

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. OF 2026

(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

IN THE MATTER OF:

A. A. RAHIM M.P.

VERSUS

1.

RESPONDENT NO. 1

2.

RESPONDENT NO. 2

3.

RESPONDENT NO. 3

4.

,

RESPONDENT NO. 4

5.

,

RESPONDENT NO. 5

WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF

INDIA

TO
THE HON'BLE CHIEF JUSTICE
OF INDIA AND HIS COMPANION
JUSTICE OF THE HON'BLE SUPREME COURT

THE HUMBLE PETITION OF THE
PETITIONER ABOVE NAMED

MOST RESPECTFULLY SHOWETH:

That the following facts of public importance are being raised in the present
Public Interest Petition (PIL):

1. The present Public Interest Litigation under Article 32 of the Constitution of India challenges the deployment by the Delhi Police of facial recognition technology and allied mass-surveillance measures against persons who participated in the peaceful public assembly at Jantar Mantar, New Delhi, led by the Cockroach Janta Party and various student and youth organisations. The Petitioner seeks a declaration that such surveillance is unconstitutional, and, *inter alia*, consequential directions to forthwith cease and desist from deploying facial recognition technology, and allied surveillance measures against persons participating in peaceful public assemblies, until a legislation authorising it is validly enacted. That the present Petition is *bona fide* and is filed solely in the public interest. The Petitioner has no personal interest, private grievance or oblique motive in instituting these proceedings. The Petitioner does not stand to derive any personal gain, benefit or advantage from the outcome of the petition.
2. The impugned surveillance is carried on without the sanction of any law, rule or published safeguard, and in violation of Articles 14, 19 and 21 of the

Constitution. It is not confined to this assembly alone. It reflects a standing and expanding practice of biometric surveillance of peaceful protest by the Delhi Police, conducted in a legal vacuum, which affects the fundamental rights of the public at large. The present petition is therefore filed in public interest. The facts averred by the Petitioner herein are to the best of the Petitioner's knowledge and as ascertainable from various reports on the gathering(s).

3. That the Petitioner humbly submits that this Petition is maintainable under Article 32 of the Constitution of India. The email ID of the Petitioner herein is _____, and the mobile phone number is +91-_____. The annual income of the Petitioner is _____, Pan Card No. _____.

marked as **ANNEXURE P-1 (PAGES 35 TO 36)**.

4. That the present petition is being filed under Article 32 of the Constitution of India seeking appropriate writ, order, or directions has been sought to issue a writ of mandamus or any other appropriate writ, order or direction to the Union of India.
5. That the Respondent(s) are instrumentalities of the State, hence State within the meaning of Article 12 of the Constitution of India.

6. The Respondent authorities/organisations have been arrayed as parties to the present Petition in view of the nature of issues raised herein and the reliefs sought. Respondent No. 1 is the Union of India, through the Secretary, Ministry of Home Affairs, under whose authority the Delhi Police functions. Respondent No. 2 is the Commissioner of Police, Delhi, being the authority that has deployed and is responsible for the impugned surveillance at Jantar Mantar. Respondent No. 3 is the National Crime Records Bureau, an attached office of the Ministry of Home Affairs. It is the nodal agency for the Crime and Criminal Tracking Network & Systems (CCTNS) and operates the National Automated Fingerprint Identification System (NAFIS), against which fingerprints captured through the “Abhigyan” mobile application are matched. Respondent No. 4, M/s CP PLUS (Aditya Infotech Limited), is the private entity that designed, developed and supplied the "Ikshana" facial recognition surveillance vehicle deployed at the assembly, and whose software is integrated for its live monitoring. Respondent No. 5, M/s Dimension NXG Private Limited, is the private entity that develops and supplies the “AjnaLens” artificial-intelligence-enabled facial recognition smart spectacles deployed by the police at the assembly.
7. That the Petitioner has no personal interest in the litigation and the petition is not guided by self-gain or for the gain of any other person/ institution/body, and that there is no motive other than of public interest in filing the writ

petition. The present petition is not guided by any professional considerations and is being filed purely in the public interest by the Petitioner.

