
UNDER THE ALGORITHMIC EYE: EVALUATING AI-DRIVEN SURVEILLANCE AND THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Amardeep, PhD Research Scholar, Rajiv Gandhi National University of Law, Patiala

Dr. Geetika Walia, Associate Professor of Law, Rajiv Gandhi National University of Law, Patiala

ABSTRACT

The Digital Personal Data Protection Act, 2023 is commonly presented as the statute that gives effect to the right to informational privacy recognised in *Justice K.S. Puttaswamy v. Union of India*. This article tests that presentation against a practice the Act is poorly equipped to govern, namely the use of artificial intelligence by police and administrative agencies to identify and track individuals in public space. The Act is built for consent based collection by private fiduciaries. Algorithmic surveillance does not work that way. Data is captured without any act of provision by the individual, and the injury it produces is an injury of inference. Section 17(2) (a), which permits the Central Government to exempt any instrumentality of the State from the whole of the Act by a simple notification, then turns that gap into a permission. Reading the exemption power together with Sections 7 and 36 of the Act, Rule 23 of the Digital Personal Data Protection Rules, 2025, and the amendment of Section 8(1)(j) of the Right to Information Act, 2005, the article argues that the framework fails the legality limb of the proportionality standard well before any question of necessity or balancing is reached. A reform agenda follows, drawing on the European Union's Artificial Intelligence Act and on *R (Bridges) v. Chief Constable of South Wales Police*.

Keywords: informational privacy; facial recognition; Digital Personal Data Protection Act, 2023; proportionality; algorithmic accountability; state surveillance.

I. INTRODUCTION

In July 2026 the Delhi Police trained facial recognition cameras on demonstrators at Jantar Mantar. Within a fortnight two petitions had been filed, one before the Delhi High Court by a former student union president and the other before the Supreme Court by a Member of the Rajya Sabha. Neither turned on the accuracy of the software. Both asked who had authorised its use, and both arrived at the same answer, which is that no statute names the power and no authority reviews its exercise.¹ The Delhi High Court declined to decide the matter on merits and observed that the petitioner should first examine the existing statutory framework.² The difficulty with that observation, and it is the difficulty this article takes up, is that the framework in question is the very thing the petitioners say does not exist.

Since 2023 the Union Government has maintained that the Digital Personal Data Protection Act, 2023 completes India's constitutional commitment to informational privacy.³ There is something to the claim. The Act was passed in the shadow of a nine judge Bench decision placing privacy within Article 21, and it arrived after five years of drafting, redrafting and one outright withdrawal.⁴ The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, full compliance falls due on 13 May 2027, and the Data Protection Board has been constituted.⁵ India now has an operative regime.

My argument is that the Act does not answer the surveillance question at all, and that its silence has a structural source. Begin with the model of processing the statute assumes. An identifiable

¹ Writ petition filed by Aishe Ghosh before the Delhi High Court on July 15, 2026, seeking a declaration that the mass biometric surveillance of student protesters at Jantar Mantar is unconstitutional and directions for the destruction of the data collected; and public interest litigation filed by A.A. Rahim, Member of Parliament, before the Supreme Court in July 2026, challenging the use of facial recognition and biometric surveillance by the Delhi Police at the same protest site. Case numbers were not in the public domain at the time of writing. See *CPI(M) MP Moves Supreme Court Against Use of Facial Recognition Tech by Police at Jantar Mantar Protest Site*, BAR & BENCH (July 28, 2026), <https://www.barandbench.com/news/litigation/cpim-mp-movessupreme-court-against-use-of-facial-recognition-tech-by-police-at-jantar-mantar-protest-site>.

² The Division Bench made an oral observation that the petitioner should examine the existing statutory framework and consider whether a fresh petition was required; the matter was directed to be listed on August 25, 2026.

³ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act], <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

⁴ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India). The legislative sequence ran from the Personal Data Protection Bill, 2019, through its withdrawal in August 2022, to the Digital Personal Data Protection Bill, 2022 and the enacted statute of 2023.

