, is a strong proxy for sympathy with it. A database of attendees therefore operates as a database of political sympathisers, even if every entry was created for a different stated purpose.

Face-based inference adds a second route. Kosinski's 2021 study reported that political orientation could be predicted from facial images at above-chance accuracy.¹⁴ The study has drawn methodological criticism, including the concern that it may be capturing grooming, expression and background features rather than anything intrinsic to the face. The paper does not treat the result as established. Its significance for law is that a regime which permits mass collection of attendee faces cannot rely on the claim that political inference is technically impossible. The prudent legal response is to prohibit the inference by rule and not to wait for proof that it works.

C. Accuracy, Thresholds and the Cost of a False Match

Facial recognition is probabilistic. The Delhi Police stated in a 2022 response to a right to information request, obtained by the Internet Freedom Foundation, that it treated a match as “positive” where the system returned a similarity score of 80 per cent or above.¹⁵ That figure is a match-confidence threshold for acting on a candidate and not

¹³*Puttaswamy* (n 6).

¹⁴Kosinski (n 8).

¹⁵The right to information replies were obtained by the Internet Freedom Foundation, which published the Delhi Police response of 25 July 2022: Internet Freedom Foundation, ‘Delhi Police’s Claims That FRT Is Accurate With a 80% Match Are 100% Scary’ (17 August 2022) <https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/> accessed 7 October 2026; ‘80% Accuracy in Facial Recognition Database Is a Positive Match for Delhi Police: Report’ (Deccan Herald, 17 August 2022) <https://www.deccanherald.com/india/80-accuracy-in-facial-recognition-database-is-a-positive-match-for-delhi-police-report-1136806.html> accessed 7 October 2026.

an error rate. The quantities that measure error are the false match rate and the false non-match rate, neither of which the police have published. Accuracy is also not uniform across populations. The Gender Shades study found markedly higher error rates for darker-skinned women than for lighter-skinned men in commercial classification systems, and the National Institute of Standards and Technology found demographic differentials in false positive rates across a large body of algorithms.¹⁶

A false match at a protest is not a neutral error. It links a person to a criminal record and to a political event in the same entry. The Indian Express examined 205 of the 2,873 people flagged, selected from serious-offence categories rather than at random, and found at least 25 of them in prison at the time.¹⁷ That sample cannot yield an error rate for the whole list, and “at least” signals that the true figure is unknown, but it shows that a list of matches cannot be treated as a list of people present. The police themselves accepted that a match is only an initial screen requiring field verification.

D. The Chilling Effect

The decisive harm of protest surveillance is often the protest that does not take place. Empirical work on online surveillance has found measurable reductions in willingness to engage with sensitive topics once people know they are watched.¹⁸ The Aishe Ghosh petition pleaded the same point in constitutional terms, arguing that the threatened use of surveillance material to identify and expose student protesters turned passive monitoring into a tool of coercion, chilling rights under Articles 19(1)(a) and 19(1)(b).¹⁹ The chilling effect is the link between informational privacy and the freedom of assembly, and it explains why the two rights should be analysed together.

¹⁶Joy Buolamwini and Timnit Gebru, ‘Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification’ (2018) 81 Proceedings of Machine Learning Research 77; Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, National Institute of Standards and Technology, December 2019).

¹⁷Outlook News Desk, ‘25 People Flagged’ (n 5), reporting an examination by The Indian Express of 205 of the 2,873 persons flagged, drawn from serious-offence categories and not selected at random.

¹⁸Jonathon W Penney, ‘Chilling Effects: Online Surveillance and Wikipedia Use’ (2016) 31 Berkeley Technology Law Journal 117.

¹⁹Prasad (n 7).

V. THE INDIAN FRAMEWORK: PRIVACY, ASSEMBLY AND THE STATUTORY GAP

A. Constitutional Standard

Article 19(1)(b) guarantees the right to assemble peaceably and without arms, subject to reasonable restrictions in the interests of sovereignty, integrity and public order under Article 19(3). Article 19(1)(a) protects expression. Article 21 protects life and personal liberty and, since *Puttaswamy*, informational privacy.²⁰ The Court there required that an interference be backed by law, pursue a legitimate State aim, be proportionate to that aim, and carry procedural safeguards against abuse. The Aadhaar judgment applied the proportionality structure to a state database and asked whether the measure was necessary and whether a less intrusive alternative existed.²¹

Earlier decisions bear on the same problem. *Kharak Singh* invalidated night-time domiciliary visits under Article 21, but its holding that privacy is not a guaranteed right, on which it upheld the shadowing of history-sheeters, was overruled in *Puttaswamy*.²² Only the invalidation of the domiciliary visits survives, and the shadowing of history-sheeters now falls to be tested against the *Puttaswamy* requirements, which matters directly to a deployment matched against history-sheeter records. *PUCL* required procedural safeguards for telephone tapping in the absence of a statute and treated an unregulated power of interception as unconstitutional.²³ These decisions support the proposition that surveillance power must be authorised and bounded in advance and cannot rest on executive convenience.

B. The Right to Protest

The Supreme Court has treated peaceful protest as a constituent of democratic life. In *Ramlila Maidan* the Court held that the right to assemble and protest peaceably, and

²⁰Constitution of India 1950, arts 19(1)(a), 19(1)(b), 19(3) and 21; *Puttaswamy* (n 6).

