



AI-POWERED SURVEILLANCE AND THE RIGHT TO PRIVACY: IS INDIAN CONSTITUTIONAL LAW PREPARED FOR ALGORITHMIC STATE SURVEILLANCE?

Khushboo Chaudhary

Advocate, Delhi High Court & Supreme Court of India

B.A. LL.B., LL.M. (Criminal Law), India

ABSTRACT

The Indian State now observes its population through facial recognition networks linked to city-wide camera grids, biometric records gathered under the Criminal Procedure (Identification) Act, 2022, and spyware capable of taking control of a mobile device. This paper asks whether the constitutional framework settled in Justice K.S. Puttaswamy (Retd.) v. Union of India, and developed by the courts between 2020 and 2025, is equipped to discipline surveillance of this kind. It analyses the proportionality standard, the Telecommunications Act, 2023 and the Digital Personal Data Protection Act, 2023, and compares the Indian position with the European Union's Artificial Intelligence Act and the English and Strasbourg jurisprudence. It argues that Indian doctrine is, in principle, adequate to the task, but that the statutory and institutional machinery needed to give those principles effect is largely missing, so that most algorithmic surveillance in India operates without the legal foundation Puttaswamy treats as the first condition of legitimacy.

Keywords: algorithmic surveillance; facial recognition technology; right to privacy; proportionality; Digital Personal Data Protection Act, 2023; Telecommunications Act, 2023.

INTRODUCTION

When the police in Hyderabad stopped a social worker on his way home in May 2021, and photographed him after he declined to remove his mask, the encounter lasted only a few minutes, but the legal questions it raised have still not been answered. His legal notice to the Commissioner of Police received no reply, and the public interest petition he then filed before the High Court for the State of Telangana, became the first judicial challenge in India directed at the deployment of facial recognition technology as such.¹ The episode is a useful point of entry because a single street-level interaction displays the features that distinguish algorithmic surveillance from its older forms: the capture of biometric data from a person who is not

¹S.Q. Masood v. State of Telangana, Public Interest Litigation, High Court for the State of Telangana (notice issued on January 3, 2022); Internet Freedom Foundation, "Telangana High Court issues notice in India's first legal challenge to the deployment of Facial Recognition Technology" (January 3, 2022), available at: <https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/> (last visited on September 12, 2026).



suspected of any offence, the absence of any statute authorising the practice, and the practical impossibility for the affected person of discovering what was later done with the data.

Indian privacy law did not begin with technology. The nine-judge Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* restated that tradition in 2017 by recognising privacy as a fundamental right grounded in Articles 14, 19 and 21, and by requiring that every intrusion satisfy the tests of legality, legitimate aim and proportionality.² What *Puttaswamy* could not settle, because the facts before the Court did not require it, was how these tests would apply to systems that observe everyone in order to find someone, that produce inferences rather than simply recording facts, and whose internal logic may not be intelligible.

This paper addresses that unsettled question: whether Indian constitutional law, as it stands in 2026, is prepared for algorithmic State surveillance. Preparedness has two senses. The doctrinal asks whether the standards courts apply to privacy intrusions can reach the particular harms of automated monitoring; the institutional asks whether the statutes, rules and oversight bodies through which those standards operate actually exist and function as the Constitution requires. Drawing on decisions between 2020 and 2025, on legislation notified up to 2026, and on comparative material from the European Union, the United Kingdom and the United States, it argues that Indian doctrine is broadly adequate, but that the absence of any legislative framework for facial recognition, the breadth of the State's exemptions under the data protection law, and continued reliance on executive self-review leave those tools with little to operate upon.

WHAT MAKES ALGORITHMIC SURVEILLANCE DIFFERENT

The expression "algorithmic surveillance" describes monitoring in which the collection, analysis or use of personal data is carried out wholly or substantially by automated systems. Facial recognition is the most visible example, but the category also includes automated number plate recognition, predictive policing, social media monitoring and the analysis of communications metadata. Four characteristics separate these systems from conventional surveillance, each with consequences for the constitutional analysis that follows.

The first characteristic is scale. A police officer can follow one person at a time, whereas a camera network linked to a face-matching server can, in principle, compare every face passing through a railway concourse against a watchlist in real time. On the most recent estimates compiled by Comparitech, Hyderabad and Indore have more public CCTV cameras per thousand residents than any other city outside China, and Bengaluru follows closely behind

²*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295; *Gobind v. State of M.P.*, (1975) 2 SCC 148.

them.³ Camera density is not in itself evidence that facial recognition is being used, but it provides the infrastructure on which facial recognition and video analytics are layered.