⁵ Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology on Nov. 13, 2025 (India) [hereinafter DPDP Rules]. Rules 1, 2 and 17 to 21, dealing with the constitution and functioning of the Data Protection Board, came into force immediately; Rules 3, 5 to 16, 22 and 23 come into force on May 13, 2027. See Press Information Bureau, DPDP Rules, 2025 Notified (Nov. 17, 2025), <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>.

individual furnishes information to a fiduciary for a stated purpose, and the obligations attach to that transaction. A facial template extracted from a live camera feed is not furnished. It is generated, and the person walking past the lens performs no act at all. There is a second difficulty. The injury in these cases is an injury of inference. What is objectionable about a match at a protest site is not that an image was captured but the conclusion the State proceeded to draw about association, belief and movement, and what it did next. On inference, profiling and automated decision making the Act says nothing, which sets it apart from the instrument on which it is otherwise loosely modelled.⁶ The third difficulty largely subsumes the first two. Section 17(2) (a) permits the Central Government to place any instrumentality of the State outside the whole statute by notification, so that even those protections the Act does contain remain defeasible at the option of the actor they were meant to restrain.⁷

This is a narrower claim than the familiar complaint that the Act is a weak piece of legislation. On algorithmic state surveillance the Act does more than leave a gap. Section 36, read with Rule 23 of the 2025 Rules, allows the Central Government to requisition information from any data fiduciary and to forbid disclosure of the requisition. That combination opens a route into private databases which had no earlier equivalent.⁸ Part II sets out what is currently deployed and shows that no Indian statute authorises suspicionless biometric identification in public space. Part III applies the legality limb of *Puttaswamy*. Parts IV and V take up the Act and the Rules and then compare the European, British and American responses to the same problem. Part VI turns to the pending litigation, and Part VII to reform.

II. DEPLOYMENT WITHOUT AUTHORISATION

A. The Operational Record

The Delhi Police has operated an Automated Facial Recognition System since 2018. Responses to applications under the Right to Information Act, 2005, obtained by the Internet Freedom Foundation, disclosed that the force treats a similarity score above eighty per cent as a positive

⁶ Compare Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, art. 22, 2016 O.J. (L 119) 1 [hereinafter GDPR] (right not to be subject to a decision based solely on automated processing), with DPDP Act, ch. III (containing no equivalent provision).

⁷ DPDP Act, § 17(2)(a).

⁸ DPDP Act, § 36; DPDP Rules, r. 23 and sch. VII.

match.⁹ Why the figure is eighty has never been explained. In practical terms it amounts to an acceptance of a twenty per cent margin of error at the moment an officer is told that the person being scanned appears in a criminal database. The same disclosures suggest that scores below the threshold, which the force classifies as false positives, are not always discarded. They are pursued where what the police describe as corroborative material is available.¹⁰ A person whom the system fails to match may therefore stay under investigation on the strength of the failed match. It is worth recalling that in 2018 the same force had informed the Delhi High Court that the system it had procured had an accuracy rate of roughly two per cent and was not good enough for the purpose.¹¹

Delhi is not exceptional. Telangana hosts the largest concentration of facial recognition projects in the country. Hyderabad, which ranks among the most heavily surveilled cities anywhere, has more than three lakh seventy thousand closed circuit cameras, and its Command and Control Centre has been reported as capable of processing feeds from as many as six hundred thousand cameras at once.¹² Amnesty International and ARTICLE 19 recorded officers stopping members of the public, directing them to remove face coverings and photographing them without consent, and called for a prohibition on the use of the technology for mass surveillance.¹³ Their documentation emphasised something that doctrinal analysis tends to lose. Misidentification and pretextual stops do not fall evenly across a population. They fall on Muslims, Dalits, Adivasis and transgender persons.¹⁴

B. Is There an Authorising Law?

Where, then, is the authority to be found? Three statutes are sometimes offered, and none of

⁹ *Delhi Police's Claims That FRT Is Accurate at 80% Are 100% Scary*, INTERNET FREEDOM FOUND. (Aug. 2022), <https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/>. The disclosures were obtained through applications under the Right to Information Act, No. 22 of 2005, Acts of Parliament, 2005 (India).

¹⁰ *Id.* Matches falling below the eighty per cent threshold are classified as false positives but are, on the Foundation's account, pursued where corroborative material is available.