²¹Justice KS Puttaswamy (Retd) v Union of India (2019) 1 SCC 1.

²²*Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295; *Puttaswamy* (n 6), overruling *Kharak Singh* to the extent that it held that the right to privacy is not protected by the Constitution.

²³*People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

the right to be free from arbitrary police action against it, flow from Articles 19 and 21.²⁴ In *Mazdoor Kisan Shakti Sangathan*, which concerned Jantar Mantar itself, the Court held that the State may regulate the time, place and manner of protest but may not impose a blanket prohibition, and it set aside the prohibition on protests at Jantar Mantar and Boat Club.²⁵ *Anuradha Bhasin* confirmed that restrictions on fundamental freedoms are subject to proportionality review and must be published and reasoned.²⁶

C. The Statutory Position

No Indian statute regulates police facial recognition as such. Two enactments touch it. The Criminal Procedure (Identification) Act 2022 authorises the collection of “measurements”, a term that expressly includes photographs alongside finger and palm impressions, iris and retina scans, biological samples and behavioural attributes. Section 3 reaches any person convicted of an offence, ordered to give security for good behaviour under the Code of Criminal Procedure, arrested in connection with an offence punishable under any law, or detained under a preventive detention law. The only offence-based limitation is the proviso exempting certain arrested persons from giving biological samples.

Section 5 permits a Magistrate to direct any person to give measurements for the purpose of an investigation, whether or not that person has been arrested, and section 4 allows the records to be retained for seventy-five years.²⁷ The police relied on the Act before the Supreme Court, stating that matched biometric records are held by the National Crime Records Bureau in compliance with statutory provisions. That reliance is misplaced. Sections 3 and 5 authorise the taking of measurements from persons brought within the criminal process or named in a Magistrate's order. Neither authorises capturing the face of a person attending a public assembly, who has been

²⁴Ramlila Maidan Incident, In re (2012) 5 SCC 1.

²⁵*Mazdoor Kisan Shakti Sangathan v Union of India* (2018) 17 SCC 324.

²⁶*Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

²⁷Criminal Procedure (Identification) Act 2022, ss 2(1)(b), 3, 4 and 5. For the police's reliance on the Act, see Pathak (n 4).

neither arrested nor made the subject of such an order, in order to search it against the database those provisions build.

The Digital Personal Data Protection Act 2023 recognises a right to privacy in digital personal data but exempts processing by the State on broad grounds. Its commencement is staggered. The Digital Personal Data Protection Rules 2025 were notified on 13 November 2025, and the notification of the same date brought into immediate force only the definitions, the provisions establishing the Data Protection Board and certain procedural provisions. Sections 3 to 17, which carry the duties of notice and consent along with the exemptions, and Rules 3, 5 to 16, 22 and 23, come into force eighteen months after publication, in May 2027.²⁸

In July 2026, therefore, neither the obligations of notice, consent and purpose limitation nor the State exemptions were enforceable, which qualifies both the statutory-gap analysis below and the reliance placed on the Act in the petition seeking restraint on biometric surveillance. Once in force, section 17(1)(c) will exempt processing in the interest of the prevention, detection, investigation or prosecution of any offence, and section 17(2)(a) will permit the Central Government to exempt notified instrumentalities of the State in the interests of sovereignty, security and public order.

Section 17(1)(c) applies of its own force; section 17(2)(a) operates only on notification, and no notification extending it to the Delhi Police has been issued. The statute will therefore leave most police use of facial data outside its obligations of notice, purpose limitation and erasure once those obligations commence. The Srikrishna Committee, whose report preceded the Act, had recommended that State surveillance be placed

²⁸Digital Personal Data Protection Act 2023, ss 17(1)(c) and 17(2)(a); Digital Personal Data Protection Rules 2025, r 1; Ministry of Electronics and Information Technology, commencement notification dated 13 November 2025, bringing section 2, sections 18 to 26, section 35, sections 38 to 43 and section 44(1) and (3) into force on publication and sections 3 to 17 eighteen months thereafter.

on a statutory footing with independent oversight, a recommendation that the 2023 Act did not adopt.²⁹

The consequence is a layering of three conditions. The constitutional standard requires a law, the statutes supply none specific to facial recognition at protests, and the practice proceeds under internal standard operating procedures. That is the gap into which the Jantar Mantar events fall.

VI. CASE STUDY: THE JANTAR MANTAR STUDENT PROTEST AND POLICE ACTION, JULY 2026

A. Background

The Cockroach Janta Party began as an online satirical movement in May 2026 and became the organising body for a student agitation over the alleged paper leak in the NEET-UG 2026 examination. Its sit-in and hunger strike at Jantar Mantar began on 20 June 2026.³⁰ According to the Delhi High Court petition discussed below, a permanent surveillance tower had been installed at the site, and the monitoring extended to eating, resting and seeking medical help as well as to protest activity.³¹ The Delhi Police also stationed surveillance vehicles, including one called Ikshana, near the site.³²

On 20 July 2026 students attempted a march to Parliament. The Delhi Police, with the assistance of the Rapid Action Force of the Central Reserve Police Force, used tear gas and lathi charge, and a petition before the Supreme Court alleges that pellets were fired.³³ The agitation intensified after the police action. On 25 July the Union

²⁹Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, 27 July 2018).