Table 1: Public CCTV camera density in selected Indian and foreign cities (2025 estimates)

City	Estimated public CCTV cameras	Population used for estimate	Cameras per 1,000 people
Hyderabad (India)	900,000	11,337,900	79.38
Indore (India)	251,500	3,482,830	72.21
Bengaluru (India)	585,284	14,395,400	40.66
Moscow (Russia)	250,000	12,737,400	19.63
Singapore	112,999	6,157,270	18.35
London (UK)	Over 130,000	Not stated	13.40
Los Angeles (USA)	46,766	Not stated	12.40
New York City (USA)	80,303	Approx. 7.9 million	10.12
Delhi (India)	313,332	34,665,600	9.04
Mumbai (India)	82,390	22,089,000	3.73

Source: Rebecca Moody, "Surveillance camera statistics: which are the most surveilled cities?", Comparitech (updated June 25, 2025), available at: <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/>. Comparitech notes that figures are compiled from government reports, police websites and news reports, that the lower estimate is used where sources differ, and that some private cameras may be included for certain cities.

The second characteristic is inference. Older methods of surveillance recorded what a person said or where he went, while algorithmic systems draw conclusions from that material,

³Rebecca Moody, "Surveillance camera statistics: which are the most surveilled cities?", *Comparitech* (updated June 25, 2025), available at: <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/> (last visited on September 12, 2026).



predicting that a face belongs to an individual, that a locality is a likely crime site, or that call patterns indicate group membership. Information obtained by the Internet Freedom Foundation disclosed that the Delhi Police treated facial recognition results above 80 per cent similarity as positive matches.⁴

The third characteristic is opacity. A person subjected to algorithmic surveillance seldom knows that it has taken place, and even where he does, the reasoning of the system may be unavailable to him because it is proprietary, technically complex, or withheld on grounds of security. Frank Pasquale's account of a society in which consequential decisions are made by systems whose operation is hidden from those whom they affect has particular force when the decision-maker is the police.⁵

The fourth characteristic is the uneven distribution of harm. Because algorithmic systems learn from historical records and are deployed where the State already concentrates its policing, their errors and intrusions tend to fall most heavily upon communities already heavily policed. An empirical study published by the Vidhi Centre for Legal Policy mapped police station jurisdictions and the distribution of cameras in Delhi, and concluded that the use of facial recognition by the police there was likely to affect Muslims disproportionately.⁶ This dimension carries the constitutional question beyond Article 21 and into the guarantees of equality and non-discrimination under Articles 14 and 15.

THE CONSTITUTIONAL STANDARD AFTER PUTTASWAMY

The three-fold test and its procedural supplement

In *Puttaswamy*, the plurality opinion of Chandrachud J. held that an invasion of privacy must be justified by a law which prescribes a fair, just and reasonable procedure, must pursue a legitimate aim of the State, and must be proportionate to the object it seeks to achieve. Kaul J. formulated the test in comparable terms and added that there must be procedural guarantees against the abuse of State power. Scholars writing shortly after the judgment observed that this

⁴Internet Freedom Foundation, "Delhi Police's claims that FRT is accurate with a 80% match are 100% scary" (August 17, 2022), available at: <https://www.internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/> (last visited on September 12, 2026).

⁵Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge, MA, 2015).

⁶Jai Vipra, *The Use of Facial Recognition Technology for Policing in Delhi: An Empirical Study of Potential Religion-Based Discrimination* (Vidhi Centre for Legal Policy, New Delhi, 2021), available at: <https://vidhilegalpolicy.in/research/the-use-of-facial-recognition-technology-for-policing-in-delhi/> (last visited on September 12, 2026).



framework, if applied with seriousness, would call into question much of the existing surveillance regime.⁷

Proportionality in *Anuradha Bhasin* and its limits

The first major application of the *Puttaswamy* standard to restrictions in the digital sphere came in *Anuradha Bhasin v. Union of India*, where a three-judge Bench examined the suspension of internet services in Jammu and Kashmir after August 2019.⁸ The Court held that restrictions on the use of the internet must satisfy the test of proportionality, that orders suspending services must be published so that they can be challenged, and that suspension for an indefinite period was not permissible. In *Foundation for Media Professionals v. Union Territory of Jammu and Kashmir* the Court again avoided a determination of the merits and constituted a special committee, headed by the Union Home Secretary, to examine the matter.⁹ The pattern of these decisions is instructive, because the Court accepted proportionality as the governing standard and insisted upon transparency of orders, but entrusted the practical application of that standard to bodies within the executive.

A more exacting form of proportionality review appears in *Association for Democratic Reforms v. Union of India*, in which a Constitution Bench struck down the Electoral Bond Scheme in February 2024.¹⁰ The Court recognised that informational privacy extends to a citizen's political affiliation, and it required the State to show that the measure it had adopted was the least restrictive of the means reasonably available. The judgment was not concerned with surveillance technology, but its treatment of political affiliation as a protected category of information bears directly on systems that identify participants in demonstrations or map associations through the analysis of social media.

Continuous monitoring as a distinct harm: *Frank Vitus*

The Supreme Court's decision in *Frank Vitus v. Narcotics Control Bureau* adds a further element to the doctrine.¹¹ The Court held that a bail condition cannot be used to keep constant watch over an accused person's movements, and that permitting the investigating agency to peep continuously into the private life of a person released on bail would violate the right to privacy guaranteed by Article 21. The Court treated continuous location monitoring as a qualitatively different intrusion from an obligation to report periodically to a police station.