¹¹ The submission was made by the Delhi Police in proceedings before the Delhi High Court in 2018 concerning the tracing of missing children, in which the force stated that the accuracy of the procured system was approximately two per cent. See INTERNET FREEDOM FOUND., *supra* note 9.

¹² Amnesty Int'l, *India: Hyderabad "On the Brink of Becoming a Total Surveillance City"* (Nov. 11, 2021), <https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/>.

¹³ *Id.*; see also ARTICLE 19, *India: Hyderabad "On the Brink of Becoming a Total Surveillance City"* (Nov. 2021), <https://www.article19.org/resources/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/>. The campaign was conducted under the banner "Ban the Scan."

¹⁴ Amnesty Int'l, *supra* note 12; *Hyderabad Becoming "Surveillance City," Use of Facial Recognition Must Stop: Amnesty*, THE NEWS MINUTE (Nov. 11, 2021), <https://www.thenewsminute.com/article/hyderabad-becoming-surveillance-city-use-facialrecognition-must-stop-amnesty-157449>.

them will bear the weight. The Criminal Procedure (Identification) Act, 2022 replaced the Identification of Prisoners Act, 1920 and considerably widened the class of measurements that may be taken, extending it to iris and retina scans, biological samples and behavioural attributes, with a retention period of seventy five years.¹⁵ The scheme is custodial in design. Measurements are taken by a police or prison officer from persons convicted, arrested or detained in defined circumstances, which presupposes an individual already identified and already inside the criminal process. Nothing in the Act addresses the capture of biometric data from members of the public who are neither arrested nor accused, and it does not contemplate a general population database against which crowds might be matched in real time.

Section 69 of the Information Technology Act, 2000 and Section 5(2) of the Indian Telegraph Act, 1885 deal with the interception of communications. What they regulate is the content and metadata of a transmission. They say nothing about the face of a person standing in a public square. The safeguards built around the second of them are worth pausing on for a different reason. In *People's Union for Civil Liberties v. Union of India* the Supreme Court held that telephone tapping engaged Article 21 and, finding no statutory procedural protection in place, laid down binding guidelines governing who could authorise interception, for how long, on what record and subject to what review.¹⁶ Those guidelines were afterwards codified as Rule 419A of the Indian Telegraph Rules, 1951. India accordingly has a worked example of a court imposing procedure on a surveillance technology ahead of Parliament. The example has not been extended to biometrics, and so far as I can see no petitioner has yet asked in terms for a *PUCL* style direction in this field.

The upshot is that the most intrusive identification technology in operational use by Indian police forces rests on no identifiable statutory foundation. It is bought under general executive powers and run under departmental standing orders. No external body audits it. The July 2026 petitions put the point squarely, contending that neither the Delhi Police standing orders on public assemblies nor the Act of 2022 authorises what was done at Jantar Mantar, and asking for a restraint until Parliament passes a law that does.¹⁷

¹⁵ The Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India), §§ 2(1)(b), 3, 4(2). The Act repealed the Identification of Prisoners Act, 1920.

¹⁶ *People's Union for Civil Liberties v. Union of India*, (1997) 1 S.C.C. 301 (India). The guidelines were subsequently given statutory form as Rule 419A of the Indian Telegraph Rules, 1951.

¹⁷ See *supra* note 1. The petitioners contend that neither the Delhi Police standing orders governing public protests nor the Criminal Procedure (Identification) Act, 2022 authorises the deployment, and seek a restraint on the use of such technologies until Parliament enacts a law regulating them.

III. THE CONSTITUTIONAL BASELINE

In *Justice K.S. Puttaswamy (Retd.) v. Union of India* a nine judge Bench held unanimously that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and of the freedoms guaranteed by Part III, and recognised informational privacy as a facet of that right.¹⁸ Kaul J.'s concurrence anticipated the present problem with some precision. He warned that the aggregation of otherwise innocuous data enables profiling, and that the knowledge of being watched alters behaviour in ways that erode the conditions for dissent.¹⁹