³⁰Prasad (n 7).

³¹*ibid.*

³²Outlook News Desk, 'CJP Protest Under AI Watch: Delhi Police's Facial Recognition Vans Spark Privacy Concerns' (Outlook India, 24 July 2026) <https://www.outlookindia.com/national/cjp-protest-under-ai-watch-delhi-polices-facial-recognition-vans-spark-privacy-concerns> accessed 7 October 2026.

³³Victor Dasgupta, 'Supreme Court Makes Strong Remark on Lathi-Charge During Student Protest, Says "Right to Peaceful Protest Is Guaranteed Under Constitution"' (India.com, 27 July 2026) <https://www.india.com/news/india/supreme-court-cockroach-janta-party-cjp-abhijeet-dipke->

Education Minister resigned, and the Centre, according to the Solicitor General's later account, gave the movement's leaders assurances that cases against protesters would be withdrawn, that fresh FIRs would not be registered over the same events, and that compensation for affected families would be considered.³⁴

B. The Facial Recognition Deployment

The Delhi Police stated in an affidavit filed in the Supreme Court on 17 August 2026 that its facial recognition teams at Jantar Mantar between 20 and 26 July identified 2,873 people who matched existing records. Of these, 2,402 matches came from its Crime Kundli database and 471 from police dossier records. The police said that 92 of those identified were named in more than ten criminal cases and 47 were history-sheeters.³⁵

The affidavit denied that the system created a profile of every person present, that biometric information was collected from all protesters, that Aadhaar details were used to summon people, or that personal information was shared with private companies. It described the system as an initial screening tool and said no action would follow from a match alone, because the individual would be physically verified at the spot first. In support of the need for screening, it cited crime figures for the area during the period: seven vehicle thefts, 67 thefts and 123 reports of lost property.³⁶

Three features of this account deserve attention. First, a deployment that checks every attending face against a criminal database necessarily scans every attending face, whatever the system later does with non-matches. The affidavit's denial of "profiling" every person does not address whether non-matching images were stored, for how long, or on what rules. Second, the crime statistics cited are of the kind found in any

[saurav-das-delhi-police-jantar-mantar-amit-shah-home-minister-neet-paper-leak-narendra-modi-8485357/](https://telanganatoday.com/petition-in-supreme-court-seeks-ban-on-pellet-guns) accessed 7 October 2026; 'Petition in Supreme Court Seeks Ban on Pellet Guns' (Telangana Today, 28 July 2026) <https://telanganatoday.com/petition-in-supreme-court-seeks-ban-on-pellet-guns> accessed 7 October 2026.

³⁴Outlook News Desk, 'Supreme Court Quashes FIRs Against Students Involved in CJP Protests' (Outlook India, 1 September 2026) <https://www.outlookindia.com/national/supreme-court-quashes-firs-against-students-involved-in-cjp-protests> accessed 7 October 2026; Dasgupta, 'Lathi-Charge' (n 33), reporting the Education Minister's resignation.

³⁵Pathak (n 4).

³⁶ibid.

busy part of central Delhi in any week. They do not describe a threat of the kind that, under *Puttaswamy*, would make suspicionless biometric screening of a political assembly necessary. Third, the affidavit as reported does not say whether all 2,873 people were accused, convicted or merely named in criminal cases, a gap noted in the Indian Express investigation.³⁷

C. The Petitions

1. **The Delhi High Court surveillance petition:** Aishe Ghosh, a former president of the Jawaharlal Nehru University Students' Union, filed a public interest litigation, *Aishe Ghosh v Union of India*, W.P.(C) 9639/2026, before the Delhi High Court on 15 July 2026, through counsel. It challenged continuous, indiscriminate and intrusive photography and videography at Jantar Mantar and sought the suspension of mass photography and videography until there was a proximate, real and imminent threat to public order.³⁸ It pleaded that the monitoring amounted to a tool of intimidation, and it raised the bodily privacy and dignity of women protesters who were filmed while drenched by heavy rain. It sought a legal framework governing police surveillance, data protection and the use of facial recognition technology.³⁹
2. **The petitions before the Supreme Court:** A batch of petitions before the Supreme Court, led by *Shailendra Mani Tripathi v Union of India*, Diary No 44078/2026, dealt with the police action of 20 July. One sought an independent investigation into the use of lathi charge and tear gas and the preservation of CCTV footage, body-camera recordings and other electronic evidence, together with compensation for the injured.⁴⁰ A second, *Yashovardhan Azad v Union of India*, W.P.(C) 917/2026, filed by a former

³⁷Outlook News Desk, '25 People Flagged' (n 5).

³⁸Outlook News Desk, 'AI Watch' (n 32); Prasad (n 7).

³⁹IANIS, 'Centre Tells Delhi HC Every Protest Is Videographed as Accepted Law-and-Order Measure' (The Hawk, 24 July 2026) <<https://www.thehawk.in/news/india/centre-tells-delhi-hc-every-protest-is-videographed-as-accepted-law-and-order-measure>> accessed 7 October 2026; Prasad (n 7).

⁴⁰Dasgupta, 'Lathi-Charge' (n 33).

