
AI SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: CONSTITUTIONAL CHALLENGES AND LEGISLATIVE GAPS

Mayank Uday Kumar, LL.B., Faculty of Law, University of Delhi (Campus Law Centre)

ABSTRACT

The Supreme Court's nine-judge bench decision in **Justice K.S. Puttaswamy (Retd.) v Union of India (2017)** recognised privacy as a fundamental right under Article 21 of the Constitution of India, yet the **Digital Personal Data Protection Act 2023** creates what this article terms a constitutional paradox: it recognises and operationalises informational privacy rights for ordinary data processing while simultaneously exempting, through Section 17, the very state surveillance systems that pose the most significant threat to that same right.¹

Adopting a doctrinal methodology, the article analyses constitutional jurisprudence, the relevant statutory framework, the parliamentary record of the DPDP Act's enactment, and comparative material from the European Union and the United States, to assess the extent to which India's AI surveillance infrastructure satisfies the proportionality standard articulated in Puttaswamy and the equality and due process guarantees under Article 14. Drawing on documented deployments including facial recognition use during the Anti-CAA protests of 2019-2020, at the Kumbh Mela of 2019 and the Maha Kumbh Mela of 2025, through the expanding NATGRID platform, and via the DigiYatra system the article finds that India's principal AI surveillance systems operate without clear statutory authorisation, that Section 17 substantially exempts state surveillance from the DPDP Act's protective obligations, and that documented accuracy disparities in facial recognition technology raise independent concerns under Article 14's guarantees of equality and non-arbitrariness. The article concludes by proposing a dedicated legislative framework, independent oversight, and mandatory impact assessments addressing both privacy and equality concerns.

Keywords: AI Surveillance; Right to Privacy; Puttaswamy; Digital Personal Data Protection Act 2023; Facial Recognition; NATGRID; Article 14; Algorithmic Bias; Proportionality.

¹Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

I. INTRODUCTION, RESEARCH QUESTIONS, AND METHODOLOGY

A. Background

The deployment of artificial intelligence in state surveillance has accelerated considerably in India over the past decade. Facial recognition technology was first documented in a public setting at the **2019 Kumbh Mela in Prayagraj**², and was subsequently used by Delhi Police and Uttar Pradesh Police to identify protesters during the Anti-CAA demonstrations of December 2019. The National Intelligence Grid (NATGRID), conceived after the 2008 Mumbai attacks, became operational in 2023 and has since expanded in both its agency access and its database integrations.³ These developments have occurred alongside, rather than pursuant to, a clear legislative mandate.

The constitutional backdrop to this expansion is the Supreme Court's decision in *Puttaswamy*, which held that privacy is intrinsic to human dignity and is protected under Article 21, read with Articles 14 and 19. The decision did not, and could not, resolve every subsequent question concerning the application of this right to algorithmic and biometric surveillance technologies that have developed in its wake. This article addresses that residual question, with particular attention to a statutory provision Section 17 of the Digital Personal Data Protection Act 2023 whose constitutional compatibility with *Puttaswamy* has not, in the existing literature, been subjected to a sustained, element-by-element audit.

B. Research Questions

This article addresses four research questions: first, whether India's principal AI surveillance systems are compatible with the constitutional standard for restricting the right to privacy established in *Puttaswamy*; second, whether Section 17 of the Digital Personal Data Protection Act 2023, considered specifically against the elements of legality, necessity, proportionality, procedural safeguards, and judicial review, is itself constitutionally compatible with that standard; third, whether documented accuracy disparities and algorithmic opacity in facial recognition technology raise independent concerns under Article 14's guarantees of

²Internet Freedom Foundation, Project Panoptic: Tracking Facial Recognition in India (2021), documenting use of facial recognition technology at the 2019 Kumbh Mela in Prayagraj for crowd management and identification of missing persons.

³Ministry of Home Affairs, National Intelligence Grid (NATGRID): Background Note (Government of India, 2023).

equality, non-arbitrariness, and due process; and fourth, what legislative or institutional reforms would be necessary to address these concerns.

C. Methodology

This article adopts a doctrinal research methodology. It proceeds through the analysis of primary legal sources the Constitution, relevant statutes, parliamentary debates, and judicial decisions supplemented by secondary sources including government committee reports, parliamentary documents, and academic and policy literature on surveillance, data protection, and algorithmic accountability. Particular weight is given, in Part V, to the parliamentary record of the DPDP Bill's passage, since the manner of a statute's enactment is itself relevant evidence of the legislative scrutiny or its absence that a security-related exemption of this kind received. Comparative analysis is employed in respect of the European Union's General Data Protection Regulation and the United States' California Consumer Privacy Act. The article does not undertake independent empirical or quantitative research into the operational accuracy of specific Indian AI systems; where such findings are referenced, they are drawn from published secondary sources, principally the Internet Freedom Foundation's Project Panoptic, and from international demographic accuracy studies including the NIST Face Recognition Vendor Test and the MIT Media Lab's Gender Shades study, applied to the Indian context by inference rather than independent verification.

D. Literature Review

The existing literature on privacy and surveillance in India can be situated along four broad strands. The first is the doctrinal constitutional literature engaging directly with Puttaswamy and its proportionality framework. The second is policy-oriented work produced by government-constituted committees, most significantly the Justice A.P. Shah Committee's 2012 report on privacy principles⁴ and the Justice B.N. Srikrishna Committee's 2018 report.⁵ The third strand consists of civil society and journalistic documentation of specific surveillance deployments, of which the Internet Freedom Foundation's Project Panoptic is the most comprehensive Indian example. A fourth, more recent strand, developing substantially in 2024-

⁴Group of Experts on Privacy (Justice A.P. Shah Committee), Report of the Group of Experts on Privacy (Planning Commission, Government of India, 2012).