The Court also settled the standard of review. A restriction on privacy must satisfy legality, meaning the existence of a law; legitimate aim; and proportionality, understood as a rational connection between means and object together with the absence of a less intrusive alternative. Chandrachud J. added the requirement of procedural guarantees against abuse.²⁰ In the Aadhaar judgment the Court applied the same test in a four part formulation, though the majority and the dissent parted company sharply over whether the necessity limb had been independently satisfied.²¹ *Anuradha Bhasin v. Union of India* then applied proportionality to internet suspension orders and directed that such orders be published and subjected to periodic review, treating the availability of procedure as part of what proportionality itself demands.²²

Applied to algorithmic surveillance the analysis stops at the first limb. Legality is not satisfied by a general executive power to procure equipment, by an internal standing order, or by a line in a budget. It calls for a law that authorises the intrusion, marks out its scope and identifies the officer competent to sanction it. For facial recognition in India there is no such law. The deployments described in Part II are on that footing constitutionally infirm however effective they may be and however compelling the security interest advanced in their support. Whether the DPDP Act, enacted to give content to the *Puttaswamy* right, supplies the missing law is the

¹⁸ *Puttaswamy*, (2017) 10 S.C.C. 1 (per Chandrachud, J., for the plurality; Nariman, Bobde, Chelameswar, Kaul and Sapre, JJ. concurring separately).

¹⁹ *Id.* (Kaul, J., concurring).

²⁰ *Id.* (Chandrachud, J.) (identifying legality, need and proportionality, and adding the requirement of procedural guarantees against abuse).

²¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India) (the Aadhaar judgment). On the divergence between the majority and the dissent in the application of the necessity limb, see *The Aadhaar Judgment and the Constitution II: On Proportionality*, INDIAN CONST. L. & PHIL. (Sept. 30, 2018) (guest post), <https://indconlawphil.wordpress.com/2018/09/30/theaadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/>.

²² *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).

question for the remainder of this article. In my view it does not, and Part IV sets out why.

IV. THE DPDP ACT AND THE ALGORITHMIC STATE

A. The Scope of Section 17(2)(a)

Section 17(2)(a) empowers the Central Government to notify any instrumentality of the State as exempt from the provisions of the Act on grounds relating to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, the maintenance of public order, or preventing incitement to any cognizable offence relating to those matters.²³ What makes the provision remarkable is less the breadth of the grounds, which track Article 19(2) and are familiar enough, than the manner and the extent of the relief conferred. The exemption operates on the whole of the Act. A notified agency is relieved of the consent requirement, but equally of purpose limitation, of storage limitation, of the security and breach notification duties, and of the jurisdiction of the Board. It is conferred by notification, which requires no prior sanction from Parliament and attracts no subsequent scrutiny there. Nothing in the section imposes a time limit, a review requirement or an assessment of necessity.

The contrast with the draft that preceded it is worth setting out. The Committee of Experts chaired by Justice B.N. Srikrishna proposed in 2018 that exemptions for national security be permitted only where authorised by law and where the processing was necessary and proportionate to the interest pursued.²⁴ Justice Srikrishna later described the enacted framework in unusually direct terms, warning that a provision allowing the executive to place its own agencies outside the statute at its discretion risked producing an Orwellian State.²⁵ The doctrinal objection can be put more precisely than that. Section 17(2)(a) fails the third and fourth limbs of the proportionality standard, because it makes no attempt at a least intrusive design and contains no procedural safeguard of the sort the Supreme Court itself read into telephone tapping in *PUCL*.²⁶ Whether the provision is for that reason unconstitutional is a

²³ DPDP Act, § 17(2)(a).

²⁴ Comm. of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

²⁵ The observation was made in public commentary following the introduction of the 2023 Bill, in which Justice Srikrishna criticised the breadth of the executive exemption power and its capacity to permit access to personal data on grounds of sovereignty or public order.

²⁶ *PUCL*, (1997) 1 S.C.C. 301. For a sustained argument to this effect, see State Exemptions Under the Digital Personal Data Protection Act, 2023: Testing Section 17(2)(a) Against the Proportionality Standard, INDIAN J.L. & LEGAL RSCH., <https://www.ijlrr.com/post/state-exemptions-under-the-digital-personal-data-protection-act-2023-testing-section-17-2-a-again>.

question now before a larger Bench, and Part VI returns to it.