Indian Police Service officer and two persons who said they were injured, sought a ban on metallic projectiles and pellets fired from pump-action guns for dispersal of civilian assemblies.⁴¹ Other petitions, including some filed by persons associated with the protests and some seeking action against protesters accused of assaulting police, were heard with them.⁴² A note on the petitioners is needed. The record identifies the petitioners in the Delhi High Court case and the pellet petition as, respectively, a former student union president and a former police officer with two injured individuals, and not as office-bearers of the Cockroach Janta Party. The party's founder, Abhijeet Dipke, and its spokesperson, Saurav Das, were closely involved in the litigation and its aftermath as participants in the negotiations with the Centre, as commentators on the orders, and as the persons on whose behalf the withdrawal of the 5 September march was announced to the Court. The paper accordingly treats the petitions as litigation arising from, and aligned with, the CJP agitation, and does not attribute the filing of any particular petition to the party's leaders.⁴³

D. What the Courts Said

1. **The Delhi High Court on the surveillance petition:** The Division Bench of Chief Justice Devendra Kumar Upadhyaya and Justice Tejas Karia heard the petition on 24, 27 and 28 July. The order of 24 July records only that counsel for the parties had addressed the Court, that their arguments remained inconclusive, and that the matter would be taken up on 27 July; contemporaneous reports of that hearing add that the Bench noted that similar petitions were already pending before the High Court, and that the Centre argued that videography of protests was routine and that there

⁴¹'Petition in Supreme Court Seeks Ban on Pellet Guns' (n 33).

⁴²Debayan Roy, 'CJP Protests: Supreme Court Stays Action Against Protestors in All States, Orders Immediate Release of Minors' (Bar and Bench, 28 July 2026), as reproduced at <https://www.moneylife.in/article/cjp-protests-supreme-court-stays-action-against-protestors-in-all-states-orders-immediate-release-of-minors/81178.html> accessed 5 October 2026.

⁴³Outlook News Desk, 'FIRs Quashed' (n 34).

could be no reasonable expectation of privacy at a public protest.⁴⁴ On 27 July the Additional Solicitor General argued that the protest had concluded and that the reliefs sought had become infructuous, and the Bench orally remarked that the petitioner could file a better-framed petition seeking guidelines, in which the respondents would place on record whatever mechanism existed and the Court would pass orders.⁴⁵ On 28 July the Bench orally suggested that the petitioner examine the existing framework, including the Delhi Police standard operating procedure, the Data Protection Act and the Public Records Act, and then decide whether to file a fresh petition. The Court said it was not adjudicating the legality of the surveillance and that its remarks were general and not tied to the incident. The matter was listed for 25 August.⁴⁶

2. **The Supreme Court on police action:** On 27 July 2026 the Supreme Court, hearing the petitions on the 20 July police action, said that the Constitution guarantees the right to peaceful protest and that a lathi charge cannot be justified merely because a demonstration is taking place.⁴⁷ On 28 July it passed an interim order directing that no coercive action be taken against protesters across the States, other than those with criminal antecedents, and that detained minors without such antecedents be released. It allowed investigations in registered FIRs to continue. It took note of the allegation that pellet guns had been used and that a student had lost his eyesight.⁴⁸ It also directed the preservation of CCTV footage, drone recordings and body-worn camera footage.⁴⁹ The Cockroach Janta Party described the order as

⁴⁴ IANS (n 39).

⁴⁵ Prasad (n 7).

⁴⁶ *ibid.*

⁴⁷ Dasgupta, 'Lathi-Charge' (n 33).

⁴⁸ Roy (n 42); 'Supreme Court Halts Coercive Measures in CJP Protest Cases, Directs Release of Minors' (Manupatra, 29 July 2026)

<https://updates.manupatra.com/roundup/contentsummary.aspx?iid=51584> accessed 7 October 2026.

⁴⁹ 'Release All Minors Held Over Student Protests: SC' (Superkalam, 29 July 2026)

<https://superkalam.com/current-affairs/29-07-2026/release-all-minors-held-over-student-protests-sc-pg1-793e6773-7114-48fc-b0be-508555fc836f> accessed 5 October 2026.

unacceptable because it permitted investigations to continue against the Centre's assurance of withdrawal.⁵⁰ On 30 July the Court said that police are authorised to use pellet guns in extraordinary circumstances and questioned a prayer for a complete ban, while directing the Delhi Government to ensure medical treatment for the injured, directing the Centre to preserve the ammunition records of the Rapid Action Force personnel deployed at Jantar Mantar, and indicating that it was prepared to examine the use of pellet guns on 20 July.⁵¹ On 3 August a bench of Chief Justice Surya Kant and Justices Joymalya Bagchi and V Mohana clarified that Delhi and the States were at liberty to close or withdraw FIRs against protesters, and that "criminal antecedents" in the 28 July order was to be read as grave and heinous offences.⁵² On 1 September 2026 the same bench, invoking Article 142, ordered the closure of the FIRs registered across the country over the student protests of 20 to 25 July and barred fresh FIRs, extending relief nationwide although only the Centre and four State governments had applied. It said the order rested on the circumstances of the case and was not a precedent. It recorded the Centre's assurance that a compensation policy for the families of students who died by suicide after the cancellation of NEET-UG 2026 would be framed within three months. It permitted the Delhi Police to proceed with one FIR against the 2,873 people said to have been present at Jantar Mantar and to have serious criminal

⁵⁰Supreme Court's Conditions Unacceptable, Centre Must Withdraw FIRs as Promised: CJP's Saurav Das' (The Week, 28 July 2026) <https://www.theweek.in/news/india/2026/07/28/supreme-court-saurav-das-cjp-fir-modi-government.html> accessed 5 October 2026.