8. That the petition, if allowed, would benefit the public at large, as the rule of law is essential for democracy, and such brazen violation of law by the Respondents can be stopped by the orders of this Hon'ble Court only.
9. That the people affected by such acts of the State are numerous and are not in a position to approach the Hon'ble Court; hence the Petitioner is filing the present PIL on behalf of such affected persons.
10. That the Petitioner has based the instant petition on authentic information and documents obtained from various government departments/portals/ RTI applications and has determined the veracity of the same.
11. That the Petitioner undertakes to pay the costs, if any, imposed by the Hon'ble Court on the present PIL at any stage.
12. That the brief facts leading to the rise of the present case are enumerated hereunder:
 - a) The regulation of protests in Delhi is governed by a body of Delhi Police standing orders and circulars. These regulate the grant of permission for, and the conduct and dispersal of, assemblies. However, none of these standing orders or circulars provide for, address or authorise, the indiscriminate collection or use of biometric information, and facial recognition technologies, or any safeguard / guardrails against its misuse. Critically, no

procedure with respect to the usage of such information / linking to databases concerning an individual has been provided for whatsoever.

True and typed copies of the standing orders and circulars issued by the Delhi Police in relation to the regulation of protests are annexed as **ANNEXURE P-2 (PAGES 37 TO 109).**

- b) In 2022, the government think tank NITI Aayog identified in its latest discussion paper on Artificial Intelligence (AI) and facial recognition technology that biased training models, lack of algorithmic transparency, absence of a grievance redressal system, inadequate privacy protections are some of the risks and challenges posed by FRT.

True copy of the Niti Ayog Discussion Paper dated December 2022 is annexed as **ANNEXURE P-3 (PAGES 110 TO 190).**

- c) On or around 20 June 2026, a peaceful sit-in and hunger strike led by the Cockroach Janta Party (“CJP”) and various student and youth organisations. commenced at Jantar Mantar, New Delhi with due permission from the Delhi Police. The assembly, comprising students, journalists and ordinary citizens, swelled at its peak to a reported gathering of over 10,000 persons, to the best of the Petitioner’s knowledge and as ascertainable from various reports on the gathering(s).
- d) From the outset of the protest, the Delhi Police subjected the protesters to continuous and indiscriminate surveillance. This surveillance took three principal forms: first, the widespread acquisition of video footage and

photographs of the persons present; second, the processing of such footage through automated facial recognition technology; and third, the collection and matching of fingerprints through a mobile fingerprint-identification application.

- e) Indiscriminate footage acquisition: The acquisition of footage was pervasive and indiscriminate. Digital video and photographs of the persons present were captured, in real time, through pre-existing CCTV cameras as well as those mounted on the “Mobile Command and Control Vehicle”, towers installed at the site, aerial drones. There were also police photographers and officers using body-worn cameras, hand-held devices and their personal mobile phones.
- f) In the present case, the collection of biometric data began the moment any individual stepped into the radius of the site(s) of demonstration through the key entry-points regardless of intention to participate. First, the existing CCTV cameras installed at the entry and exit points around the Connaught Place area would have captured persons merely making their way from the Connaught Place Circle to Jantar Mantar. Next, police officials, some in fluorescent vests and others in plain clothes, subjected the persons present to recording through cameras mounted on vans and aerial drones. Further, police officials filmed the persons present at close quarters on hand-held devices, including official cameras and their personal mobile phones. Every person present and naturally included the ordinary activities and bodily

functions performed at the specified locations, where people often spent hours at time and were therefore constrained to eat, rest, sleep, endure, police brutality and unfavourable weather conditions and seek medical assistance. Plain-clothes policemen were dispersed across the venue who intermittently launched lathi-charge upon the peaceful assembly.

- g) Further, the existing surveillance mechanism was extended as additional CCTV cameras were installed around Jantar Mantar on the night of 23rd July and the images/footage collected was analysed on screens in the mobile police control room. The general public was unaware whether the footage so acquired includes sound recordings.

True copy of the articles titled “*Delhi police deploys facial recognition cameras at Jantar Mantar to track wanted criminals*” dated 24.07.2026 published by the Times of India and “*Protest venue under a web of cameras and facial recognition systems*” dated 24.07.2026 published by The Hindu are annexed as **ANNEXURE P-4 (PAGES 191 TO 196).**

- h) At no stage were the persons present given any notice or disclosure that they were being subjected to CCTV, drone, body-worn camera or facial recognition surveillance, nor were they informed of the coverage, the purpose, the retention or the databases against which their images and biometric data would be processed. No signage or public notice to that effect was displayed at or around the assembly. On the contrary, a substantial part of the recording was carried out covertly, by officers in plain clothes and on

their personal mobile devices. This is so notwithstanding that the disclosure of camera surveillance to the persons subjected to it is a settled legal requirement, as set out in the Grounds hereinbelow.