⁷Vrinda Bhandari and Karan Lahiri, "The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World" 3(2) *University of Oxford Human Rights Hub Journal* 15 (2020).

⁸*Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

⁹*Foundation for Media Professionals v. Union Territory of Jammu and Kashmir*, (2020) 5 SCC 746.

¹⁰*Association for Democratic Reforms (Electoral Bond Scheme) v. Union of India*, (2024) 5 SCC 1 : 2024 INSC 113.

¹¹*Frank Vitus v. Narcotics Control Bureau*, 2024 INSC 479 : 2024 LiveLaw (SC) 441 (Criminal Appeal arising out of SLP (Crl.) Nos. 6339-6340 of 2023, decided on July 8, 2024).



Surveillance directed at the State: *Paramvir Singh Saini*

One further decision complicates any account in which surveillance technology is regarded simply as a threat to liberty. In *Paramvir Singh Saini v. Baljit Singh*, the Supreme Court directed that CCTV cameras be installed in every police station, and that the recorded footage be preserved for a prescribed period.¹² The case demonstrates that the constitutional objection is not to cameras or data as such, but to their deployment without purpose limitation, legal authority and accountability.

THE STATUTORY ARCHITECTURE

Interception under the Telecommunications Act, 2023

The legal basis for the interception of communications now lies in section 20(2) of the Telecommunications Act, 2023, which replaced section 5(2) of the Indian Telegraph Act, 1885 while retaining its essential structure. Interception is permitted on the occurrence of a public emergency or in the interest of public safety, where the competent authority is satisfied that it is necessary or expedient on grounds of security, public order and the integrity of the State. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, notified on 6 December 2024, supersede Rules 419 and 419A of the Indian Telegraph Rules, 1951.¹³

The rules thus reproduce the model of executive self-review that the Supreme Court approved in *People's Union for Civil Liberties v. Union of India* as an arrangement pending legislation. They make no provision for prior judicial authorisation, impose no obligation to notify the person whose communications were intercepted once secrecy is no longer needed, and establish no independent body to adjudicate complaints. Nor do they contemplate the automated analysis of intercepted material at scale, which is precisely what can convert interception from a targeted measure into an instrument of generalised monitoring.

The judgment of the Madras High Court in *P. Kishore v. Secretary to Government, Ministry of Home Affairs*, delivered on 2 July 2025, illustrates both the force of the statutory limits and the fragility of their safeguards.¹⁴ N. Anand Venkatesh J. held that public emergency and public safety are not secretive conditions but situations that would be apparent to a reasonable person, and that a covert operation undertaken to detect the commission of an offence fell outside section 5(2) of the Telegraph Act as that provision had been interpreted in *People's Union for*

¹²*Paramvir Singh Saini v. Baljit Singh*, (2021) 1 SCC 184.

¹³The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, notified by the Department of Telecommunications on December 6, 2024 under s. 20 of the Telecommunications Act, 2023 (44 of 2023); *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

¹⁴*P. Kishore v. Secretary to Government, Ministry of Home Affairs*, 2025:MHC:1510 (Madras High Court, decided on July 2, 2025).



Civil Liberties. The Court also found that the review mandated by Rule 419A had not been carried out. The interception order was quashed, and the Court directed that the intercepted material should not be used for any purpose, while leaving the prosecution free to rely on evidence gathered independently of it.

The Information Technology Act, 2000

Section 69 of the Information Technology Act, 2000 empowers the Union and State Governments to direct the interception, monitoring or decryption of any information in a computer resource, on grounds that include the investigation of any offence, far wider than section 20(2) of the Telecommunications Act. Section 69 was drafted with the interception of specific communications in view; it does not address remote access tools that compromise the device itself rather than the communication passing through a network, and offers no guidance on whether, and under what conditions, the State may deploy spyware of the kind at the centre of the Pegasus litigation.

Data protection and the State

The Digital Personal Data Protection Act, 2023 was widely expected to supply the missing framework for the processing of personal data by the State, but in its enacted form it does considerably less than that expectation suggested. Section 17(2)(a) empowers the Central Government to exempt, by notification, any instrumentality of the State from the provisions of the Act in the interests of the sovereignty and integrity of India, the security of the State. Section 17(1)(c) separately excludes processing in the interest of the prevention, detection, investigation or prosecution of any offence from most of the obligations owed to data principals. The Digital Personal Data Protection Rules, 2025 bring the scheme into force in stages.¹⁵

The combined effect of these provisions is that the law enforcement and intelligence uses most likely to involve algorithmic surveillance fall largely outside the statute. The provision that speaks most directly to algorithmic risk, namely the obligation under Rule 13 on significant data fiduciaries to observe due diligence to verify that algorithmic software deployed by them is not likely to pose a risk to the rights of data principals, can be displaced for any State instrumentality by a single notification under section 17(2). The constitutional validity of sections 17(1)(c), 17(2), 33(1), 36 and 44(3) of the Act, and of Rules 17 and 23(2), is now under challenge before the Supreme Court in *Venkatesh Nayak v. Union of India*, in which notice was issued on 16 February 2026 without any interim stay, and the Court indicated that the questions raised required consideration by a larger Bench.¹⁶

¹⁵The Digital Personal Data Protection Act, 2023 (22 of 2023), ss. 17(1)(c), 17(2)(a) and 36; the Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), notified on November 13, 2025, rr. 1, 13 and 23 and Seventh Schedule.