⁵¹Victor Dasgupta, 'Supreme Court's Big Observation on Security Forces' Action During CJP Protest: "Police Are Authorized to Use Pellet Guns"' (India.com, 30 July 2026) <https://www.india.com/news/india/supreme-court-cjp-protest-cockroach-janta-party-neet-paper-leak-delhi-police-jantar-mantar-amit-shah-crfp-gp-singh-abhijeet-dipke-saurav-das-8488062/> accessed 5 October 2026.

⁵²Ashish Tripathi, 'Supreme Court Clears Path for States to Close FIRs Against Student Protesters in Accordance with Law' (Deccan Herald, 3 August 2026) <https://www.deccanherald.com/amp/story/india/supreme-court-clears-path-for-states-to-close-firs-against-student-protesters-in-accordance-with-law-4097769> accessed 5 October 2026.

antecedents. Mr Das told the bench that the party was withdrawing its call for a march on 5 September in view of the assurances and the order.⁵³

E. Actions Suggested and Directed

The record yields three groups of actions. The first consists of directions and clarifications addressed to the parties: release of minors, restraint on coercive action, preservation of video and ammunition records, medical treatment, closure of FIRs, and a compensation policy within three months. The second consists of assurances given by the Delhi Police rather than directions of either court. Chief among them is field verification before any action on a facial recognition match, which appears in the affidavit filed in the Supreme Court and in the Solicitor General's submission, and which no order in the record directs.

The Internet Freedom Foundation argues that field verification is not a safeguard at all, because the inquiries made at the home, workplace and neighbourhood of a flagged person themselves communicate a supposed connection to the protest, and the State's error surfaces only once an officer arrives; the paper records that as one view.⁵⁴ The third consists of suggestions that were left for the petitioners and the executive to take forward. The Delhi High Court suggested a fresh petition seeking guidelines on police surveillance during protests, framed after examining the standard operating procedure and the data protection and public records statutes, and indicated that it would examine whether those provisions were adequate once the respondents placed the mechanism on record.

⁵³Outlook News Desk, 'FIRs Quashed' (n 34).

⁵⁴Pathak (n 4), reporting the affidavit's statement that a person matched would be physically verified at the spot before any action was taken; 'Facial Recognition Tech Used at CJP Protests Only to Find Those With Criminal Record: Delhi Police to Supreme Court' (Bar and Bench, 18 August 2026) <https://www.barandbench.com/news/litigation/facial-recognition-tech-used-at-cjp-protests-only-to-find-those-with-criminal-record-delhi-police-to-supreme-court> accessed 7 October 2026; Internet Freedom Foundation, 'Delhi Police's Facial Recognition Flagged 25 Jailed People at Jantar Mantar, This Dragnet Must End' (4 September 2026) <https://internetfreedom.in/delhi-polices-facial-recognition-flagged-25-jailed-people-at-jantar-mantar-this-dragnet-must-end/> accessed 7 October 2026.

The Supreme Court's July observations on peaceful protest and the August order on pellet guns invited examination of the force used, and the evidence-preservation directions kept the factual basis available for later proceedings.⁵⁵

F. Assessment

Three conclusions follow, each limited by the incomplete record.

First, neither court decided whether facial recognition of protesters is lawful. The Delhi High Court said in terms that it was not adjudicating the legality of the surveillance, and the Supreme Court's orders concerned force, FIRs and release. The Supreme Court's carve-out for the 2,873 people leaves the use of the facial recognition output as a basis for criminal process untested at the level of principle. The question that *Puttaswamy* makes central, whether the intrusion is backed by law and proportionate, was not reached.

Second, the Delhi High Court's suggestion that the petitioner look to the standard operating procedure, the Data Protection Act and the Public Records Act is a reminder that a regulatory framework exists on paper. As Part V showed, the Data Protection Act exempts most police processing, and a standard operating procedure is an executive document that can be changed by the authority it binds. A petition seeking guidelines is the correct next step, but it asks the Court to supply what Parliament has not.

Third, the 2,873-person carve-out and the later finding that at least 25 matches concerned people in custody together illustrate why the police's "field verification" assurance is the only safeguard presently standing between a match and a consequence.⁵⁶ It is internal, undefined and unaudited. The Court's restriction of the carve-out to persons with grave and heinous antecedents is a useful narrowing, but it depends on the accuracy of the underlying records, which the affidavit did not describe.

⁵⁵Prasad (n 7).

⁵⁶Outlook News Desk, '25 People Flagged' (n 5); Pathak (n 4).