- i) Automated facial recognition: The footage so acquired was subjected to automated facial recognition technology (“AFRT”). The feeds were processed in real time within the “Ikshana” vehicle, and through “AjnaLens” smart spectacles worn by officers. The biometric data (i.e. measurements of the facial features) were extracted and compared with an undisclosed database to check for similarity.
- j) The deployment of the "AjnaLens" artificial-intelligence-enabled smart spectacles by the Delhi Police is further evidenced by official procurement and acquisition records, which demonstrate that the said equipment was procured from Respondent No. 5, M/s Dimension NXG Private Limited, for operational use by the Delhi Police. The said records establish the direct involvement of Respondent No. 5 in the supply of AI-enabled smart spectacles equipped with facial recognition capabilities to the Delhi Police. True copies of the documents evidencing the acquisition of the "AjnaLens" spectacles from Respondent No. 5, are annexed herewith and marked as **ANNEXURE P-5 (PAGES 197 TO 216)**.
- k) At this juncture, at the own admission of the Delhi Police, it has become apparent that the footage of the persons present at Jantar Mantar has been subjected to AFRT. The Delhi Police declared to the press that four (4)

Facial Recognition System (“FRS”) units have been installed at key entry and exit points around the protest venue and are linked to the Delhi Police database. Given the sheer daily footfall, the Delhi Police has captured and identified the biometric details of thousands of citizens.

l) It is important to flag that, in response to a Right to Information (RTI) application filed in 2022, the Delhi Police categorically stated that AFRS is generally restricted to searches for missing persons, heinous cases or the identification of dead bodies. The Delhi Police has however, provided no justification for the deployment of such extreme measures, given that it

m) In the said reply the Delhi Police also stated that an 80% similarity score is treated as a positive facial recognition match. However, the repercussions of being identified and matched using AFRS are not laid down in any SOP, guideline or regulation. Further, there are no safeguards to ensure identified individuals are apprised of such inclusion, its basis and the similarity percentage. The Delhi Police has further claimed that the said technology helped identify numerous persons with criminal antecedents. The said claims are unverified, and the Respondents are put to strict proof thereof.

True copies of the relevant RTIs and their responses are annexed as **ANNEXURE P-6 (PAGES 217 TO 221).**

A true copy of the article titled ‘*Police identify 2500 people with criminal records at Jantar mantar protest through facial recognition cameras*’ dated

24.07.2026 published by The Times of India is annexed as **ANNEXURE P-7.**
(PAGES 222 TO 223).

A True copy of the Indian Express article "*Live video feeds, AI-aided facial recognition: How police are surveilling protesters at Jantar Mantar*" dated 24.07.2026 is annexed as **ANNEXURE P-8. (PAGES 224 TO 227).**

- n) Even so, the basis on which any action was taken against persons said to bear a prior database record remains wholly unclear. The Delhi Police has offered no clarification, whether in its press statements or otherwise, of the protocol for matching the images collected against the database, of the identity and particulars of that database, or which images and footage are added to it. The entire exercise is thus opaque and incapable of verification.
- o) Mobile fingerprint identification: The protesters were reportedly also subjected to biometric identification through "Abhigyan", a mobile application developed by the NCRB. The fingerprints of the persons present were captured and run against the National Automated Fingerprint Identification System ("NAFIS"), without any arrest or formal proceeding.
- p) Delhi Police subjected individuals present to fingerprint verification at random, in order to intimidate those gathered, in a grave violation of their right to privacy. However, the criteria for fingerprint matching are not provided, but more importantly, such arbitrary collection of biometric data lacks any legal sanction.

- q) The progression of the demonstrations revealed that the above-mentioned cameras and recording devices were being used by the police to capture routine and private activities of the protesters such as footage of them eating, resting and seeking medical assistance. The instances of indiscriminate collection of photographic and biometric data of unsuspecting citizens have been reported in the mainstream media that involve coercion and outrage of modesty of women.
- a) For example, a group of female protesters were deliberately photographed and filmed in rain-soaked constituting a grave intrusion into their bodily modesty, privacy and dignity.
- b) Similarly, it was also reported that certain young non-violent protesters were blackmailed by the police officials who threatened that their photographs would be transmitted to their parents and educational institutions.
- r) The nature of the images captured using facial recognition technology by the apparatus listed above enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. The facial recognition derived biometric data is information of an intrinsically private character. In view of its continuous use in course the week, it is apprehended that the Delhi Police

is now in possession of the private data of thousands of citizens, which was acquired without reason or consent.