⁵Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, 2018).

2026, addresses the constitutional accountability of algorithmic and automated state decision-making specifically under Articles 14 and 21, examining concepts such as 'technological due process' and the constitutional treatment of algorithmic opacity.⁶

Internationally, the OECD's Recommendation on Artificial Intelligence and the UN Human Rights Council's 2021 report on the right to privacy in the digital age provide normative frameworks against which domestic surveillance practices can be assessed. What remains comparatively underdeveloped is, first, a sustained application of the Puttaswamy proportionality test to specific, named AI surveillance systems operating in India, and second, an integration of the Article 21 proportionality analysis with the Article 14 equality and non-arbitrariness analysis within a single framework. This article attempts to address both gaps.

E. Limitations

This article is concerned primarily with state-deployed AI surveillance, although Part III.C examines DigiYatra as an instance of public-private surveillance infrastructure. It does not undertake an extensive independent examination of purely private-sector data processing practices. Nor does it offer an empirical assessment of the comparative accuracy of facial recognition systems specifically deployed in India; the accuracy concerns discussed in Parts III and VII rely on findings reported in existing secondary literature, both Indian and international, rather than on independent technical testing conducted for this article.

II. THE RIGHT TO PRIVACY: CONSTITUTIONAL EVOLUTION

A. The Pre-Puttaswamy Position

For much of its constitutional history, India did not have a settled position on whether privacy was a fundamental right. In *M.P. Sharma v Satish Chandra* (1954), an eight-judge bench held that the Constitution did not recognise a right to privacy comparable to the Fourth Amendment protection in the United States. In *Kharak Singh v State of UP* (1963), a six-judge bench similarly declined to recognise an independent right to privacy, although it held that

⁶'Automated Decision-Making by the State in India: Constitutional Accountability under Articles 14 and 21' (2026) International Journal of Law, Law and Research; 'Automated State Action in India: Administrative Justice, Privacy and Constitutional Accountability' (Research Square, 2025) [preprint].

nocturnal domiciliary visits by police violated the personal liberty guarantee under Article 21.⁷

This position was progressively complicated by later decisions recognising privacy interests in specific contexts without these decisions being reconciled into a single constitutional principle. The resulting doctrinal inconsistency was the immediate occasion for the nine-judge reference that produced the Puttaswamy decision.

B. Puttaswamy (2017): The Proportionality Standard

The nine-judge bench in Puttaswamy unanimously held that M.P. Sharma and Kharak Singh were incorrect to the extent that they denied a fundamental right to privacy, and recognised privacy as intrinsic to human dignity, protected under Article 21 read with Articles 14 and 19.⁸ Justice Chandrachud's opinion identified privacy as encompassing bodily integrity, informational privacy, and decisional autonomy. The operative proportionality standard requires that any restriction on privacy (i) have a basis in law, (ii) pursue a legitimate state aim, and (iii) be proportionate to, and necessary for, the achievement of that aim.

C. The Aadhaar Judgment (2018)

In Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar), the Supreme Court, by a majority of four to one, upheld the core architecture of the Aadhaar Act 2016 while striking down provisions permitting mandatory linkage by private entities.⁹ Justice Chandrachud, dissenting, held that the Aadhaar system constituted a surveillance architecture inconsistent with the constitutional values articulated in Puttaswamy.

D. Anuradha Bhasin v Union of India (2020): Refining the Test

The proportionality standard was further developed in *Anuradha Bhasin v Union of India* (2020), concerning internet shutdowns in Jammu and Kashmir.¹⁰ The Court held that restrictions on fundamental rights must satisfy a refined test requiring a legitimate aim, a rational connection between the measure and that aim, the absence of a less restrictive but equally effective alternative, and the absence of a disproportionate impact on the right-holder.

⁷M.P. Sharma v Satish Chandra AIR 1954 SC 300; Kharak Singh v State of UP AIR 1963 SC 1295.

⁸Puttaswamy (n 5) para 325 (Chandrachud J).

⁹Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar) (2018) 1 SCC 809.

¹⁰Anuradha Bhasin v Union of India (2020) 3 SCC 637.

Bhasin is significant because it demonstrates the Court's willingness to apply a structured proportionality analysis to executive security measures lacking clear legislative backing.

E. Selvi v State of Karnataka (2010): Bodily Privacy and Investigative Technology

Although decided before Puttaswamy, *Selvi v State of Karnataka* (2010) remains relevant.¹¹ The Court held that involuntary narcoanalysis, polygraph examination, and brain electrical activation profiling violated Articles 20(3) and 21, emphasising that investigative techniques involving the body and mind require meaningful consent. The decision establishes, by analogy, that investigative technology use against individuals is subject to constitutional limits that do not yield automatically to claims of investigative utility a principle equally applicable to facial recognition.

III. THE AI SURVEILLANCE LANDSCAPE IN INDIA

A. Facial Recognition Deployments: A Documented Timeline

It is necessary to be precise about the documented history of facial recognition deployment in India, since public reporting has occasionally conflated distinct systems. The National Crime Records Bureau issued a tender in 2019 for a centralised National Automated Facial Recognition System.¹² The nationwide NAFRS project, as originally tendered, has experienced delays and has been the subject of controversy; various state and city-level facial recognition systems have in fact been deployed independently of, and in advance of, the centralised NAFRS framework.

The earliest documented public deployment was at the 2019 Kumbh Mela in Prayagraj, used for crowd management and the location of missing persons. This 2019 deployment is reported by the Internet Freedom Foundation as the earliest documented use of facial recognition technology by Indian authorities in a public setting, predating its subsequent use in protest policing later the same year.

The use of facial recognition for protest surveillance was first documented at scale during the Anti-CAA protests of December 2019. Following the passage of the Citizenship

¹¹*Selvi v State of Karnataka* (2010) 7 SCC 263.