VII. COMPARATIVE EXPERIENCE: THE EUROPEAN UNION, THE UNITED KINGDOM AND THE EUROPEAN COURT OF HUMAN RIGHTS

A. The European Union: Prohibition with Narrow Exceptions

Regulation (EU) 2024/1689, the Artificial Intelligence Act, prohibits the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement, subject to exhaustively listed objectives, such as the targeted search for victims of specified crimes and the prevention of a specific and imminent threat, and subject to prior authorisation by a judicial or independent administrative authority.⁵⁷ It also prohibits biometric categorisation systems that categorise individuals by their biometric data in order to deduce or infer political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation, with a limited exception for the labelling or filtering of lawfully acquired biometric datasets in law enforcement.⁵⁸ The prohibitions applied from 2 February 2025.

Two features are of interest for India. The Regulation fixes in advance the list of purposes that can justify real-time identification and requires an authorisation decision before use, which contrasts with the standing operational discretion in the Delhi Police deployment. It also names political opinion as a category that biometric systems may not be used to infer, which is the legal form of the concern raised in Part IV. The cost of the model is complexity and a heavy reliance on administrative capacity; a point developed in the comparison in Part VII.D.

B. The United Kingdom: Judicial Scrutiny of Police Deployment

In *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal held that the police's use of automated facial recognition in public places was not "in accordance with the law" for the purposes of Article 8 of the European Convention on Human Rights, because the legal framework left too much discretion to individual officers

⁵⁷Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L2024/1689, art 5(1)(h) and art 5(3).

⁵⁸*ibid* art 5(1)(g).

over who could be placed on a watchlist and where the technology could be deployed. It also found that the data protection impact assessment was deficient and that the force had not complied with the public sector equality duty because it had not investigated whether the software was biased on grounds of race or sex.⁵⁹

The decision is relevant to India for its method. The court did not hold facial recognition unlawful in principle. It required the police to operate within a framework that fixed who could be targeted and where, and it required an assessment of discriminatory performance before deployment. Both requirements are absent from the Indian record as it stands.

C. The European Court of Human Rights: Protester Identification

In *Glukhin v Russia* the European Court of Human Rights considered the use of facial recognition technology to identify a man who had held a lone picket in the Moscow metro and to prosecute him for failing to notify the authorities. It held that the use of facial recognition to identify and locate a person who was exercising peaceful expression was a particularly intrusive interference, that the domestic law offered no adequate safeguards, and that the interference violated Articles 8 and 10 of the Convention.⁶⁰

The judgment links the privacy and expression questions in the way the *Aishe Ghosh* petition attempted to link Articles 21 and 19. It does so within the ordinary test of what is necessary in a democratic society, but it calibrates that test to the technology: the Court held that a high level of justification is required for measures of this kind, with the highest level of justification required for the use of live facial recognition technology, and it found that the use made of the technology against the applicant did not correspond to a pressing social need.

Commentators have read the judgment as establishing a standard of strict necessity, but the Court itself did not use that language. Two further findings bear directly on Part IV. The Court observed that the data processed revealed the applicant's political

⁵⁹*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.

⁶⁰*Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023).

opinion, and that the use of highly intrusive facial recognition to identify and arrest participants in peaceful protest could have a chilling effect on the rights to freedom of expression and assembly.⁶¹

D. Reading the Three Together

None of the three is available to India in an unmodified form. The European Union's prohibition rests on an administrative architecture of notified authorities and market surveillance bodies that India have not built. The United Kingdom's approach rests on litigation under a human rights statute and a developed body of data protection guidance.

The European Court's approach rests on a treaty system with a standing court, and no Indian equivalent exists for individuals to challenge systems of this kind. What each does supply is a design lesson: a pre-fixed list of permitted purposes and a prohibition on political inference from the Union, a legally defined framework and a pre-deployment bias assessment from the United Kingdom, and, from Strasbourg, the requirement of the highest level of justification where facial recognition is used to identify a protester. The Indian response should draw on all three while relying on its own constitutional standard, which in *Puttaswamy* is already as demanding as these models.

VIII. TOWARDS A CALIBRATED MODEL: PROTECTING PROTEST ATTENDANCE IN INDIA

The record considered above points away from two responses: leaving facial recognition at protests to executive standard operating procedures, and prohibiting all police use of the technology in public places. The first fails the legality limb of *Puttaswamy*. The second is probably unachievable and could prevent uses, such as the search for a missing child, that are plainly legitimate. The model proposed here is a narrower, sequenced framework built around seven choices.

⁶¹Glukhin (n 60) paras 86, 88 and 89.

The first choice is a dedicated statute. The legality requirement means that the authority for facial recognition against assembled persons should be set out in an Act of Parliament and not in internal procedure. The statute should define the permitted purposes, identify the officers who may authorise deployment, fix the databases against which faces may be matched, and bind every police force and central agency. The Srikrishna Committee's recommendation of a statutory footing for State surveillance remains the most developed domestic proposal.⁶²

The second choice is prior authorisation. Deployment at a lawful assembly should require a written, reasoned order from a judicial or independent authority, identifying the specific threat, the duration and the area, and should lapse on a short-fixed date. The Indian courts have long required comparable authorisation for telephone interception, and the reasoning of *PUCL* applies at least as strongly to a technology that scans a crowd.⁶³ The model should make clear that the existence of past criminal records among the general population in a city is not a threat specific to a gathering.