¹⁶*Venkatesh Nayak v. Union of India*, W.P. (C) No. 177 of 2026 (Supreme Court of India, notice issued on February 16, 2026); Fox Mandal, "SC Hears Petitions Challenging DPDP Act Provisions Diluting the RTI" (August 2026),

Biometric collection and the absence of a facial recognition law

The Criminal Procedure (Identification) Act, 2022 authorises police and prison officers to take "measurements" including photographs, iris and retina scans, biological samples and behavioural attributes from convicted and arrested persons, and requires the National Crime Records Bureau to preserve them for seventy-five years. The Act enlarges the pool of biometric data available for automated matching, but says nothing about its use in facial recognition, about matching against images gathered from the public, or about accuracy thresholds and the correction of errors. There is, in short, no statute in India that authorises or regulates police use of facial recognition, and the systems in Table 2 rest on executive decisions, procurement tenders and project documents rather than legislation.

Table 2: Selected indicators of facial recognition and algorithmic surveillance in India

Indicator	Reported figure	Source
Facial recognition systems tracked across India by Project Panoptic	170	Biometric Update (June 17, 2024), citing IFF Panoptic Tracker
Systems reported as operational (including in Telangana, Delhi and Maharashtra)	20	Same
Share of systems at tender, procurement or implementation stage	More than 85%	Same
Reported public expenditure on FRT systems	About Rs. 1,513 crore (Union: Rs. 770 crore; States: Rs. 743 crore)	Same
Similarity score treated by Delhi Police as a positive FRT match	Above 80%	IFF, RTI analysis (August 17, 2022)
Tamil Nadu Police FRT portal data leak (May 2024)	About 8 lakh data points; about 50,000 accused or suspected persons	IFF, Project Panoptic updates

available at: <https://foxmandal.in/News/supreme-court-hearing-dpdp-act-challenges-to-rti/> (last visited on September 12, 2026).

Indicator	Reported figure	Source
FRT-enabled CCTV cameras proposed in Indian Railways coaches by tender	3.3 lakh	IFF, Project Panoptic updates
Devices examined by the Supreme Court-appointed Pegasus technical committee	29 (malware found in 5; Pegasus not established)	The Tribune (April 29, 2025)

The policy documents that exist confirm the gap rather than fill it. The discussion paper on facial recognition published by NITI Aayog in November 2022 examined the risks of the technology, but it did not propose a legislative framework for policing uses.¹⁷ The India AI Governance Guidelines of 5 November 2025 deliberately adopted a light regulatory approach, preferring to rely on existing statutes such as the Information Technology Act and the Digital Personal Data Protection Act instead of enacting a dedicated law on artificial intelligence.¹⁸ Yet it leaves the use of artificial intelligence for State surveillance to be governed by statutes which, as the preceding discussion shows, either exempt the State or were never designed with automated analysis in mind.

THE COURTS AND ALGORITHMIC SURVEILLANCE, 2020-2025

The Pegasus proceedings

The most direct encounter between the Indian judiciary and technologically advanced State surveillance occurred in the Pegasus litigation. In *Manohar Lal Sharma v. Union of India*, a Bench presided over by N.V. Ramana C.J. responded to reports that the telephones of journalists, politicians and activists had been targeted with spyware by appointing an independent technical committee.¹⁹ The order of 27 October 2021 is remembered chiefly for the Court's statement that the State cannot obtain a free pass every time the spectre of national security is raised, and for its refusal to accept a limited affidavit from the Union that neither admitted nor denied the use of the software. The Court also recognised that surveillance, and

¹⁷NITI Aayog, *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology* (Discussion Paper, November 2022), available at: https://niti.gov.in/sites/default/files/2024-09/Ai_for_All_2022_02112022_0.pdf (last visited on September 12, 2026).

¹⁸Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines* (November 2025), available at: <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf> (last visited on September 12, 2026).

¹⁹*Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985 (W.P. (Crl.) No. 314 of 2021, decided on October 27, 2021).



the awareness that one may be under surveillance, affects the manner in which individuals exercise their rights, and it treated the resulting chilling effect on the press as a constitutional injury in its own right.

The later course of the proceedings has been less encouraging. In August 2022, the Court recorded that malware had been found in five of the twenty-nine devices examined and that the Union had not cooperated with the inquiry. When the matter was heard on 29 April 2025, a Bench of Surya Kant and N. Kotiswar Singh JJ. observed that there was nothing wrong in a country possessing spyware, that the real question was against whom it was used, and that the technical report would not be disclosed to the extent that it touched upon the security and sovereignty of the country, although individuals who wished to know whether they were affected could be informed.²⁰ Read together, the orders reveal a gap between the Court's doctrinal statements and its remedial practice.