B. Consent Displaced

Even where no notification under Section 17 has issued, the State enjoys considerable latitude within the Act itself. Section 7 sets out a closed list of legitimate uses for which personal data may be processed without consent. Clause (b) covers processing by the State for the provision of any subsidy, benefit, service, certificate, licence or permit, where the individual has previously consented for a comparable purpose or the data is already held in a State register.²⁷ Clause (c) permits processing for the performance of any function under law, or in the interest of the sovereignty and integrity of India or the security of the State, and clause (h) permits it during a disaster or a breakdown of public order.²⁸

Read together these clauses allow a policing or administrative agency to dispense with consent for very nearly every processing activity it is likely to undertake. Clause (c) is the most consequential of them, since "performance of any function under law" is capacious enough to accommodate an argument that general policing powers will do. The Second Schedule to the 2025 Rules prescribes standards for State processing, but standards laid down in subordinate legislation and enforced by a regulator appointed by the same executive are a thin substitute for a statutory authorisation requirement.²⁹ Let me be clear about what is and is not being claimed here. Consent was never going to be a workable governance device for state surveillance, since nobody meaningfully consents to being scanned in a crowd. My objection is to what has taken its place, or rather to the fact that nothing has. Authorisation and independent oversight are the mechanisms that ought to occupy the ground consent cannot, and the Act does not supply them.

C. Section 36 and Rule 23

Section 36 empowers the Central Government to require any data fiduciary, intermediary or the Board itself to furnish such information as it may call for.³⁰ Rule 23 operationalises the power. It permits requisition for the purposes set out in the Seventh Schedule, and permits a

²⁷ DPDP Act, § 7(b).

²⁸ DPDP Act, §§ 7(c), 7(h).

²⁹ DPDP Rules, sch. II (prescribing standards for the processing of personal data by the State and its instrumentalities and for processing under Section 17(2)(b) of the Act).

³⁰ DPDP Act, § 36.

further direction that the entity must not disclose that any requisition has been made, where disclosure would prejudice interests including the sovereignty and security of the State.³¹ The Rule comes into force on 13 May 2027.³²

A compelled disclosure power coupled with a statutory gag matters a good deal for the argument advanced here. Databases assembled by private fiduciaries, among them telecommunications operators, payment processors, platform intermediaries and identity verification services, become available to the State without the individual ever learning that access occurred and without any judicial officer standing between the two. Whatever protective value the Act's obligations carry as against private actors is to that extent contingent, since the same data can be routed onward through a channel the Act itself constructs. It should be said that Section 36 is not on its face a surveillance power, and some provision of the kind is probably necessary for ordinary regulatory supervision. The objection is to its breadth and to the secrecy attaching to it.

D. Section 44(3) and the Right to Information Act

Section 44(3) of the Act amends Section 8(1)(j) of the Right to Information Act, 2005, which had exempted personal information from disclosure unless the Public Information Officer was satisfied that a larger public interest justified it. The amended clause exempts information which relates to personal information, and the public interest override is gone.³³ More than one hundred and twenty Members of Parliament from the Opposition have sought the repeal of the provision, arguing that it disables citizens, journalists and activists from scrutinising the conduct of public officials.³⁴

For present purposes the significance of the amendment is evidentiary. Almost everything publicly known about the operational parameters of facial recognition in India, the eighty per cent threshold included, came out through the Right to Information Act.³⁵ A statute which exempts state agencies from data protection duties while also narrowing the principal route by

³¹ DPDP Rules, r. 23, sch. VII.

³² Press Information Bureau, *supra* note 5.

³³ DPDP Act, § 44(3), amending the Right to Information Act, No. 22 of 2005, Acts of Parliament, 2005 (India), § 8(1)(j).

³⁴ *INDIA Bloc MPs Urge Centre to Roll Back DPDP Act Amendment Diluting RTI Provisions*, OUTLOOK INDIA, <https://www.outlookindia.com/national/india-bloc-mps-urge-centre-to-roll-back-dpdp-act-amendment-diluting-rti-provisions>.