The third choice is a statutory bar on the inference of political belief. The statute should prohibit the use of facial recognition, attendance logs and the images captured at an assembly to infer, record or categorise the political opinion, religious belief or union membership of any attendee, and should prohibit the creation of attendee lists or databases from such images. Non-matching images should be deleted immediately, and matching images retained only for the period needed for the verified purpose. This follows the approach of Article 5(1)(g) of the Artificial Intelligence Act and responds to the inferential risk discussed in Part IV.B.⁶⁴

The fourth choice is accuracy and bias standards that are tested before deployment and published. The *Bridges* decision shows that a deficient assessment is a legal defect and not a technical detail. A system used on Indian crowds should be independently tested on Indian population data and should publish its false match and false non-match rates, disaggregated by sex and skin tone, rather than a single match-confidence

⁶²Srikrishna Committee (n 29).

⁶³*PUCL* (n 23).

⁶⁴Regulation (EU) 2024/1689 (n 57) art 5(1)(g); Kosinski (n 8).

threshold of the kind the Delhi Police reported. An audit should follow before and after each deployment.⁶⁵

The fifth choice is an independent oversight body with powers of audit and a duty to report to Parliament. The Data Protection Board established under the 2023 Act is not confined to the private sector. "Person" in section 2(s) includes the State, section 7(b) contemplates processing by the State and its instrumentalities, and Rule 5 of the 2025 Rules prescribes standards for such processing, so the Board will have jurisdiction over State data fiduciaries.

The limits lie elsewhere. The section 17 exemptions remove most police processing from the Board's reach, and the executive controls its composition, since the Rules place a search-cum-selection committee chaired by the Cabinet Secretary in charge of recommending the Chairperson.⁶⁶ A separate oversight authority for State surveillance, with access to logs of every deployment and a footing independent of executive appointment, would give effect to the procedural guarantee limb of *Puttaswamy*.

The sixth choice is notice and remedy. Signage at the site, a public register of authorisations and a route for any person identified to learn of the match and challenge it are modest steps that the Delhi Police affidavit does not mention. A person who is named in a list of those "identified at a protest" and finds that the list leads to an FIR should be able to see the basis of the match. The Supreme Court's own carve-out of 2,873 people for continued proceedings makes this need concrete.

The seventh choice is a protest-specific rule that treats the exercise of the right to assemble as a factor weighing against the proportionality of surveillance. In the *Mazdoor Kisan Shakti Sangathan* judgment the Court recognised that protest sites are public forums for dissent, and a framework that reaches Jantar Mantar should begin

⁶⁵*Bridges* (n 59); Outlook News Desk, '25 People Flagged' (n 5); Buolamwini and Gebru (n 16).

⁶⁶Digital Personal Data Protection Act 2023, ss 2(i), 2(s), 7(b), 17 and 18(1); Digital Personal Data Protection Rules 2025, rr 5 and 17 to 21.

from the premise that dissent is the activity to be protected and not the risk to be managed.⁶⁷

These choices should be sequenced, and the Supreme Court is now the forum in which the sequence should begin. On 13 August 2026 the Court tagged the petition of A A Rahim, which asks it to declare indiscriminate biometric surveillance at peaceful assemblies unconstitutional and to restrain such surveillance until Parliament legislates, with the matters already before it on the Jantar Mantar deployment.⁶⁸ That prayer matches the first choice proposed above and can be cited in its support.

The statute and the oversight body should precede any wider deployment, and interim relief in those proceedings is the appropriate bridge: deletion of non-matching images, subject to the Court's own direction preserving the video record, written authorisation for any further matching, and a published pre-deployment audit. The surveillance petition before the Delhi High Court was listed for 25 August 2026. A guidelines petition there retains value, but it can no longer be the primary vehicle for a question of which the Supreme Court is now seised.

IX. CONCLUSION

The events at Jantar Mantar in July 2026 present a clear picture of the question this paper set out to address. A State deployed facial recognition against a student protest, reported a large number of matches against criminal records, said that it would act only after verification, and was met by two sets of petitions. The courts gave strong statements about the right to peaceful protest, quashed the FIRs and preserved the evidence, and left the question of the legality of protest-site facial recognition undecided.

⁶⁷Mazdoor Kisan Shakti Sangathan (n 25).

⁶⁸AA Rahim v Union of India (SC, order of 13 August 2026), tagged with the petitions already pending on the Jantar Mantar deployment; 'SC Agrees to Hear Plea Against Police's Use of "Facial Recognition" at Jantar Mantar Protest' (The Hitavada, 14 August 2026) <https://www.thehitavada.com/Encyc/2026/8/14/sc-agrees-to-hear-plea-against-polices-use-of-facial-recognition-at-jantar-mantar-protest.html> accessed 7 October 2026.

The Delhi High Court's suggestion that the petitioner seek guidelines on a better-framed petition, together with the Supreme Court's carve-out for the 2,873 people, shows that the matter is still open.

The comparative record shows that other legal systems have answered the same question with prohibitions, judicial scrutiny and a requirement of the highest level of justification, and that none of them treats a protest as a place where a person gives up control over the record of her presence. India's own constitutional standard is as demanding as these models, but it has not yet been applied.