¹²National Crime Records Bureau, Request for Proposal for National Automated Facial Recognition System (Ministry of Home Affairs, 2019).

Amendment Act, Delhi Police filmed protesters at demonstration sites and ran the footage through its Automated Facial Recognition Software, drawing on a database reportedly compiled from earlier protests. The Uttar Pradesh Police independently deployed comparable technology, supplied by a different private vendor, to identify protesters in that state. Following the communal violence in northeast Delhi in February 2020, Delhi Police later disclosed that of 755 persons arrested in connection with the riots, 231 were traced using CCTV or other video footage, of whom approximately 137 were identified specifically through facial recognition matching.¹³ The episode is significant because it illustrates concretely the chilling-effect concern raised in Part VI.C: protesters reportedly circulated guidance on covering their faces specifically in response to the known use of this technology, a direct and observable instance of surveillance altering the willingness of citizens to exercise their Article 19(1)(a) rights.¹⁴

The scale of facial recognition deployment increased considerably at the Maha Kumbh Mela held in Prayagraj between January and February 2025, where the Uttar Pradesh government deployed over 2,750 AI-enabled CCTV cameras alongside more than 100 dedicated facial recognition cameras, intended to manage an estimated 400-450 million pilgrims. Unlike the 2019 deployment and the protest-related uses discussed above, the stated purpose was explicitly humanitarian: police officials reported that the technology was used to locate missing persons, with authorities crediting AI-assisted facial matching for reuniting over 20,000 individuals with their families. This deployment is instructive for the proportionality analysis in Part VI for a specific reason: even where the stated aim is unambiguously benign, the underlying legal infrastructure executive deployment, the absence of any statute, the absence of published accuracy data, and the absence of any mechanism for an individual to learn that their facial data was captured remains identical to that used in the 2019 protest context. A legitimate and even laudable purpose does not, on the analysis in Part VI.A, cure the absence of a statutory basis; it simply makes the absence less visible.

Civil society organisations have documented concerns regarding accuracy disparities in facial recognition systems generally, particularly affecting darker-skinned individuals and

¹³Rest of World and other reporting on the statement of the Delhi Police Commissioner that, of 755 persons arrested in connection with the February 2020 northeast Delhi riots, 231 were traced using video footage, of whom approximately 137 were identified through facial recognition matching.

¹⁴HuffPost India and Global Voices, reporting on protester guidance to cover faces during the Anti-CAA protests in response to known facial recognition surveillance, December 2019-January 2020.

women. Comprehensive, India-specific accuracy data for the systems currently deployed is not publicly available, which is itself indicative of a transparency gap discussed further in Part VII.

B. NATGRID and CCTNS

NATGRID is an intelligence-sharing platform that connects approximately 21 categories of government and private-sector databases for access by authorised agencies. The platform became operational in 2023. The expansion of NATGRID's reach has continued through 2024 and 2025: access, initially confined to ten designated central security agencies, has since been extended to State police officers at the rank of Superintendent of Police, following directions issued after the 2024 conference of Directors General of Police. Recent reporting also indicates that NATGRID has begun integrating facial recognition capability with its existing database architecture, and has been linked in part to the National Population Register, although the precise current scope of this integration is not independently verifiable from public sources and should be treated with corresponding caution.¹⁵ This pattern of expansion broadening both the range of agencies with access and the categories of data linked occurs entirely through executive and administrative action, without any amendment to NATGRID's statutory basis, reinforcing the legality concern raised in Part VI.A.

CCTNS performs a related but more limited function, linking police stations nationally to facilitate the sharing of crime and criminal records.¹⁶ Neither NATGRID nor CCTNS is established by primary legislation; both operate as administrative initiatives, without a statutory basis defining their scope, data retention limits, or the rights of individuals whose data is processed.

C. DigiYatra and the Public-Private Surveillance Interface

DigiYatra illustrates a distinct category of AI surveillance that does not fit neatly within either the state or private surveillance categories. Launched by the Ministry of Civil Aviation in December 2022 and coordinated through the Digi Yatra Foundation a Section 8 not-for-profit company in which the Airports Authority of India holds a 26 per cent stake alongside five private airport operators the system uses facial recognition to verify passenger identity at

¹⁵Wikipedia contributors, 'NATGRID' (2025)

¹⁶National Crime Records Bureau, Crime and Criminal Tracking Network and Systems (CCTNS): Scheme Document (Ministry of Home Affairs).

airport checkpoints, linked to Aadhaar-based enrolment.¹⁷ By mid-2025 the system had over 15 million enrolled users across 24 airports.

DigiYatra raises a structural accountability concern distinct from NAFRS or NATGRID. Because the Digi Yatra Foundation is constituted as a private company rather than a government department, it is not directly answerable to requests under the Right to Information Act 2005, notwithstanding the Airports Authority of India's minority shareholding. This structure allows a facial recognition system operating at the threshold of national infrastructure to remain substantially outside the transparency obligations that would apply to an equivalent government-operated system. The Internet Freedom Foundation has separately raised concerns regarding non-consensual enrolment, citing reports of airport staff capturing passenger biometrics without adequate disclosure of purpose. A further governance lapse emerged in 2024, when DigiYatra's original technology vendor was implicated in a money-laundering investigation, during which the personal data including facial biometrics of over 3.3 million users was found to have been hosted on the vendor's own infrastructure rather than government-controlled servers, contrary to the data-handling assurances made to enrolled passengers. DigiYatra is, in this sense, a case study in the public-private blurring identified more generally in Part III.D below: a facial recognition system serving a state function, substantially funded and overseen through a state-owned enterprise, but structured as a private entity in a manner that limits the transparency and accountability obligations that would otherwise attach to comparable government surveillance infrastructure.

