



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

REGULATING ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS: LEGAL, ETHICAL, AND CONSTITUTIONAL CHALLENGES IN INDIA

AUTHORED BY - ATUL VERMA

ABSTRACT

The deployment of artificial intelligence (“AI”) in criminal investigation in India — spanning facial recognition, predictive policing, automated forensic analysis and AI-assisted evidence authentication — has expanded rapidly since 2019, culminating in the National Crime Records Bureau's Crime and Criminal Tracking Network and Systems (CCTNS)-linked Crime and Criminal Profiling Identification (CrPI) platform launched in mid-2026. This growth has substantially outpaced the statutory and constitutional framework meant to govern it. This paper undertakes a doctrinal and analytical examination of the legal, ethical and constitutional dimensions of AI-enabled policing in India, situating the enquiry within the post-Puttaswamy privacy jurisprudence, the newly enacted criminal law trilogy — the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 — and the Digital Personal Data Protection Act, 2023 together with its Rules of 2025. The paper traces the statutory foundation supplied by the Criminal Procedure (Identification) Act, 2022 and evaluates the ongoing constitutional challenges to that statute before the Delhi High Court and, earlier, the Supreme Court. It further interrogates the evidentiary status of AI-generated and AI-authenticated material under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, and examines the ethical concerns of algorithmic bias, opacity, function creep and disproportionate impact on marginalised communities that have already surfaced in the Delhi Police's use of the Automated Facial Recognition System. The analysis extends to the November 2025 MeitY India AI Governance Guidelines and asks whether a “light-touch”, sector-agnostic governance model can adequately discipline a high-stakes, coercive state function such as criminal investigation.

KEYWORDS

Artificial Intelligence; Criminal Investigation; Facial Recognition Technology; Right to Privacy; Bharatiya Sakshya Adhiniyam, 2023; Criminal Procedure (Identification) Act, 2022; Digital Personal Data Protection Act, 2023; Algorithmic Policing; Constitutional Law; India.

1. INTRODUCTION

Artificial intelligence has moved from the periphery of Indian policing to its operational core within less than a decade. What began as isolated pilot projects — automated number-plate recognition in metropolitan traffic units and rudimentary facial-matching software deployed to trace missing children — has matured into a nationally networked architecture of algorithmic investigation. The Ministry of Law and Justice's press communication of 25 February 2025, quoting the Prime Minister's aspiration for a “justice system that will be fully future-ready”,¹ formally confirmed what practitioners had long observed: Indian law-enforcement agencies are integrating AI into surveillance, crime detection and criminal investigation as a matter of stated national policy. The most visible manifestation of this shift is the National Crime Records Bureau's (“NCRB”) Crime and Criminal Profiling Identification (“CrPI”) platform, a multi-modal biometric system launched in June 2026 that enables police officers to match facial images, fingerprints, iris scans and DNA profiles against national criminal databases in real time, operating within the NCRB's broader Inter-Operable Criminal Justice System that links CCTNS, e-Courts, e-Prisons, e-Forensics and e-Prosecution on a shared data architecture.²

The Delhi Police's Automated Facial Recognition System (“AFRS”), initially deployed in the aftermath of the February 2020 north-east Delhi riots, offers the starkest illustration of the risks such technologies carry. Subsequent judicial scrutiny of prosecutions built partly on AFRS identification revealed serious reliability concerns, contributing to acquittals or discharges in a striking eighty-two per cent of decided riot cases as of early 2025.³ That single statistic captures, in microcosm, the central tension this paper addresses: the same technology celebrated by the executive as a tool of speedy and efficient justice has, in practice, generated wrongful suspicion, prolonged pre-trial incarceration and — because facial recognition systems trained largely on non-representative datasets exhibit differential error rates across skin tone, gender and age — a disproportionate burden on already vulnerable groups.