The measure of a future Indian framework will be whether the authority to scan an assembly is stated in a statute, whether a neutral authority approves it before it is used, whether political inference from attendance data is prohibited, whether errors are measured and published, and whether a person who is wrongly matched has a remedy. Until those conditions exist, the attendance of a citizen at a protest remains a record that the State can create without her knowledge and use without her consent.

X. BIBLIOGRAPHY

A. Primary Legislation and Regulatory Instruments

1. Constitution of India 1950, arts 14, 19 and 21.
2. Criminal Procedure (Identification) Act 2022.
3. Digital Personal Data Protection Act 2023.
4. Digital Personal Data Protection Rules 2025.
5. European Convention on Human Rights, arts 8 and 10.
6. Ministry of Electronics and Information Technology, Notification bringing specified provisions of the Digital Personal Data Protection Act 2023 into force (13 November 2025).
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L2024/1689.

B. Cases

1. *AA Rahim v Union of India* (Supreme Court of India, order of 13 August 2026).
2. *Aishe Ghosh v Union of India*, W.P.(C) 9639/2026 (Delhi High Court, orders of 24, 27 and 28 July 2026, pending).
3. *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.
4. *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023).
5. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
6. *Justice KS Puttaswamy (Retd) v Union of India* (2019) 1 SCC 1.
7. *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.
8. *Mazdoor Kisan Shakti Sangathan v Union of India* (2018) 17 SCC 324.
9. *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.
10. *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.
11. *Ramlila Maidan Incident, In re* (2012) 5 SCC 1.
12. *Shailendra Mani Tripathi v Union of India*, Diary No 44078/2026 (Supreme Court of India, orders of 28 and 30 July, 3 and 13 August and 1 September 2026).
13. *Yashovardhan Azad v Union of India*, W.P.(C) 917/2026 (Supreme Court of India).

C. Reports and Official Materials

1. Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, 27 July 2018).

2. Grother P, Ngan M and Hanaoka K, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, National Institute of Standards and Technology, December 2019).

D. Books, Articles and News Sources

1. '80% Accuracy in Facial Recognition Database Is a Positive Match for Delhi Police: Report' (Deccan Herald, 17 August 2022).
2. Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.
3. Dasgupta V, 'Supreme Court Makes Strong Remark on Lathi-Charge During Student Protest, Says "Right to Peaceful Protest Is Guaranteed Under Constitution"' (India.com, 27 July 2026).
4. Dasgupta V, 'Supreme Court's Big Observation on Security Forces' Action During CJP Protest: "Police Are Authorized to Use Pellet Guns"' (India.com, 30 July 2026).
5. 'Facial Recognition Tech Used at CJP Protests Only to Find Those With Criminal Record: Delhi Police to Supreme Court' (Bar and Bench, 18 August 2026).
6. IANS, 'Centre Tells Delhi HC Every Protest Is Videographed as Accepted Law-and-Order Measure' (The Hawk, 24 July 2026).
7. Internet Freedom Foundation, 'Delhi Police's Claims That FRT Is Accurate With a 80% Match Are 100% Scary' (17 August 2022).
8. Internet Freedom Foundation, 'Delhi Police's Facial Recognition Flagged 25 Jailed People at Jantar Mantar, This Dragnet Must End' (4 September 2026).
9. Kosinski M, 'Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images' (2021) 11 Scientific Reports 100.
10. Nissenbaum H, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

11. Outlook News Desk, 'CJP Protest Under AI Watch: Delhi Police's Facial Recognition Vans Spark Privacy Concerns' (Outlook India, 24 July 2026).
12. Outlook News Desk, 'Jantar Mantar Protest: 25 People Flagged by Facial Recognition Were in Jail for Rape, Murder' (Outlook India, 4 September 2026).
13. Outlook News Desk, 'Supreme Court Quashes FIRs Against Students Involved in CJP Protests' (Outlook India, 1 September 2026).
14. Pathak A, '2,873 Faces Scanned at Jantar Mantar? Delhi Police Rejects Mass Surveillance Claims During CJP Protests' (India.com, 18 August 2026).
15. Penney J, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Technology Law Journal 117.
16. 'Petition in Supreme Court Seeks Ban on Pellet Guns' (Telangana Today, 28 July 2026).
17. Prasad M, 'Jantar Mantar Protests: Delhi High Court Suggests Filing Fresh Plea on Police Surveillance After Examining SOPs, Data Protection Act' (LiveLaw, 28 July 2026).
18. 'Release All Minors Held Over Student Protests: SC' (Superkalam, 29 July 2026).
19. Roy D, 'CJP Protests: Supreme Court Stays Action Against Protestors in All States, Orders Immediate Release of Minors' (Bar and Bench, 28 July 2026), as reproduced in Moneylife.
20. 'SC Agrees to Hear Plea Against Police's Use of "Facial Recognition" at Jantar Mantar Protest' (The Hitavada, 14 August 2026).
21. Solove D, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.
22. 'Supreme Court Halts Coercive Measures in CJP Protest Cases, Directs Release of Minors' (Manupatra, 29 July 2026).

23. 'Supreme Court's Conditions Unacceptable, Centre Must Withdraw FIRs as Promised: CJP's Saurav Das' (The Week, 28 July 2026).
24. Tripathi A, 'Supreme Court Clears Path for States to Close FIRs Against Student Protesters in Accordance with Law' (Deccan Herald, 3 August 2026).