D. Private Sector Surveillance and the Blurring of Boundaries

AI surveillance in India is not confined to state actors and quasi-state entities such as DigiYatra. Private telecommunications and technology companies process personal data at a scale that, in aggregate, likely exceeds the volume held in state systems. The pattern that Shoshana Zuboff has described as 'surveillance capitalism' — the conversion of behavioural data into predictive commercial products — is well documented in the Indian digital economy.¹⁸ The point of particular constitutional significance is the intersection between

¹⁷Ministry of Civil Aviation / Digi Yatra Foundation, on the structure of the Digi Yatra Foundation as a Section 8 company with Airports Authority of India holding a 26 per cent stake alongside five private airport operators, launched December 2022.

¹⁸Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

commercial data holdings and state surveillance, examined further in Part IV.

IV. THE LEGISLATIVE FRAMEWORK AND ITS GAPS

A. The Information Technology Act 2000

Section 69 of the Information Technology Act 2000 empowers the Central and State Governments to direct interception, monitoring, or decryption of information, on grounds including sovereignty, security, public order, and prevention of incitement to cognisable offences.¹⁹ Concerns have been raised regarding the breadth of these grounds, the absence of any requirement for prior judicial authorisation, and the limited transparency of the review committee constituted under the Act.

In *People's Union for Civil Liberties v Union of India* (1997), the Supreme Court laid down procedural safeguards specifically for telephone interception.²⁰ These safeguards predate Puttaswamy by two decades and were designed for individually authorised wiretaps; their adequacy for AI-enabled surveillance systems has not been authoritatively tested.

B. The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 is India's first comprehensive data protection statute. It establishes a consent-based framework for the processing of digital personal data, recognises data principal rights including access, correction, and erasure,²¹ and creates the Data Protection Board of India as the principal regulatory authority.²²

The legislative history of the relevant provision is itself instructive. The Digital Personal Data Protection Bill 2023 was passed by the Lok Sabha on 7 August 2023 and by the Rajya Sabha two days later, after what civil society monitoring records as approximately two hours of combined debate across both Houses, with only sixteen Members of Parliament participating in total. In the Lok Sabha specifically, the discussion lasted approximately fifty minutes and involved eight speakers, each allotted under three minutes. During this debate, the Union Minister for Electronics and Information Technology defended the Bill's security

¹⁹Information Technology Act 2000 (India), s 69, 69A, 69B.

²⁰*People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

²¹Digital Personal Data Protection Act 2023 (India), ss 4, 7, 8.

²²Digital Personal Data Protection Act 2023 (India), s 28 (Data Protection Board of India).

exemptions by comparing them to the GDPR, stating that the European framework contains sixteen exemptions for government processing against four under the Indian Bill; this comparison has been disputed by civil society analysis on the ground that the Bill clusters several distinct exemption grounds, spread across Sections 7 and 17, into a single headline figure, making the numerical comparison potentially misleading. Opposition members raised concerns during the limited debate regarding the independence of the Data Protection Board and the absence of safeguards accompanying the security exemption, though the brevity of the discussion meant these concerns received no recorded ministerial response of substance.²³ The comparative absence of legislative scrutiny is significant for the constitutional analysis in Part VI: a provision enacted with this degree of deliberation is, on the legality reasoning advanced there, harder to characterise as the product of the considered legislative judgment that a restriction on a fundamental right is ordinarily expected to reflect.

Section 17 of the Act exempts the processing of personal data by, or on behalf of, instrumentalities of the State from a substantial range of the Act's obligations, where such processing is necessary in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or the prevention of cognisable offences.²⁴ It would be an oversimplification to characterise the Act as failing to regulate surveillance altogether: data fiduciaries remain subject to general processing obligations outside the scope of the exemption, and data principal rights continue to apply to processing that does not fall within Section 17. The more precise concern, examined in detail in Part VI, is that Section 17 permits exemption on grounds that are not narrowly defined, without a requirement for prior independent authorisation or subsequent judicial review of the exemption's invocation.

C. Comparative Perspective: GDPR and CCPA

The European Union's General Data Protection Regulation classifies biometric data processed for unique identification as a special category of personal data, subject to processing only in narrowly defined circumstances, with law enforcement use separately governed by a dedicated Directive.²⁵ The California Consumer Privacy Act provides consumers with rights

²³Lok Sabha and Rajya Sabha Debates on the Digital Personal Data Protection Bill 2023 (3-9 August 2023), as summarised in Internet Freedom Foundation (n 36) and ThePrint (n 37).

²⁴Digital Personal Data Protection Act 2023 (India), s 17.

²⁵Regulation (EU) 2016/679 (General Data Protection Regulation), art 9.

of access, deletion, and opt-out that extend to certain law-enforcement-adjacent contexts.²⁶

India's framework does not yet provide a comparable categorical protection for biometric data, and the Data Protection Board's independence and investigative powers in respect of state surveillance are more limited than those of supervisory authorities operating under the GDPR.

V. POST-PUTTASWAMY JUDICIAL DEVELOPMENTS

The Aadhaar judgment remains the most sustained post-Puttaswamy judicial engagement with biometric technology at the Supreme Court level. At the High Court level, the Delhi High Court has been seized of a public interest litigation concerning Delhi Police's use of facial recognition technology, which remains pending.²⁷ The litigation has resulted in some disclosure, in court filings, of operational details concerning the relevant system, including the 80 per cent matching threshold discussed in Part VII.A.

Anuradha Bhasin indicates that courts are prepared to apply a structured proportionality analysis to executive measures affecting fundamental rights even where those measures are not directly authorised by a specific surveillance statute. Taken together, these developments suggest that courts have acknowledged the privacy and proportionality concerns raised by executive surveillance measures, while generally preferring that the underlying statutory framework be supplied by the legislature.