- s) It is humbly submitted, that the Article 21 protections of the Constitution are engaged by the initial gathering of the information and that it is sufficient if biometric data is captured, stored and processed, even momentarily. In fact, in the light of constitutional protections, the right to privacy extends to biometric data derived from a person's facial features that are manifest in public.
- t) The instances of the violation of Article 21 rights of peaceful protestors (and even innocent bystanders) are illustrative of the absence of pervasive protections and the lacunae in the framework as it currently exists. The lack of prescriptions to curb the collection of personal and biometric data by the police leaves citizens powerless against the inclusion of their particulars in a database. Further, beyond collection, the parameters for the processing, storage and sharing remain undefined.
- u) That aggrieved by the aforesaid act, the Petitioner is before this Hon'ble Court, inter alia, following which are without prejudice to one another:

GROUND

The Petitioner most respectfully submits the following grounds for the issuance of a writ under Article 32 of the Constitution of India:

- A. BECAUSE** the sheer scale and intensity of the impugned surveillance was such that it ceased to be mere observation and became, in itself, an

interference with the right to protest under Articles 19(1)(a) and 19(1)(b) of the Constitution. The surveillance was continuous, pervasive and multi-layered. It was conducted at close quarters and in an overtly intrusive manner. Cameras and recording devices were thrust directly at the faces of individual protesters. Officers filmed them from close range, followed their movements, and trained devices upon them as they spoke, gathered and rested. The chilling effect was thus not speculative but actual and manifest. A person under the shadow of surveillance cannot move, speak or associate freely: *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (Subba Rao, J., **dissenting**), as approved in *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1. A measure that deters citizens from exercising a constitutional right injures the right itself: *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

B. BECAUSE the right to privacy, including informational and bodily privacy, is a fundamental right under Article 21, and every State intrusion upon it must satisfy the threefold requirement of legality, legitimate aim and proportionality — including necessity and the adoption of the least restrictive alternative — as held in *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 [SCR Para 180] (“*Puttaswamy I*”), and *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1 (“*Puttaswamy II*” or “*Aadhaar Judgement*”). The impugned live facial recognition and blanket videographic surveillance satisfy none of these requirements.

- C. BECAUSE impugned actions of surveillance are unconstitutional for want of the sanction of law. The capture of biometric identifiers of persons attending a peaceful assembly, and the subsequent processing, storage, sharing and use of such data, each constitutes an intrusion into the right to privacy guaranteed under Article 21 of the Constitution. Per **Puttaswamy I**, it must at the threshold satisfy the requirement of legality, namely the existence of a valid enacted law authorising the intrusion. There exists no statute empowering the Delhi Police to collect the biometric or personal data of persons present at a lawful assembly. An executive notification, such as Delhi Police Standing Order does not satisfy the requirement of a valid law contemplated in **Puttaswamy I** and **Puttaswamy II**. Absent any law, it is ex facie unconstitutional.
- D. BECAUSE the Criminal Procedure (Identification) Act, 2022 does not supply the requisite authority either. That Act permits the taking of “measurements” only of persons convicted or arrested for an offence, persons ordered to give security for good behaviour, and persons detained under a preventive detention law (Sections 3 and 5); it confers no power upon the police to capture the facial images, biometric identifiers or video footage of members of the public attending a peaceful assembly. The impugned collection therefore falls wholly outside the scheme of the said Act and cannot derive any legitimacy from it. In any event, the constitutional validity of the said Act, and the Rules made thereunder, is

itself pending challenge before this Hon'ble Court in *Harshit Goel v. Union of India*, W.P. (Crl.) 869/2022 along with *Sahibe Alam v. Union of India*, W.P. (Crl.) 672/2026.

E. BECAUSE the impugned surveillance is precisely the kind of roving, suspicionless intrusion into privacy that this Hon'ble Court has held to be unconstitutional. In *District Registrar and Collector v. Canara Bank*, (2005) 1 SCC 496, it was held that the State cannot have unrestricted access to inspect and seize or make roving inquiries into the personal data of individuals without any reliable information, and that in the absence of some probable or reasonable cause or basis, and of adequate safeguards. The impugned surveillance is the very embodiment of such a roving intrusion. It captures and processes the biometric data of every person present, without any individualised suspicion, reasonable cause or recorded basis, except their presence at the protest. It is attended by no safeguard against abuse. It was further held in *Canara Bank* (supra) that the right to privacy inheres in the person, and is not lost merely because information has passed out of one's own custody. [Pg. 523, Para 53]. To like effect, in *PUCL v. Union of India*, (1997) 1 SCC 301, this Hon'ble Court held that surveillance cannot be sustained in the absence of procedural safeguards against its arbitrary exercise; the Court accordingly laid down safeguards to govern it.