³⁵ *See supra* note 9.

which their practices can be documented leaves a critic with very little to work with. Sections 17, 36 and 44(3) were not drafted as a package, and I do not suggest that they were. Their combined effect is nonetheless considerable.

E. The Regulator

Section 18 establishes the Data Protection Board of India. Section 19 provides that it shall consist of a Chairperson and such number of other Members as the Central Government may notify, appointed by the Central Government in the prescribed manner.³⁶ Appointment follows the recommendation of a search cum selection committee itself constituted by the Central

Government, so that the composition of the regulator is settled by the executive whose agencies it must supervise.³⁷ The Board functions under the administrative aegis of the Ministry of Electronics and Information Technology, and Section 36 permits the Central Government to call for information from the Board itself.³⁸

Two other provisions matter here. Section 29 routes appeals to the Telecom Disputes Settlement and Appellate Tribunal, a body constituted for an unrelated subject matter and without particular expertise in privacy.³⁹ Section 39 bars civil courts from entertaining any suit in respect of matters for which the Board is empowered, and prohibits injunctions against action taken under the Act.⁴⁰ Put together, what emerges is a regulator appointed and supervised by the executive, from which appeal lies to a tribunal outside its field, and around which the ordinary civil remedies have been closed off. That is some distance from the independent supervisory authority which comparative practice treats as the minimum institutional condition of a functioning regime.⁴¹

F. Inference, Profiling and the Limits of the Act

The deficiencies so far described concern the Act's treatment of the State. A further omission

³⁶ DPDP Act, §§ 18, 19.

³⁷ *Data Protection Board of India: A Watchdog Without Teeth*, SOFTWARE FREEDOM L. CTR., <https://sfllc.in/data-protection-boardof-india-a-watchdog-without-teeth/>.

³⁸ DPDP Act, § 36; see also *Is India's Data Protection Board Independent Enough to Protect You?*, LIVELAW, <https://www.livelaw.in/articles/india-data-protection-board-542731>.

³⁹ DPDP Act, § 29 (appeal to the Appellate Tribunal, being the Telecom Disputes Settlement and Appellate Tribunal, within sixty days).

⁴⁰ DPDP Act, § 39.

⁴¹ See GDPR, arts. 51 to 54 (requiring supervisory authorities to act with complete independence and prescribing conditions of appointment and tenure).

is more general. The Act contains no provision on automated decision making or profiling, and therefore no analogue to Article 22 of the General Data Protection Regulation, under which a person has the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significant consequences.⁴² In a jurisdiction where algorithmic systems are already at work in credit scoring, hiring, welfare targeting and policing, the absence of any right to contest an automated determination or to obtain an explanation of it is a substantial gap.⁴³

There is a conceptual point underneath the drafting gap. The Act regulates personal data that a data principal provides, and its duties are triggered by collection. Inference falls outside that frame. A system which converts a face captured on a public camera into a mathematical template, matches the template to a name, and concludes from repeated matches that a person attends particular assemblies has, at the moment of greatest consequence, collected nothing. It has made something. The Act does not address the generation of personal data by observation, and observation at scale is what machine learning has made cheap.

Relief from a dedicated artificial intelligence statute looks unlikely in the near term. The India AI Governance Guidelines released on 5 November 2025 decline to propose a new law and favour what they call a "techno-legal" approach, under which existing statutes are adapted and compliance is embedded in technical design.⁴⁴ For commercial deployment there is a respectable case for that strategy. It does not help here, for the plain reason that the existing statute one would be adapting says nothing on the subject.

V. COMPARATIVE PERSPECTIVES

Three jurisdictions have met the same question within the last decade, and the way each has answered it throws the Indian position into relief. The European Union legislated directly. Article 5 of Regulation (EU) 2024/1689 prohibits real time remote biometric identification in publicly accessible spaces for law enforcement as a default rule. Three narrow exceptions are carved out, covering the targeted search for victims of abduction or trafficking and for missing persons, the prevention of a specific and imminent terrorist threat, and the localisation of a

⁴² GDPR, art. 22.

⁴³ See A Comparative Study on GDPR and the DPDP Act, 6 INT'L J. RSCH. PUBLICATION & REVS. no. 10, <https://ijrpr.com/uploads/V6ISSUE10/IJRPR54121.pdf>.