VI. SECTION 17 DPDP ACT: CONSTITUTIONAL COMPATIBILITY WITH PUTTASWAMY

The preceding Part has shown that Indian courts have engaged with the privacy and proportionality implications of surveillance technology without striking down any specific programme for want of a statutory basis. This Part undertakes a more granular constitutional audit of the provision that, on the analysis advanced in Part IV, does the most work in keeping AI surveillance outside the reach of statutory protection: Section 17 of the Digital Personal Data Protection Act 2023. There is, at the outset, something worth naming plainly: the Digital Personal Data Protection Act 2023 creates a constitutional paradox by recognising privacy

²⁶California Consumer Privacy Act, Cal Civ Code ss 1798.100-1798.199.

²⁷ High Court of Delhi, In Re: Facial Recognition Technology by Delhi Police, WP(C) 8654/2019 (pending).

rights while simultaneously exempting the very state surveillance systems that most threaten informational privacy. The Act's preamble speaks the language of Puttaswamy; its substantive architecture, through Section 17, withdraws that language precisely where the threat to informational privacy is greatest. This Part examines whether that paradox is merely an awkward legislative choice or a constitutional defect, considering legality, necessity, proportionality, procedural safeguards, and judicial review in turn.

A. Legality

Section 17 satisfies the most basic sense of the legality requirement: it is a provision of an Act of Parliament, and in that narrow sense possesses a 'basis in law' that NAFRS and NATGRID do not. The more demanding question is whether Section 17 itself is precise and foreseeable in the way Puttaswamy's legality limb requires. Here the analysis becomes considerably less favourable: each of Section 17's grounds reproduces, almost verbatim, the language of Section 69 of the Information Technology Act 2000, a provision whose breadth this article has already criticised in Part IV.A. A ground for exemption is not rendered precise merely by being enacted; if 'public order' was insufficiently precise to satisfy the legality requirement when used to authorise interception under the IT Act, it is difficult to see why the same phrase becomes precise when used to authorise exemption from data protection obligations. The legality limb is, on this reasoning, satisfied only formally, not substantively.

B. Necessity

Section 17, as drafted, does not require the State to demonstrate that no less restrictive measure was available. It does not require a specific processing activity to be necessary; it requires only that the activity be undertaken 'in the interests of' one of the listed grounds, a formulation considerably weaker than a necessity test and closer to a test of mere relevance. A data fiduciary that is also a state instrumentality need not demonstrate, before invoking the exemption, that no less privacy-intrusive method was available. This is a significant departure from the standard applied in Puttaswamy, and from the refined formulation in Anuradha Bhasin, which requires the absence of a less restrictive but equally effective alternative as a freestanding element of the test. Section 17 does not merely fail to mention this requirement; it structurally cannot accommodate it, because the exemption operates *ex ante*, at the point of processing, rather than through any subsequent inquiry into whether a less intrusive alternative existed.

C. Proportionality

Even granting that the underlying aims are legitimate, proportionality in the strict sense requires that the benefit secured be weighed against the severity of the privacy intrusion. The structural difficulty with Section 17 is that it removes precisely the mechanism data principal rights, fiduciary obligations, Board oversight through which this weighing would ordinarily occur. A data principal subject to surveillance processing exempted under Section 17 cannot exercise the rights of access, correction, or erasure that would otherwise allow them, or an oversight body acting on their behalf, to assess whether the processing was proportionate to its stated aim. The proportionality inquiry is foreclosed at the level of process, because the exemption removes the informational and procedural predicates on which any proportionality assessment would depend.

D. Procedural Safeguards

Puttaswamy's proportionality framework, particularly as developed in *Bhasin*, contemplates procedural safeguards as a distinct element — periodic review, defined duration, and a recorded necessity finding. Section 17 contains none of these. It is not subject to a sunset clause; it does not require the State to record the specific necessity finding said to justify exemption in a given instance; and it applies to an open-ended category of state processing. By comparison, the procedural safeguards laid down for telephone interception in PUCL themselves criticised in Part IV.A as inadequate for AI-scale surveillance at least required a recorded order, a review committee, and periodic destruction of records. Section 17 does not import even this comparatively modest procedural architecture into the data protection context, notwithstanding that the PUCL safeguards were available as a template.

E. Judicial Review

As a matter of formal law, an aggrieved data principal is not barred from seeking judicial review of executive action taken under Section 17, and constitutional remedies under Articles 32 and 226 remain available in principle. The practical difficulty is that Section 17, by withdrawing the data principal's rights of access and grievance redressal, removes the ordinary evidentiary basis on which such review would proceed. A petitioner cannot meaningfully challenge the proportionality of a specific instance of exempted processing without first knowing that the processing occurred, what data was collected, and for what stated purpose

precisely the information that Section 17 permits the State to withhold. Judicial review survives in form but is considerably weakened in substance.

F. Recent Developments (2024-2026)

The constitutional concerns identified above have acquired sharper practical significance as the DPDP Act has moved from enactment toward implementation. Although the Act received presidential assent in August 2023, it remained substantially dormant until the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules 2025 on 13 November 2025, together with notifications establishing the Data Protection Board of India.²⁸ Implementation has proceeded in three phases: Phase I, effective immediately upon notification, established the Board itself; Phase II, scheduled for November 2026, operationalises the Consent Manager framework; and Phase III, under which the substantive data-fiduciary obligations become enforceable, is scheduled to commence on 13 May 2027.²⁹

This phased timeline has a direct bearing on the argument advanced in this Part. For the period between the Act's notification and the full commencement of Phase III, the substantive rights that would, on ordinary processing, allow a data principal to test the proportionality of state action are not yet enforceable even outside the Section 17 exemption. The constitutional paradox identified at the outset of this Part is, in this sense, temporarily compounded rather than resolved by the implementation timeline: state surveillance processing remains exempted under Section 17, while the general rights regime against which that exemption is most usefully measured has not yet come into full legal effect. It remains to be seen, once Phase III commences, whether the Data Protection Board itself a body appointed by and answerable to the Central Government will be either willing or institutionally equipped to scrutinise the boundaries of an exemption that operates, in substantial part, for the benefit of the same executive that appoints the Board's members.