Pandemic data and the problem of function creep

The COVID-19 pandemic produced two decisions that anticipated many of the issues now raised by algorithmic surveillance. In *Balu Gopalakrishnan v. State of Kerala*, the Kerala High Court examined a contract under which the State Government shared the health data of COVID-19 patients and persons in quarantine with Sprinklr Inc..²¹ By its interim order of 24 April 2020, a Division Bench of Devan Ramachandran and T.R. Ravi JJ. directed that the data be anonymised before being made available to the firm, that citizens be informed and their specific consent obtained for access by third parties, and that the firm be restrained from using the data for any other purpose.

In *Anivar A. Aravind v. Ministry of Home Affairs*, the Karnataka High Court considered the Aarogya Setu contact-tracing application, which had been downloaded by well over a hundred million users.²² By its order of 25 January 2021, a Division Bench of Abhay S. Oka C.J. and S. Vishwajith Shetty J. held, *prima facie*, that informed consent had not been obtained for the sharing of users' response data under the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, and restrained the Union and the National Informatics Centre from sharing such data without consent, while declining to halt the use of the application itself.

²⁰"Won't disclose report that touches country's security, sovereignty: SC on Pegasus row", *The Tribune* (April 29, 2025), available at: <https://www.tribuneindia.com/news/india/pegasus-row-nothing-wrong-in-using-spyware-against-adverse-elements-says-sc/> (last visited on September 12, 2026); "Pegasus row: Supreme Court to hear pleas for probe on April 22", *Deccan Herald* (April 2025), available at: <https://www.deccanherald.com/india/pegasus-row-supreme-court-to-hear-pleas-for-probe-on-april-22-3437266> (last visited on September 12, 2026).

²¹*Balu Gopalakrishnan v. State of Kerala*, W.P. (C) No. 9498 of 2020 (Kerala High Court, interim order dated April 24, 2020).

²²*Anivar A. Aravind v. Ministry of Home Affairs*, W.P. No. 7483 of 2020 (GM-RES-PIL) (Karnataka High Court, order dated January 25, 2021).



Facial recognition before the High Courts

The Masood petition in Telangana raises the legality question in its sharpest form, because the State's use of facial recognition there rests on no statute. On the public record the petition has not been finally decided. Its resolution will test whether a High Court will hold that the legality limb of *Puttaswamy* cannot be satisfied by executive instructions, procurement documents or general policing powers a conclusion for which there are strong reasons, since *Puttaswamy* demanded a law, and the insistence in *Anuradha Bhasin* that restrictive orders be published presupposes that the source and extent of the State's authority can be identified and examined by a court.

COMPARATIVE PERSPECTIVES

The European Union and the Strasbourg jurisprudence

The European Union has chosen to address algorithmic surveillance through a combination of ex ante regulation and rights-based adjudication. Regulation (EU) 2024/1689, the Artificial Intelligence Act, prohibits real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement, subject to narrowly defined exceptions: the targeted search for specific victims of abduction, trafficking or sexual exploitation and for missing persons, the prevention of a specific and imminent threat to life or of a genuine and foreseeable terrorist attack, and the localisation or identification of persons suspected of serious offences listed in the Regulation.²³ Each use under these exceptions requires prior authorisation by a judicial authority or by an independent administrative authority.

Alongside legislation, the European Court of Human Rights has begun to articulate the limits imposed by Article 8 of the Convention. In *Glukhin v. Russia*, decided on 4 July 2023, the Court held that Russia had violated Articles 8 and 10 when the Moscow police used facial recognition to identify and arrest a man who had staged a peaceful solo demonstration on the metro.²⁴ The Court described facial recognition technology as highly intrusive, emphasised that its use to identify and arrest peaceful protesters was capable of producing a chilling effect on the freedoms of expression and assembly, and held that detailed rules governing the scope and application of such measures, together with strong safeguards against abuse, were essential. In *Big Brother Watch v. United Kingdom*, the Grand Chamber had earlier accepted that bulk

²³Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, arts. 5(1)(h), 5(2), 5(3), 26(10), 113 and Annex III.

²⁴*Glukhin v. Russia*, App. No. 11519/20 (ECtHR, July 4, 2023).

interception is not in itself incompatible with the Convention, but insisted on "end-to-end safeguards", including authorisation, supervision and independent review.²⁵

The United Kingdom

The decision of the Court of Appeal in *R (Bridges) v. Chief Constable of South Wales Police*, delivered on 11 August 2020, remains the leading authority on police use of live facial recognition.²⁶ The Court held that the deployment of the AFR Locate system was unlawful because the governing framework left too broad a discretion to individual officers as to who could be placed on a watchlist and where the system could be deployed, with the result that the interference with Article 8 rights was not in accordance with the law. The Court further held that the data protection impact assessment was deficient, and that the police force had failed to discharge the public sector equality duty because it had not taken reasonable steps to establish whether the software was biased on grounds of race or sex. *Bridges* is instructive for India because it shows a court applying the legality requirement rigorously, and because it treated the risk of algorithmic bias as an enforceable legal duty.