India's constitutional and statutory landscape has, in principle, kept pace with these technological developments. The nine-judge bench decision in *Justice K.S. Puttaswamy v.*

¹Ministry of Law and Justice, Press Release, 25 February 2025, cited in Oxford Institute of Technology and Justice, “India: Increasing Use of AI Across the Justice System”, available at <https://www.techandjustice.bsg.ox.ac.uk/research/india> (last visited 4 August 2026).

²“Facial Recognition in Indian Criminal Investigations”, Budding Forensic Expert (2026), available at <https://www.buddingforensicexpert.in/2026/07/facial-recognition-in-indian-criminal-investigation.html> (last visited 4 August 2026).

³“Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations: Delhi Riots Lessons on Rights and Reliability”, Eng. Proc. 2026, 143(1), 17, DOI: 10.3390/engproc2026143017.

Union of India recognised privacy as intrinsic to Article 21 and prescribed a four-fold proportionality standard — legality, legitimate aim, necessity and proportionality *stricto sensu* — for any state action that infringes it.⁴ The criminal procedure trilogy that replaced the colonial-era codes on 1 July 2024 — the Bharatiya Nyaya Sanhita, 2023 (“BNS”), the Bharatiya Nagarik Suraksha Sanhita, 2023 (“BNSS”) and the Bharatiya Sakshya Adhiniyam, 2023 (“BSA”) — was projected by the Government as an opportunity to modernise investigative and evidentiary procedure for the digital age. Separately, the Criminal Procedure (Identification) Act, 2022 (“CPIA”) supplied the first explicit statutory basis for the collection of modern biometric “measurements” by police and prison authorities, while the Digital Personal Data Protection Act, 2023 (“DPDPA”) — brought into substantive operation through the Digital Personal Data Protection Rules, 2025 notified on 14 November 2025 — created India's first comprehensive data protection regime, albeit one carrying broad exemptions for law-enforcement processing.⁵

Yet none of these instruments was drafted with AI-driven investigation specifically in contemplation. The CPIA speaks of “measurements” and biometric capture but is silent on the algorithmic processes — machine-learning classification, probabilistic matching, automated risk-scoring — that convert raw biometric data into investigative leads. The BSA modernised the evidentiary treatment of electronic records through Section 63 but leaves largely unaddressed the distinct problem of evidence that is not merely stored or transmitted electronically but generated, enhanced or authenticated by an AI system whose internal reasoning is not fully explicable even to its operators. And a dedicated Facial Recognition Technology (Regulation of Police Powers) Bill, first introduced as a private member's bill in 2023, remains pending before Parliament, leaving facial recognition — arguably the most invasive of the current generation of AI policing tools — without any dedicated statutory regulation whatsoever.⁶

This regulatory gap has already precipitated litigation. The constitutionality of the CPIA was challenged before the Supreme Court, which declined to entertain the writ petition under

⁴Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

⁵Digital Personal Data Protection Rules, 2025, notified 14 November 2025; see “The 2026 Guide to Facial Recognition and Privacy in India”, Hyperverge (2026), available at <https://hyperverge.co/blog/facial-recognition-privacy-india/> (last visited 4 August 2026).

⁶Anmol Prasad, “Why India Must Pass the Pending Facial Recognition Technology Bill”, Bar & Bench, 4 April 2026, available at <https://www.barandbench.com/columns/why-india-must-pass-the-pending-frt-law> (last visited 4 August 2026).

Article 32 and directed the petitioners to the jurisdictional High Court;⁷ a corresponding writ petition is now pending before the Delhi High Court, brought by two students whose biometrics were collected by the police, contending that the Act violates Articles 14, 19 and 21 by permitting indefinite data retention, inter-agency sharing without regulation, and delegation of core safeguards to executive rule-making.⁸ Most recently, in July 2026 a Member of Parliament invoked the Supreme Court's writ jurisdiction under Article 32 to challenge the deployment of facial recognition and AI-enabled surveillance against participants in public protests, raising the deployment of AI investigative tools against the exercise of Article 19(1)(b) freedoms squarely before the apex court.⁹