²⁸Digital Personal Data Protection Rules 2025, GSR 846(E) (13 November 2025).

²⁹Ministry of Electronics and Information Technology, Enforcement Notification for the Digital Personal Data Protection Act 2023 (13 November 2025), establishing a three-phase implementation timeline with the Data Protection Board constituted in Phase I, the Consent Manager framework in Phase II (November 2026), and substantive data-fiduciary obligations enforceable from Phase III (13 May 2027).

VII. AI SURVEILLANCE AND ARTICLE 14: EQUALITY, NON-ARBITRARINESS, AND DUE PROCESS

The analysis in Part VI was conducted principally through the lens of Article 21 and the Puttaswamy proportionality standard. This is necessary but not sufficient. A separate and increasingly significant line of constitutional concern arises under Article 14, and this Part examines that concern specifically, before drawing the equality and due process strands together with the privacy analysis already advanced.

A. False Positives and Wrongful Identification

Facial recognition systems do not identify individuals with certainty; they generate probabilistic matches subject to a threshold set by the operating agency. Delhi Police has disclosed that matches scoring above 80 per cent similarity are treated as positive results, while matches below that threshold are treated as 'false positives' that may nonetheless prompt further human investigation rather than being discarded outright. No public reasoning has been offered for the selection of 80 per cent as the relevant threshold, and the practice of subjecting sub-threshold matches to continued investigative attention means that an individual who has been wrongly flagged may face follow-up scrutiny without ever being informed that a facial recognition match was the original basis for it.

The consequence of a false positive in this context is not a minor inconvenience. Where facial recognition is used, as documented in Part III, to identify individuals at protests or during the investigation of communal violence, an erroneous match exposes the misidentified individual to police questioning, potential arrest, and the social and reputational consequences of being associated with a criminal investigation, on the basis of a probabilistic algorithmic output that the individual has no opportunity to see, test, or contest before it is acted upon.

B. Discrimination and Demographic Accuracy Disparities

The risk of wrongful identification is not evenly distributed across the population. Foundational research conducted at the MIT Media Lab found that commercial facial recognition algorithms developed by IBM, Microsoft, and Face++ produced error rates of less than one per cent for lighter-skinned male subjects, rising to as high as 34.7 per cent for darker-skinned female subjects. The United States National Institute of Standards and Technology's

2019 Face Recognition Vendor Test similarly found that the majority of algorithms tested exhibited demographic differentials in false-positive rates, with Asian and African American faces misidentified at rates ten to one hundred times higher than Caucasian faces in one-to-one matching, depending on the specific algorithm.³⁰ Subsequent research has confirmed that these disparities persist, and has identified contributing factors including the underrepresentation of women and darker-skinned individuals in the training datasets most commonly used to build these systems.

No equivalent India-specific demographic accuracy audit of the facial recognition systems deployed by Indian law enforcement agencies has been made public. In the absence of published, India-specific error-rate data disaggregated by skin tone, gender, and age, it is not possible to state with precision how the documented global pattern translates into the systems operated by Delhi Police or deployed at the Maha Kumbh Mela discussed in Part III.A. What can be said is that the burden of demonstrating the absence of discriminatory impact ought, consistently with Article 14, to rest with the deploying authority rather than with the affected individual, and that no Indian legal requirement currently imposes such a burden.

C. Algorithmic Opacity

A further structural concern, distinct from but related to demographic disparity, is the 'black box' character of the algorithms themselves. Commercial facial recognition systems are typically proprietary, and the specific weights, training data, and matching logic underlying a given match are ordinarily known only to the vendor, not to the deploying police force, the affected individual, or any reviewing court.³¹ This opacity creates two distinct difficulties. First, it prevents meaningful after-the-fact scrutiny of why a particular match was generated. Second, it forecloses the kind of transparency that due process ordinarily requires before an adverse action is taken against an individual: a person who has been identified, questioned, or arrested on the strength of an algorithmic match is, under the present framework, unable to obtain a meaningful explanation of how that match was generated, still less to challenge its underlying logic.

³⁰National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (2019), finding false-positive rate differentials of a factor of 10 to 100 between Asian and African American faces and Caucasian faces, depending on algorithm.

³¹Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

D. Connecting the Threads: Equality, Non-Arbitrariness, and Due Process

The Supreme Court's jurisprudence on Article 14 has, since *E.P. Royappa v State of Tamil Nadu* (1974), recognised that equality is the antithesis of arbitrariness, such that state action which is unreasoned, capricious, or unsupported by an intelligible basis may be struck down independently of any classification-based discrimination analysis.³² *Maneka Gandhi v Union of India* (1978) extended this reasoning into Article 21, holding that any procedure depriving a person of life or personal liberty must be fair, just, and reasonable, and not arbitrary or oppressive.³³

Applying this framework to the facial recognition practices described above yields three distinct but related conclusions. First, on equality: a system that is demonstrated, in comparable jurisdictions, to misidentify women and darker-skinned individuals at materially higher rates, and that has not been subjected to an equivalent India-specific audit, cannot presently be shown to treat similarly situated individuals alike; the absence of evidence to the contrary is not equivalent to evidence of non-discrimination, and the burden of producing such evidence should properly fall on the State. Second, on non-arbitrariness: a system that flags a 'false positive' yet continues to subject the flagged individual to investigative attention, without disclosed criteria for why an 80 per cent threshold rather than some other figure was chosen, is difficult to characterise as a reasoned or intelligible exercise of state power in the sense *Royappa* requires. Third, on due process: an individual who is identified, questioned, or investigated on the strength of an opaque algorithmic match, without notice that such a match was the basis for the State's attention and without any avenue to contest the match's reliability, is denied the fair and reasonable procedure that *Maneka Gandhi* requires before personal liberty is restricted.