F. BECAUSE the impugned surveillance was carried out covertly and without any notice or disclosure to the persons subjected to it, in breach of the requirement of transparency and prior notice that the law imposes even upon the least intrusive forms of camera surveillance. The requirement of prior notice is the first of the privacy principles endorsed by the Hon'ble Supreme Court in *K.S. Puttaswamy v. Union of India*, [2017] 10 SCR 569 [Para 184], namely that a data controller must give notice of its information practices before any personal information is collected. Consistent with this principle, the Hon'ble Supreme Court in *Paramvir Singh Saini v. Baljit Singh*, (2021) 1 SCC 184 directed that the police, and the offices of investigative and enforcement agencies, must prominently display, at the entrance and inside their premises, notice that the premises are under CCTV coverage, together with the period of retention of such footage. The obligation of disclosure thus attaches even to static CCTV operated by the police, and the transparency and notice principle is further embodied in the Digital Personal Data Protection Act, 2023. Here, by contrast, no notice or signage disclosed to the assembled persons that they were being subjected to CCTV, drone, body-camera and facial recognition surveillance, the databases against which their biometric data would be matched, or the retention and use of that data, and a substantial part of the surveillance was carried out covertly. The covert and undisclosed character of the impugned surveillance defeats any claim of notice or consent, aggravates its chilling

effect upon the exercise of the freedoms guaranteed by Article 19, and demonstrates that the impugned measures fall below even the minimal safeguards that the law attaches to ordinary CCTV, in violation of Articles 19 and 21 of the Constitution.

G. BECAUSE the impugned surveillance violates every established principle of data protection recognised by the Justice B.N. Srikrishna Committee (2018), and embodied in the Digital Personal Data Protection Act, 2023 enacted in its wake. The principles are namely, (i) collection limitation, that personal data may be collected only to the extent necessary; (ii) purpose limitation, that data may be used only for the specific purpose for which it was collected; (iii) data minimisation, that only data adequate and relevant to that purpose may be processed; (iv) storage limitation, that data must be destroyed once that purpose is served; and (v) accountability, that collection must be attended by security, oversight and redress. The impugned surveillance offends every one of them. A measure that violates every data-protection principle the State itself professes cannot survive the scrutiny of Articles 14 and 21 of the Constitution.

H. BECAUSE the real-time processing of the protesters' faces through facial recognition technology violates Articles 14 and 21 of the Constitution for being arbitrary and disproportionate. The identity, source and legal basis of the database being used to compare has not been disclosed. The Delhi Police has admitted, by its reply dated 25.07.2022, that a similarity score of 80%

and above is treated as a “positive” match. That threshold is arbitrary and scientifically unvalidated. It can generate false positives at scale. International research shows that the error rates of facial recognition are unevenly distributed across demographic groups. [*See, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, U.S. National Institute of Standards and Technology*] Thus, the impugned actions convert mere attendance at a peaceful protest into exposure to wrongful suspicion and investigation.

- I. BECAUSE the data so collected is retained without any disclosed or lawful retention regime, which is a continuing and disproportionate intrusion into the right to privacy and violates Article 21. The Respondents have not disclosed any retention period, purpose limitation or destruction schedule governing the footage, facial templates, probe images or match results of the protesters. On the contrary, a senior officer of the Delhi Police is reported to have stated that no data-retention guidelines are being followed during the protests, and that the footage may remain on police systems indefinitely. (**See, Annexure P-8**). In the absence of any retention limit, the data remains liable to be stored and searched against future databases without end. This offends the principles of purpose and storage limitation recognised in *Puttaswamy I* [Pg. 257-258, Para 184-185]. Excessive and open-ended retention of personal data was held to be disproportionate in *Puttaswamy II* [Pg. 332, Para 205].

- J.** BECAUSE the data so collected is liable to be shared and used without any limit, in breach of the right to privacy under Article 21. No restriction has been disclosed on the dissemination, transfer or further use of the footage so recorded. The principle of Purpose Limitation, that data collected for one purpose may not be used for another, has been recognised by *Puttaswamy I* [Pg. 257-258, Para 184-185] and *Puttaswamy II* [Pg. 332, Para 204-D]. For instance, the “Ikshana” system was designed and is maintained by a private vendor, M/s CP PLUS (Aditya Infotech Limited), whose software is integrated for live monitoring of the surveillance. No data-handling agreement governing this arrangement has been disclosed. There is thus a real risk that the sensitive biometric data of protesters is accessible to a private entity.
- K.** BECAUSE the surveillance has been used as an instrument of intimidation and coercion, in violation of Articles 19 and 21 of the Constitution. Police officers have also recorded the protesters on their personal mobile phones. Such recording is outside any official system, control or accountability. The footage so taken is subject to no record, safeguard or retention protocol whatsoever. Protesters have further been threatened that their photographs and videos would be transmitted to their families and educational institutions. This uncontrolled and coercive use of surveillance turns the assembly into an occasion for intimidation. It thereby violates the rights to

freedom of speech and expression and to peaceful assembly, and the right to privacy.