Five years after *Bridges*, the British Government itself has acknowledged that the framework remains inadequate. On 4 December 2025, the Home Office opened a consultation on a new legal framework for the use of biometrics, facial recognition and similar technologies by law enforcement, which closed on 12 February 2026.²⁷ The consultation proposes a statutory scheme, and the accompanying material describes the existing arrangements for oversight as fragmented across several regulators. The British experience is significant for India because it demonstrates that a jurisdiction with a mature data protection regime, a surveillance camera code and a leading judicial authority on the subject eventually concluded that primary legislation was indispensable.

The United States

The United States offers a different model, in which protection depends on the Fourth Amendment, State legislation and municipal ordinances. Federal courts have nevertheless begun to extend the reasoning of *Carpenter v. United States*²⁸, which held in 2018 that acquiring historical cell-site location data is a search requiring a warrant, to other forms of persistent location surveillance. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the

²⁵*Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 and 24960/15 (ECtHR [GC], May 25, 2021).

²⁶*R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.

²⁷Home Office (United Kingdom), *Consultation on a New Legal Framework for Law Enforcement Use of Biometrics, Facial Recognition and Similar Technologies* (December 4, 2025), available at: <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement/consultation-on-a-new-legal-framework-for-law-enforcement-use-of-biometrics-facial-recognition-and-similar-technologies-accessible> (last visited on September 12, 2026).

²⁸*Carpenter v United States*, 138 S Ct 2206 (2018).



en banc Court of Appeals for the Fourth Circuit held in 2021 that a programme of persistent aerial photography, involved a search for which a warrant was required.²⁹ The reasoning closely resembles the concern expressed by the Supreme Court of India in *Frank Vitus* about continuous tracking. Beyond the Fourth Amendment, however, the protection is strikingly uneven, for there is no comprehensive federal privacy statute and the regulation of biometric surveillance has been left largely to individual States and cities. Illinois' Biometric Information Privacy Act of 2008 requires informed consent before biometric identifiers may be collected, and several municipalities, beginning with San Francisco in 2019, have barred public authorities from using facial recognition altogether. The result is a fragmented settlement in which the intensity of protection depends heavily on where a person happens to live.

Australia

Australia illustrates how far privacy protection can be carried by statute in the absence of a constitutional guarantee. The Constitution contains no express right to privacy, and the High Court has not implied one; protection therefore rests on the Privacy Act 1988 (Cth) and the Australian Privacy Principles. The limits of that model were tested in *Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy)*³⁰, where the Privacy Commissioner found that a retailer's use of facial recognition across sixty-two stores had collected the sensitive biometric information of every entering customer without consent. Commissioner Kind reasoned that the deployment was the most intrusive option available and interfered disproportionately with the privacy of ordinary shoppers rather than the small number of individuals suspected of wrongdoing a proportionality analysis close to the one *Puttaswamy* demands, but conducted by a regulator under statute rather than a court under a bill of rights. That the Administrative Review Tribunal in 2026 subsequently narrowed the finding on one principle³¹ underlines the fragility of protection that turns on statutory exceptions. The lesson for India is that a data-protection statute can carry genuine proportionality review, yet remains exposed where a constitutional anchor is absent.

New Zealand

New Zealand's response has been shaped less by litigation than by institutional self-restraint. The New Zealand Bill of Rights Act 1990 contains no free-standing privacy right; section 21 protects against unreasonable search and seizure, and informational privacy is governed largely by the Privacy Act 2020. The catalyst for reform was the disclosure that the Police had secretly trialled Clearview AI in 2020 without a privacy impact assessment or external authorisation. Rather than await a court, the Police commissioned an independent review by Dr Nessa Lynch and Dr Andrew Chen, published in 2021³², which made ten recommendations and warned that

²⁹*Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc); *Carpenter v. United States*, 585 U.S. 296 (2018).

³⁰ *Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy)* [2024] AICmr 230.

³¹ *Bunnings Group Limited and Privacy Commissioner* (Administrative Review Tribunal, 4 February 2026).

³² Independent review of the New Zealand Police's use of facial recognition technology, conducted by Nessa Lynch and Andrew Chen (2021).

there was very limited current evidence for the efficacy and cost-benefit of live automated facial recognition in policing. The reviewers also observed that error rates were likely to fall disproportionately on Māori and Pasifika faces, echoing the bias concern that *Bridges* had treated as an enforceable duty. The Police accepted all ten recommendations and, in 2024, adopted a formal policy restricting live facial recognition. The weakness of the model is that oversight remains internal, since the Police audit themselves. New Zealand thus shows both the value and the limits of self-regulation as a substitute for statutory or constitutional control.