Recent Indian scholarship has begun to develop a doctrine of 'technological due process' addressing precisely this gap, drawing on the established Article 14 and 21 framework to argue that algorithmic state action requires, at minimum, disclosed decision criteria, a mechanism for affected individuals to contest an adverse algorithmic output, and a published accuracy and bias audit prior to deployment. This article's analysis in Parts VI and VII converges on the same conclusion from two directions: Part VI's proportionality analysis shows that NAFRS and

³²*E.P. Royappa v State of Tamil Nadu* (1974) 4 SCC 3.

³³*Maneka Gandhi v Union of India* (1978) 1 SCC 248.

NATGRID lack the statutory basis and procedural safeguards Puttaswamy requires; this Part shows, independently, that the same systems raise equality and non-arbitrariness concerns under Article 14 that exist regardless of whether a statutory basis is eventually supplied. A surveillance statute of the kind proposed in Part VIII would need to address both sets of concerns legality and proportionality under Article 21, and accuracy, disclosure, and contestability under Article 14 to bring India's AI surveillance infrastructure into full constitutional compliance.

A related free-speech dimension also deserves mention. In *Shreya Singhal v Union of India* (2015), the Court recognised that measures may violate Article 19(1)(a)³⁴ by chilling expression, independently of any direct restriction. The Anti-CAA protest surveillance documented in Part III.A is a concrete instance of this concern: protesters reportedly altered their behaviour specifically because of known facial recognition use, illustrating that the chilling effect identified abstractly in earlier scholarship is, in the Indian context, an observed rather than merely theoretical phenomenon.

VIII. APPLYING THE PROPORTIONALITY TEST TO NAFRS AND NATGRID GENERALLY

A. The Legality Requirement

Neither NAFRS nor NATGRID is established by primary legislation; both originate in executive and administrative decisions of the Ministry of Home Affairs. This is significant because the legality requirement, on the reasoning in both Puttaswamy and Bhasin, is not merely a procedural formality but reflects the principle that intrusions on fundamental rights require legislative, rather than purely executive, authorisation.

B. Legitimate Aim and Necessity

National security and the investigation and prevention of crime are legitimate state aims. The constitutional difficulty concerns the scope of surveillance conducted relative to those aims. NAFRS, as deployed at events such as the Maha Kumbh Mela, has been used to scan very large crowds rather than identified suspects, even where its stated purpose is itself benign. NATGRID similarly aggregates data drawn from the records of all individuals whose

³⁴Constitution of India 1950, art 19(1)(a).

transactions pass through its source databases. The necessity limb requires the State to demonstrate that no less intrusive measure was reasonably available a demonstration not yet made public for either system.

C. Proportionality and the Chilling Effect

The absence of published accuracy or outcome data for India's facial recognition deployments makes the proportionality assessment difficult to conduct with precision.³⁵ What can be said is that the scale of data collection particularly through NATGRID's integration of biometric and financial records represents a substantial privacy intrusion that the available public information does not yet allow to be evaluated against a clearly demonstrated benefit. As Part III.A and Part VII.D together show, this is not merely a theoretical concern: the documented Anti-CAA protest surveillance demonstrates the chilling effect in practice, while the demographic accuracy disparities discussed in Part VII.B demonstrate that the privacy intrusion itself is unevenly, and not merely uniformly, distributed across the population.

IX. RECOMMENDATIONS FOR REFORM

A. A Dedicated Legislative Framework for AI Surveillance

A legislative framework specifically addressing AI surveillance by state agencies would address the legality gap identified in Parts VI and VIII. Such legislation should define the permissible scope of AI surveillance, require judicial or independent authorisation for surveillance targeting identified individuals, restrict mass biometric surveillance to circumstances of specific and time-limited statutory authorisation, provide individuals with a right to access and correct data held about them, mandate disclosure of matching thresholds and published accuracy audits disaggregated by demographic group, and establish civil and, where warranted, criminal consequences for unauthorised surveillance.

B. Independent Oversight

The Data Protection Board, whose members are appointed by the Central Government and whose mandate does not extend to security-related processing exempted under Section 17, is not well positioned to oversee state surveillance specifically. A dedicated parliamentary

³⁵Modern Dental College and Research Centre v State of MP (2016) 7 SCC 353.

oversight mechanism, with the capacity to receive classified briefings, commission independent technical and demographic accuracy audits, and report periodically on the operation of AI surveillance systems, would address this gap.

C. Mandatory Privacy and Accuracy Impact Assessments

Prior to the deployment of any AI surveillance system, a published assessment addressing necessity, proportionality, the system's measured accuracy and any known demographic disparities in error rates, data retention and deletion policy, and the remedies available to individuals incorrectly identified, would address several of the transparency gaps identified in this article. Such assessments should be subject to review by the independent oversight mechanism proposed above prior to deployment, and should apply equally to ostensibly benign deployments, such as Maha Kumbh crowd management, and to investigative deployments, such as protest surveillance, given that the underlying legal infrastructure is identical in both cases.

D. A Narrower Section 17 Exemption

Section 17 need not be removed in its entirety, given the legitimate security interests it is intended to serve; it would, however, benefit from being narrowed so that reliance on the exemption requires specific statutory authorisation for the particular processing activity, a defined time limit, and provision for subsequent independent or judicial review, consistent with the legality, necessity, procedural safeguards, and judicial review deficiencies identified in Part VI.