L. BECAUSE the impugned surveillance is wholly bereft of the procedural safeguards that the Constitution requires. In the event of erroneous collection, abuse, or breach of the data, no mechanism for redress, compensation or accountability has been provided. The Digital Personal Data Protection Act, 2023 affords no protection either. It grants wide exemptions to State agencies for law-enforcement purposes, so that the requisite safeguards must be found within the enabling framework itself. Here, there is none. The absence of such safeguards renders the impugned surveillance arbitrary and disproportionate, in violation of Articles 14 and 21 of the Constitution.

M. BECAUSE the impugned surveillance fails the necessity prong of proportionality and falls foul of Article 21. The stated aim of maintaining law and order and preventing infiltration by persons with criminal antecedents can be achieved by far less restrictive means. Substantial physical police presence was deployed at the site, along with a range of conventional security measures. These included barricading, access control and checking, deployment of the Rapid Action Force, and conventional video monitoring short of facial recognition. Any apprehended offence could be prevented by such means. None of this requires the real-time biometric identification of every peaceful protester. Before imposing any

such restriction, the State was bound to “triangulate” the measure by considering its “*appropriateness, necessity and the least restrictive measure before being imposed*”: ***Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 [Para 72]**. There is nothing to suggest that Delhi Police undertook privacy impact assessment was conducted before deployment. The Respondents are put to strict proof for it. In fact, the untargeted biometric surveillance was the most intrusive measure available in place of the least restrictive. The impugned surveillance is therefore neither necessary nor proportionate.

N. BECAUSE, without prejudice, the Hon’ble Supreme Court has held surveillance to be permissible in very narrow limits. The impugned surveillance transgresses every one of them. Surveillance may be directed only at habitual or potential offenders, upon recorded grounds of individualised suspicion, exercised discreetly, and subject to safeguards against abuse: ***Malak Singh v. State of Punjab & Haryana*, (1981) 1 SCC 420**. The impugned surveillance is directed at every person present, and not at any identified offender. It proceeds upon no recorded ground of suspicion. It is subject to no independent review, safeguard or accountability. What five decades of precedent permitted only as a narrow exception has thus been made the default condition of attending a peaceful assembly, in violation of Articles 19 and 21 of the Constitution.

- O.** BECAUSE the Petitioner States that this Hon'ble Court has jurisdiction to entertain this petition.
- P.** That the Petitioner crave leads to add, amend, or alter any of the foregoing grounds with the permission of this Hon'ble Court.
1. That the annexures filed along with the present Public Interest Petition (PIL) are true copies of the originals.
 2. This Public Interest Litigation is made bona fide and in the interest of justice.

MAINTAINABILITY

3. That this Hon'ble Court has jurisdiction under Article 32 of the Constitution of India to enforce Fundamental Rights guaranteed under Part III, particularly Articles 14, 19 and 21, of the Constitution. The ongoing and systematic deployment of facial recognition technology and allied biometric surveillance by State authorities in the absence of any valid statutory framework or constitutionally adequate safeguards. The challenge concerns a continuing practice of indiscriminate collection, processing, retention and use of the biometric data of persons participating in peaceful public assemblies, thereby affecting a large and indeterminate class of citizens who are unable, by reason of their number and the diffuse nature of the injury, to individually approach this Hon'ble Court. The issues raised transcend any individual grievance and involve questions of substantial public and constitutional importance concerning the limits of

State surveillance, informational privacy, freedom of speech and expression, and the right to peaceful assembly. In view of the nationwide implications of the issue and absence of an efficacious alternative remedy, the Petitioner has invoked the extraordinary jurisdiction of this Hon'ble Court under Article 32 of the Constitution.

CAUSE OF ACTION

4. The cause of action for filing the present Public Interest Litigation first arose on or about 20 June 2026, when the Delhi Police commenced indiscriminate biometric surveillance of persons participating in the peaceful public assembly at Jantar Mantar, New Delhi, by deploying facial recognition technology, AI-enabled smart spectacles, CCTV cameras, drones, body-worn cameras and mobile fingerprint identification systems. The cause of action further arose when the biometric information, facial templates and personal data of thousands of participants were captured, processed and matched against undisclosed databases without the authority of any enacted law, without notice to the affected persons and without any publicly disclosed safeguards governing their collection, retention, processing or dissemination.
5. The cause of action is continuous and recurring. It continues to subsist each day that the Respondents retain, process, analyse, store, share or otherwise utilise the footage, facial templates, probe images, biometric data, similarity or match results and other personal information collected

through the impugned surveillance architecture, and each day that the Respondents continue to deploy or threaten to deploy such facial recognition and biometric surveillance technologies against persons exercising their fundamental right to peacefully assemble. The continuing retention and processing of such sensitive personal data constitutes a continuing infringement of the rights guaranteed under Articles 14, 19 and 21 of the Constitution.