Canada

Canada is perhaps the closest comparator to India, because it too protects privacy through a justiciable constitutional guarantee. Section 8 of the Canadian Charter of Rights and Freedoms secures the right against unreasonable search and seizure, which the Supreme Court has read as protecting a reasonable expectation of privacy, including informational privacy. The doctrine has proved capable of extension to new technologies. In *R v Spencer*³³ the Court held that subscriber information linked to an internet address attracts such an expectation, and in *R v Bykovets*³⁴ a narrow majority went further, holding that an IP address itself does so because of its potential to unlock a user's online activity and identity. What matters for India is the mode of reasoning: the majority assessed the privacy interest normatively, by reference to what the technology could reveal, rather than by the sparse information that a bare number discloses on its face. That approach mirrors the concern with continuous tracking expressed in *Frank Vitus*. Canada also demonstrates the reach of regulators, for the federal and provincial privacy commissioners jointly found in 2021 that Clearview AI's mass collection of facial images amounted to unlawful surveillance³⁵, reinforcing that a constitutional anchor and a strong regulator can operate together.

IS INDIAN CONSTITUTIONAL LAW PREPARED?

Doctrinal readiness

On the doctrinal side, the answer is more positive than is sometimes assumed. The *Puttaswamy* framework already contains the elements European courts have used to scrutinise facial recognition: a requirement of law, a legitimate aim, a proportionality test that includes the least restrictive means, and procedural safeguards against abuse. Taken together, these authorities support the conclusion that live facial recognition in public places, deployed without a statute, fails the legality requirement outright, and that even a statute authorising it would have to justify indiscriminate biometric capture as the least restrictive means of achieving a clearly specified and pressing aim.

³³ *R v Spencer*, 2014 SCC 43.

³⁴ *R v Bykovets*, 2024 SCC 6.

³⁵ Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada and provincial privacy commissioners (2021).

Academic writing has arrived at a similar assessment. Gautam Bhatia's reading of the early surveillance cases emphasised, several years before *Puttaswamy*, that Indian privacy doctrine had been built around the requirements of a compelling State interest and narrow tailoring, while more recent scholarship on AI-driven surveillance in India argues that the Telecommunications Act and the Information Technology Act are ill-suited to predictive policing and facial recognition, and recommends a risk-based framework informed by the European experience.³⁶ The doctrinal resources, in other words, are not the principal difficulty.

Institutional deficits

The deficits are institutional, and of four kinds. The first is the legality gap. Most facial recognition and video analytics projects in India, including those in Table 2, have no statutory foundation. Until a court applies the legality limb of *Puttaswamy* to them, the constitutional standard remains an unused instrument, and the executive has little reason to seek legislative authority for what it already does without it. The Telangana petition may provide the occasion, but its slow progress shows the cost of relying on litigation in a field where technology is installed faster than cases can be heard.

The second deficit is the absence of independent authorisation and oversight. Interception under both the Telecommunications Act and the Information Technology Act continues to rest on executive orders reviewed by committees of senior civil servants, and *P. Kishore* shows that even this internal review may not in fact take place. International standards, reflected in *Big Brother Watch* and in the report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, treat prior independent authorisation as a central safeguard.³⁷ India has no equivalent safeguard, and the practice adopted in *Anuradha Bhasin* and *Foundation for Media Professionals* of remitting questions of proportionality to executive committees has reinforced this pattern rather than corrected it.

The third deficit is the breadth of the State's exemption under the data protection law. Sections 17(1)(c) and 17(2) of the Digital Personal Data Protection Act, with Rule 23, place the most intrusive uses of personal data by the State outside the statute meant to give practical effect to *Puttaswamy*. A law that exempts the police and intelligence agencies wholesale cannot supply the procedural guarantees against abuse that Kaul J. regarded as indispensable, and *Venkatesh Nayak* will require the Supreme Court to decide whether an exemption conferred by executive notification, without any statutory standard of necessity or proportionality, can be reconciled with Article 21.

³⁶Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" 26(2) *National Law School of India Review* 127 (2014); Manu Mariyan Abraham and Shampa Dev, "AI-driven surveillance in India: Reconciling privacy, national security and legal oversight" 8(2) *Journal of Data Protection & Privacy* 183 (2025).

³⁷Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/48/31 (September 13, 2021).



The fourth deficit concerns knowledge. Algorithmic surveillance is largely invisible to those it affects. The Indian framework contains no requirement of notice after surveillance has ended, no obligation to disclose the use of facial recognition in an investigation, and no mechanism by which a person may learn that he has been placed on a watchlist. The Supreme Court's willingness in April 2025 to inform individuals whether their devices had been compromised acknowledged the problem, but depended on judicial discretion rather than any legal entitlement. Without knowledge, the right to challenge surveillance the premise of every remedy discussed here becomes largely illusory.