E. Article 14 Compliance Standards

Independently of the Article 21 reforms above, any AI surveillance system involving biometric identification should be required, prior to deployment, to publish a demographic accuracy audit; to disclose its matching threshold and the criteria for that threshold's selection; and to provide affected individuals with a mechanism to learn that an algorithmic match formed the basis of police attention and to contest that match's reliability. These measures respond directly to the false-positive, discrimination, and opacity concerns identified in Part VII, and are necessary independently of whether a comprehensive surveillance statute of the kind proposed in Part IX.A is eventually enacted.

X. CONCLUSION

At its core, this article has argued that the Digital Personal Data Protection Act, 2023 creates a constitutional paradox: it recognises privacy rights consistent with Puttaswamy's language while exempting, through Section 17, the very surveillance systems that pose the greatest threat to the right the Act purports to protect. This article has examined whether India's principal AI surveillance systems and its current data protection framework satisfy the constitutional standards established in Puttaswamy under Article 21, and developed independently under Article 14. It finds that NAFRS, NATGRID, and the documented deployments examined in Part III from the Anti-CAA protests through the Maha Kumbh Mela to DigiYatra lack a clear statutory basis, that Section 17 fails each element of the legality, necessity, proportionality, procedural safeguards, and judicial review audit conducted in Part VI, and that documented demographic accuracy disparities and algorithmic opacity raise independent and unresolved concerns under Article 14.

These findings should not be read as a claim that AI surveillance is illegitimate in principle, or that security considerations are not weighty; they plainly are, and the humanitarian use of facial recognition at the Maha Kumbh Mela illustrates that such systems can serve genuinely beneficial purposes. The argument advanced here is narrower: that the legality, necessity, and proportionality requirements articulated in Puttaswamy and refined in Anuradha Bhasin, together with the equality and non-arbitrariness requirements developed since Royappa and Maneka Gandhi, apply with equal force to AI-enabled surveillance regardless of its stated purpose, and that India's present legislative framework has not yet been adapted to meet that combined standard.

The reforms proposed in Part IX a dedicated legislative framework, independent oversight, mandatory impact assessments, a narrower Section 17 exemption, and specific Article 14 compliance standards are consistent with approaches already adopted in other jurisdictions and would not, on their own terms, prevent legitimate security or humanitarian use of these technologies. They would, however, bring India's AI surveillance infrastructure into closer alignment with the constitutional standards the Supreme Court has itself articulated across both Articles 21 and 14. Further research, particularly empirical research into the comparative accuracy of facial recognition systems specifically deployed in India, and close monitoring of the Data Protection Board's adjudicatory practice once Phase III of the DPDP

Act takes effect in May 2027, would strengthen the evidentiary basis for these proposals and is recommended as a direction for future scholarship.

REFERENCES

A. Cases

1. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
2. Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar) (2018) 1 SCC 809.
3. M.P. Sharma v Satish Chandra AIR 1954 SC 300.
4. Kharak Singh v State of UP AIR 1963 SC 1295.
5. People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
6. Shreya Singhal v Union of India (2015) 5 SCC 1.
7. Modern Dental College and Research Centre v State of MP (2016) 7 SCC 353.
8. Anuradha Bhasin v Union of India (2020) 3 SCC 637.
9. Selvi v State of Karnataka (2010) 7 SCC 263.
10. E.P. Royappa v State of Tamil Nadu (1974) 4 SCC 3.
11. Maneka Gandhi v Union of India (1978) 1 SCC 248.
12. In Re: Facial Recognition Technology by Delhi Police, WP(C) 8654/2019 (Delhi HC, pending).

B. Statutes, Rules, and Parliamentary Material

1. Constitution of India 1950.
2. Information Technology Act 2000 (India).
3. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (India).
4. Digital Personal Data Protection Act 2023 (India).

5. Digital Personal Data Protection Rules 2025, GSR 846(E) (13 November 2025).
6. MeitY, Enforcement Notification for the Digital Personal Data Protection Act 2023 (13 November 2025).
7. Lok Sabha and Rajya Sabha Debates on the Digital Personal Data Protection Bill 2023 (3-9 August 2023).
8. Regulation (EU) 2016/679 (General Data Protection Regulation).
9. Directive (EU) 2016/680 (Law Enforcement Directive).
10. California Consumer Privacy Act, Cal Civ Code ss 1798.100-1798.199.

C. Committee Reports and Government Documents

1. Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, 2018).
2. Group of Experts on Privacy (Justice A.P. Shah Committee), Report of the Group of Experts on Privacy (Planning Commission, Government of India, 2012).
3. Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019).
4. United Nations Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (2021).
5. National Crime Records Bureau, Request for Proposal for National Automated Facial Recognition System (Ministry of Home Affairs, 2019).
6. Ministry of Home Affairs, National Intelligence Grid (NATGRID): Background Note (Government of India, 2023).
7. National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (2019).

D. Academic and Civil Society Sources

1. Internet Freedom Foundation, Project Panoptic: Tracking Facial Recognition in India (2021).
2. Internet Freedom Foundation, DPDPB 2023 in the Parliament: Dialogue, Drama, and Discord (2023).
3. PRS Legislative Research, Legislative Brief: The Digital Personal Data Protection Bill 2023 (2023).
4. Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books 2019).
5. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, 2015).
6. Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.
7. Intifada P. Basheer, 'Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India' (2025) SAGE.
8. 'Automated State Action in India: Administrative Justice, Privacy and Constitutional Accountability' (Research Square, 2025) [preprint].
9. 'Automated Decision-Making by the State in India: Constitutional Accountability under Articles 14 and 21' (2026) International Journal of Law, Law and Research.
10. Vidhi Centre for Legal Policy, Regulating Automated Decision-Making in India: Accountability and Fairness (Vidhi Policy Paper, 2021).