6. The cause of action has further arisen from the Respondents' failure to disclose the legal authority, databases, operating protocols, retention policies, data-sharing arrangements and safeguards governing the impugned surveillance measures, despite public admissions regarding the deployment of facial recognition technology and biometric identification systems at the protest site. As the impugned actions disclose an ongoing pattern of unconstitutional State surveillance affecting an indeterminate class of citizens and giving rise to a continuing violation of fundamental rights, the cause of action is subsisting and continues to confer jurisdiction upon this Hon'ble Court under Article 32 of the Constitution of India.
7. That the Petitioner has no other alternative efficacious remedy except to file the present Public Interest Litigation under Article 32 of the Constitution of India seeking redress of its grievances.

8. That the Petitioner has not filed any other PIL or any other such petition seeking the identical relief before any other High Court or before this Hon'ble Court of India.
9. That no Civil, Criminal or revenue is pending against the Petitioner which could have a legal nexus with the issues involved in the Public Interest Litigation. Further, the Petitioner did not approach any statutory authority with respect to the underlying concerns of the present Petition.
10. The petitioner states that the requisite court fee as per the Rules has been paid.
11. The petitioner states that there is no period of limitation for preferring this petition, and hence, the same is within limitation.
12. The petitioner states that this Hon'ble Court has jurisdiction to entertain this petition.
13. The petitioner states that the petitioner has no other efficacious remedy than to prefer the instant Writ Petition U/A 32 of the Constitution of India. The petitioner has not filed any other petition for similar relief before any High Court or this Hon'ble Court

PRAYER

Therefore, on the facts and in the circumstances of the case, it is humbly submitted that this Hon'ble Court may graciously be pleased to:

- A. DECLARE** that the deployment by the Delhi Police of facial recognition technology and allied mass surveillance measures, and the capture,

extraction, processing, storage, matching and retention of the biometric data of persons participating in peaceful public assemblies, carried on indiscriminately and without the sanction of any law is violative of Articles 14, 19 and 21 of the Constitution;

- B.** DECLARE that the capture, extraction, storage or processing of the biometric data of persons attending a peaceful assembly by a private entity, whether on its own account or on behalf of the State, in the absence of a valid enabling law and of a disclosed data-processing agreement embodying purpose limitation, retention limits and security safeguards, is illegal and violative of Articles 14 and 21 of the Constitution of India;
- C.** ISSUE a writ, order or direction directing the Respondents to make publicly available: (a) Details of technologies and device deployed, including facial recognition technologies such as “AjnaLens” and “Ikshana” vehicle, and their respective capabilities and the specific circumstances and purposes for which they are used; (b) the database(s) against which the biometric data of the persons was matched, and their source, contents and legal basis; (c) The similarity/match threshold applied, and the action taken upon a purported match; (d) The standard operating procedures, guidelines and instructions, which were being followed, if any, governing the collection, processing, retention, sharing, destruction and oversight of the data so gathered; (e) The contracts and arrangements with any private vendor in respect of the said

systems, and the nature and extent of any access by such vendor or any third party to the data;

- D.** ISSUE a writ, order or direction directing Respondent Nos. 4 and 5 (the private vendors), and any parent, subsidiary, affiliate, sub-contractor or cloud-service provider acting for or on their behalf, to disclose on affidavit: (a) the facial-recognition, biometric and allied systems supplied, deployed, integrated or operated by them in connection with the assembly at Jantar Mantar, and their technical capabilities; (b) the contracts, work orders, licences and data-sharing or data-processing agreements governing their engagement with Respondent Nos. 1 to 3; and (c) the nature, extent and location (including any cloud or off-site storage) of any footage, images, facial templates, probe images, biometric data, similarity/match results or personal particulars of the persons present at the assembly that is or has been in their possession, custody, control or access;
- E.** Issue a writ, order or direction in the nature of mandamus directing the Respondents to forthwith cease and desist from deploying facial recognition technology, automated facial recognition technology and allied biometric-surveillance measures against persons participating in peaceful public assemblies, until a legislation authorising the same is validly enacted;
- F.** In the alternative to prayer (E), issue a writ, order or direction directing the Respondents to commission a data protection impact assessment prior to every deployment of facial recognition technology;