⁴⁴ Ministry of Elecs. & Info. Tech., Gov't of India, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (Nov. 5, 2025).

suspect in a serious offence carrying a custodial maximum of at least four years.⁴⁵ Each permitted use requires prior authorisation by a judicial or independent administrative authority, a fundamental rights impact assessment, and registration in a European Union database. The prohibitions became applicable on 2 February 2025 and are enforced through the Regulation's highest penalty tier.⁴⁶ Whether or not one endorses the substance, the design repays attention, because the constraint is placed on the state actor at the point of deployment and not on the processor at the point of collection.

The United Kingdom reached a comparable position through litigation. In *R (Bridges) v. Chief Constable of South Wales Police* the Court of Appeal held that live automated facial recognition was not in accordance with law for the purposes of Article 8 of the European Convention on Human Rights, because the framework left individual officers too broad a discretion over whose faces went on a watchlist and where the technology was deployed.⁴⁷ The force had also failed to carry out an adequate data protection impact assessment, and had not discharged the public sector equality duty by satisfying itself that the software did not produce differential error rates by race or sex.⁴⁸ Much of that transfers to the Indian setting. A force operating an identification system with an undisclosed match threshold and no published watchlist criteria would struggle on the first ground alone.

The United States has come at the problem through the Fourth Amendment. In *Carpenter v. United States* the Supreme Court held that acquiring historical cell site location information was a search requiring a warrant, and refused to extend the third party doctrine to data whose reach allowed a person's past movements to be reconstructed.⁴⁹ The reasoning turned on the difference between conventional surveillance and technologies that make comprehensive tracking effortless, which applies to networked facial recognition with at least equal force.

⁴⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 5(1)(h), 2024 O.J. (L 2024/1689) [hereinafter AI Act], <https://artificialintelligenceact.eu/article/5/>.

⁴⁶ *Id.* arts. 5(2) to 5(4), 99(3), 113. Infringement of Article 5 attracts administrative fines of up to thirty five million euro or seven per cent of total worldwide annual turnover, whichever is higher.

⁴⁷ *R (Bridges) v. Chief Constable of South Wales Police* [2020] EWCA (Civ) 1058 (Eng.) (Ground 1), <https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html>. The framework comprised the Data Protection Act 2018, the Surveillance Camera Code of Practice and local force policies.

⁴⁸ *Id.* (Grounds 3 and 5) (holding the data protection impact assessment required by section 64 of the Data Protection Act 2018 deficient because it proceeded on the footing that Article 8 was not infringed, and the public sector equality duty under section 149 of the Equality Act 2010 undischarged). The appeal failed on the separate question of proportionality under Article 8(2) (Ground 2).

⁴⁹ *Carpenter v. United States*, 585 U.S. 296 (2018).

What these three have in common is that the constraint operates before deployment and binds the state agency itself, whether by statutory prohibition with judicial authorisation, by a standard of legality applied on judicial review, or by a warrant requirement. The Indian arrangement runs the other way. Its duties bind fiduciaries, and they can be lifted from agencies by notification. I would not press the comparison further than that. The European Regulation is largely untested in practice, *Bridges* concerned a pilot deployment of modest scale, and *Carpenter* has been read narrowly by a number of lower courts in the United States. The point concerns where the constraint sits.

VI. THE PRESENT LITIGATION

Several of these questions are now before the Supreme Court. On 16 February 2026 the Court issued notice to the Union of India in petitions challenging the constitutionality of the DPDP Act and the 2025 Rules, and referred the core questions to a larger Bench.⁵⁰ The petitions came from The Reporters' Collective and the journalist Nitin Sethi, from the transparency campaigner Venkatesh Nayak, and from the National Campaign for People's Right to Information, and they challenge Section 36 read with Rule 23 as well as the amendment of Section 8(1)(j) of the Right to Information Act.⁵¹ Section 17(2)(a) is said to enable a surveillance regime without safeguard or review, and so to be manifestly arbitrary within Article 14.⁵² Interim relief was declined, and the Act and the Rules remain fully operative.⁵³ At hearings in March 2026 the Court raised the question how public data is to be distinguished from personal data, which bears directly on whether a face observed in a public place attracts statutory protection at all.⁵⁴