Constitutional interpretation and algorithmic justice

How a court reads a constitution drafted before a technology existed is not a technical preliminary; it decides whether an old guarantee can reach a new harm at all. Two methods compete. An originalist approach fixes meaning by the understanding that prevailed when the text was adopted, while a living or evolutive approach reads the same words in the light of present conditions. *Carpenter v. United States* shows both at work on the same facts: the majority extended the Fourth Amendment to cell-site location data by treating the reasonable expectation of privacy as responsive to the capacities of modern devices, whereas Gorsuch J. reached for a property-based, historically grounded route to a comparable result.³⁸ Indian law has largely settled this question in favour of the evolutive approach. The Court in *Puttaswamy* described itself as having progressively adopted a living constitutionalist reading, and in *NALSA* it treated the Constitution as a living organism.³⁹ The practical consequence is that Article 21 can be applied to facial recognition and predictive policing without waiting for a constitutional amendment. That method decides only that the guarantee reaches the technology; it does not, by itself, supply the standards of legality and proportionality that the earlier sections have examined.

A privacy-centred analysis tends to obscure a second dimension. Algorithmic systems do not fail uniformly, and the empirical material discussed earlier indicates that the burden of misidentification falls disproportionately on those already disadvantaged. Indian constitutional law now possesses the instrument to address this. In *Lt. Col. Nitisha v. Union of India* the Supreme Court formally recognised indirect discrimination under Articles 14 and 15(1), holding that facially neutral criteria which produce a disproportionate disadvantage for a protected group are constitutionally suspect.⁴⁰ A facial recognition deployment that is neutral in design but generates systematically higher error rates against a religious or caste group falls squarely within that principle. Comparative practice points the same way: the European Union's Artificial Intelligence Act treats remote biometric identification as a source of particular risk to fundamental rights and acknowledges that technical inaccuracies can produce discriminatory effects on grounds such as ethnicity, sex, or disability, while the Court of Appeal in *Bridges*

³⁸ *Carpenter v. United States*, 585 U.S. 296 (2018) (Gorsuch, J., dissenting).

³⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *National Legal Services Authority v. Union of India*, (2014) 5 SCC 438.

⁴⁰ *Lt. Col. Nitisha v. Union of India*, 2021 SCC OnLine SC 261.

treated the failure to test for bias as a breach of the public sector equality duty.⁴¹ It follows that a proportionality inquiry confined to privacy is incomplete. Where the State deploys an algorithmic system, Articles 14 and 15 should require it to demonstrate that the system does not distribute its errors along prohibited lines, and any unexplained disparity should weigh against the State when its proportionality is assessed. Read in this way, equality ceases to be a background value and becomes an operative constraint on algorithmic governance, ensuring that those least able to contest surveillance are not left most exposed to its failures.

RECOMMENDATIONS

The analysis points toward a set of reforms, each following from principles the Supreme Court has already accepted. Parliament should enact a law governing biometric and algorithmic surveillance by law enforcement and intelligence agencies. It should specify the purposes for which facial recognition may be used, prohibit live identification in public spaces or confine it to narrowly defined serious offences and imminent threats, and require prior judicial authorisation for any use matching images of the general public. It should also prescribe minimum accuracy standards, require independent testing for demographic bias, set retention limits for watchlists and captured images, and require that the use of facial recognition in an investigation be disclosed to the accused.

Interception and intrusion into devices should be brought within a single statute providing for prior judicial authorisation, subject to a strictly time-limited emergency procedure followed by judicial confirmation. Remote access tools and spyware should be addressed expressly, whether by prohibition or through a regime far more demanding than that for ordinary interception. Persons subjected to surveillance should be notified once notice would no longer prejudice the investigation, and an independent oversight body, answerable to Parliament and composed of members with judicial and technical expertise, should publish annual statistics on interception orders and facial recognition searches.

Section 17(2) of the Digital Personal Data Protection Act should be amended so that any exemption granted to an instrumentality of the State is confined to specified provisions, tied to defined purposes and subject to necessity and proportionality, with an independent authority empowered to examine compliance. Finally, the courts should build on *P. Kishore* by treating material obtained through surveillance without legal authority as presumptively inadmissible, giving investigating agencies a concrete reason to respect the statutory limits that already exist.

CONCLUSION

The question posed at the outset was whether Indian constitutional law is prepared for algorithmic State surveillance, and the answer is qualified. The principles articulated in *Puttaswamy*, and refined in *Anuradha Bhasin*, *Manohar Lal Sharma*, *Association for*

⁴¹ Regulation (EU) 2024/1689 (Artificial Intelligence Act), Recital 32; *R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.



Democratic Reforms and *Frank Vitus*, can reach the harms of automated monitoring, and the Kerala, Karnataka and Madras High Courts have applied them to data practices earlier treated as administrative. What India lacks is the legal structure through which those principles would operate in practice. Facial recognition has been deployed without statutory authority, interception rests on executive self-review, and the data protection law lets the State exempt itself from its core obligations. Each feature weakens the capacity of doctrine to shape State conduct, because doctrine is applied through litigation, and litigation depends on knowledge, standing and time that affected persons seldom possess. The pending proceedings in the Telangana High Court and in *Venkatesh Nayak* offer an opportunity to insist that the legality requirement be taken literally, but a durable solution lies with Parliament, which alone can supply the statute, independent oversight and rights of notice and redress the Constitution already demands. Until then, India's preparedness will remain a matter of constitutional doctrine rather than of law in operation.