G. Issue a writ, order or direction in the nature of mandamus directing

Respondent No. 3 (the National Crime Records Bureau):

(a) to disclose, on affidavit, the legal basis, purpose, matching protocol and data-flow governing the “Abhigyan” mobile fingerprint-identification application, including the criteria on which the fingerprints of persons present at the assembly were captured and run against the National Automated Fingerprint Identification System (NAFIS);

(b) to forthwith cease and desist from capturing, matching, enrolling, storing or retaining, whether through the “Abhigyan” application or otherwise, the fingerprints, facial templates or other biometric data of persons present at the assembly who are not connected with the investigation of any cognisable offence, into NAFIS, the Crime and Criminal Tracking Network & Systems (CCTNS), or any other database, register or watch-list; and

(c) to identify, expunge and permanently delete from NAFIS, CCTNS and every allied database maintained or operated by it, and to certify such destruction on affidavit, all fingerprints, facial templates, probe data, similarity/match results and personal particulars of the persons present at the assembly, save such limited data as this Hon'ble Court may specifically direct to be preserved for the present proceedings;

H. ISSUE a writ, order or direction against the Respondent Nos. 1-3 directing that the footage, photographs, facial templates, probe images, biometric data, similarity/match results and personal particulars collected or generated

through the surveillance at the assembly at Jantar Mantar (June–July 2026) shall not be used, processed, retained or shared for any purpose whatsoever, save such limited data as is strictly necessary for the investigation and prosecution of a specific cognisable offence and as this Hon'ble Court may permit;

I. ISSUE a writ, order or direction in the nature of mandamus directing Respondent Nos. 1 to 3 to establish, and to make publicly known within a time-bound period to be fixed by this Hon'ble Court, a transparent and readily accessible mechanism whereby any person present at the assembly at Jantar Mantar, or their authorised representative, may, upon request:

(a) ascertain and access whether their photographs, footage, facial images, facial templates, biometric data, similarity/match results or personal particulars have been collected, generated, retained, matched or shared through the impugned surveillance, and obtain the particulars thereof, including the similarity/match score, if any, on the basis of which they were identified or enrolled in any database; and

(b) apply for the correction, blocking and permanent deletion/erasure of such data;

J. and further directing the said Respondents to constitute and notify a grievance redressal mechanism, headed by a designated nodal officer, to receive, consider and dispose of such requests for access and deletion in a

time-bound manner and by a reasoned order, with a right of appeal to an independent authority;

- K.** ISSUE a writ, order or direction directing the Respondent Nos. 1-3 not to use the data collected at the assembly to build, populate or train any database, register or watch-list, including by enrolling the facial images or facial templates of persons not connected with the investigation of any cognisable offence into any facial-recognition or criminal database, or by creating any list or record of persons by reference to their participation in the protest;
- L.** ISSUE a writ, order or direction directing Respondent Nos. 4 and 5 to forthwith preserve, and restraining them from deleting, altering, transferring, disseminating, monetising or otherwise using or processing, any footage, images, facial templates, probe images, biometric data or match results of the persons present at the assembly, pending the final adjudication of the present petition;
- M.** Issue a writ, order or direction directing Respondent Nos. 4 and 5 to permanently delete, and to certify on affidavit the destruction of, all footage, images, facial templates, probe images, biometric data, similarity/match results and personal particulars of the persons present at the assembly held on their systems, servers, devices or cloud storage, save such limited data as this Hon'ble Court may specifically direct to be preserved for the present proceedings;

- N. Issue a writ, order or direction restraining Respondent Nos. 4 and 5 from using, replicating or utilising any data, image or biometric template captured at the assembly to train, develop, improve, benchmark or validate any facial-recognition, biometric or artificial-intelligence product, algorithm or model;
- O. Pass such other or further order(s) as this Hon'ble Court may deem fit and proper in the facts and circumstances of the case and in the interest of justice.

AND FOR THIS ACT OF KINDNESS THE PETITIONER AS IS IN DUTY BOUND SHALL REMAIN EVER GRATEFUL.

PETITIONER

THROUGH

DRAWN BY:
MR. SUBHASH CHANDRAN K.R.,
MR. RIBHAV PANDE,
MR. MADHAV AGGARWAL
MS. ANUKA BACHAWAT
MR. ANIRUDH K.P.

Filed by:

SUBHASH CHANDRAN K.R
ADVOCATE FOR THE PETITIONER

Place: New Delhi
Drawn on: 27.07.2026
Filed On: 28.07.2026