The two petitions arising from the Jantar Mantar deployment proceed on a narrower footing but engage the same principle.⁵⁵ These matters are pending and I anticipate no outcome. What can be said is that the questions the Court has chosen to frame are the questions identified

⁵⁰ *Supreme Court Issues Notice on Constitutional Challenge to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025*, INTERNET FREEDOM FOUND. (Feb. 2026), <https://internetfreedom.in/supreme-court-issuesnotice-on-constitutional-challenge-to-the-digital-personal-data-protection-act-2023-and-the-digital-personal-data-protectionrules-2025/>.

⁵¹ *The Reporters Collective Trust v. Union of India*, W.P. (C) No. 211 of 2026 (S.C.) (India); see also *Constitutionality of the Digital Personal Data Protection Act, 2023*, SUP. CT. OBSERVER, <https://www.scobserver.in/cases/constitutionality-of-the-digitalpersonal-data-protection-act-2023/>.

⁵² *Id.*

⁵³ *Supra* note 50.

⁵⁴ *SC Questions "Public vs Private Data" in DPDP Act Case*, MEDIANAMA (Mar. 2026), <https://www.medianama.com/2026/03/223-supreme-court-dpdp-act-challenge/>.

⁵⁵ *Supra* note 1.

above as structural, which is at least some indication that the difficulty lies in how the statute was designed.

VII. A REFORM AGENDA

Six changes seem to me to follow, and I set them out roughly in order of urgency. *First*, Parliament should enact a dedicated statute governing biometric identification by public authorities. It should prohibit real time remote biometric identification in publicly accessible spaces as a general rule, permit narrowly defined exceptions on the model of Article 5 of the European Union Regulation, and require prior authorisation by a judicial officer or independent authority with contemporaneous reasons. For the procedural component the *PUCL* guidelines are a serviceable domestic template.

Second, Section 17(2)(a) should be replaced. Exemptions ought to attach to identified obligations rather than to the whole Act, for a defined period, on a recorded finding of necessity and proportionality, subject to periodic review and to being laid before Parliament.

Third, the Act requires a provision on automated decision making and profiling conferring, at a minimum, a right to be informed that an automated system has been applied, a right to a meaningful explanation of the principal factors, and a right to human review of decisions with legal or similarly significant effects.

Fourth, Section 44(3) should be repealed and the public interest override in Section 8(1)(j) of the Right to Information Act restored, transparency being a precondition of accountability.

Fifth, the independence of the Data Protection Board should be secured through a broad based appointment committee including the Chief Justice of India or a nominee and the Leader of the Opposition, a fixed tenure that is not renewable, financial autonomy, and a duty to publish annual aggregate figures on notifications under Section 17 and requisitions under Section 36.

Sixth, no biometric identification system should be deployed publicly without a published impact assessment covering accuracy, disaggregated error rates, the justification for the match threshold, and the criteria for watchlist inclusion. Redaction for operational sensitivity is legitimate; wholesale withholding is not.

VIII. CONCLUSION

The Digital Personal Data Protection Act, 2023 does much of what it was designed to do. Individuals have rights against the commercial entities holding their data, fiduciaries owe security and breach notification duties, and complaints can be heard somewhere. A good deal of the criticism directed at the Act has been careless about the difference between a statute that is imperfect and one that is misconceived.

The problem discussed here is of the second kind, though only within its own domain. Algorithmic surveillance by the State involves data the individual never handed over, harm consisting in what is inferred, and an actor the statute allows to exempt itself. A consent based framework administered by an executively appointed regulator has little purchase on any of that. It is worth remembering how the eighty per cent threshold reached the public. A civil society organisation filed applications under a transparency statute that the DPDP Act has since narrowed.

The constitutional difficulty comes before all of this. *Puttaswamy* requires a law before it requires proportionality, and for biometric identification in public space there is no law. Until Parliament supplies one there is nothing whose proportionality a court could assess. That is an awkward position for the litigation now pending, since the petitioners must in effect ask the Court to strike down a statute for permitting a practice which no statute authorises. However, the references are decided, the legislative gap will remain to be filled.