Against this backdrop, this paper asks three interlinked questions. First, does the existing statutory architecture — the CPIA, the BNSS, the BSA, the DPDPA and the November 2025 India AI Governance Guidelines issued by the Ministry of Electronics and Information Technology (“MeitY”) — supply constitutionally adequate safeguards for AI-enabled investigation, measured against the Puttaswamy proportionality standard? Second, what evidentiary and due-process problems arise when AI-generated or AI-authenticated material is tendered in criminal trials under Section 63 of the BSA? Third, what law-reform measures are necessary to reconcile the legitimate investigative utility of AI with constitutional guarantees of privacy, equality, fair trial and freedom from self-incrimination? The paper proceeds in six further parts: a review of the extant literature (Part 2); a doctrinal and policy analysis of the constitutional, statutory and evidentiary framework (Part 3); consolidated findings (Part 4); recommendations (Part 5); and a conclusion (Part 6).

⁷Internet Freedom Foundation v. Union of India, W.P. (Crl.) Diary No. 53491 of 2023 (order of the Supreme Court declining to entertain the petition and granting liberty to approach the High Court); see Internet Freedom Foundation, “Supreme Court Dismisses Challenge to the Criminal Procedure (Identification) Act, 2022” (2024), available at <https://internetfreedom.in/supreme-court-dismisses-challenge-to-the-criminal-procedure-identification-act-2022/> (last visited 4 August 2026).

⁸Internet Freedom Foundation, “Delhi HC Issues Notice in the Constitutional Challenge to the Criminal Procedure (Identification) Act, 2022 and Rules Thereunder” (2026), available at <https://internetfreedom.in/delhi-hc-issues-notice-in-the-constitutional-challenge-to-the-criminal-procedure-identification-act-2022-and-rules-thereunder/> (last visited 4 August 2026).

⁹Tarun Choudhury, “Facial Recognition Technology at Protest Sites: Supreme Court to Examine AI Surveillance, Privacy and Protest Rights”, Legal Service India, 28 July 2026, available at <https://www.legalserviceindia.com/Legal-Articles/facial-recognition-technology-at-protest-sites-supreme-court-ai-surveillance-india/> (last visited 4 August 2026).

2. LITERATURE REVIEW

Scholarship on AI and criminal justice in India has developed along four broad strands. The first strand, doctrinal constitutional analysis, engages primarily with the CPIA. Writing shortly after the Act's passage, commentators in the *NUJS Law Review* argued that the statute's failure to tie the scope of “measurements” to a specific, legitimate investigative purpose renders it vulnerable on purpose-limitation grounds, drawing on European data-protection doctrine to test the Act's proportionality.¹⁰ A related critique published on SCC OnLine Blog identified four “fundamental concerns” with the Act — absence of a defined analytical framework for the use of collected measurements, indefinite retention, cross-agency sharing without regulatory oversight, and application to all arrestees irrespective of offence severity — concluding that the statute fails the necessity and proportionality limbs of the Puttaswamy test.¹¹ Analysis from the Constitutional Law Society at NLU Odisha goes further, contending that the Act's near-total delegation of substantive safeguards to subordinate rule-making offends the excessive-delegation doctrine articulated in the *Delhi Laws Act* reference and its progeny.¹²

A second strand focuses on facial recognition specifically. Empirical and policy-oriented work — including the Pulitzer Center's investigative reporting on AFRS deployment in Delhi and the 2026 Engineering Proceedings study on the Delhi riots prosecutions — documents the practical consequences of deploying facial recognition without accuracy audits, confidence-threshold disclosure or judicial oversight, linking algorithmic misidentification directly to wrongful arrest and prolonged remand.¹³ Comparative work situates the Indian position against the European Union, observing that while the EU's AI Act classifies real-time remote biometric identification for law-enforcement purposes as a prohibited or, at minimum, high-risk practice subject to prior judicial or independent authorisation, India has no equivalent classification and no dedicated statute — a gap several commentators trace to the continued pendency of the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 first introduced as a

¹⁰“Editorial Note: Scrutinising the Criminal Procedure (Identification) Act, 2022”, *NUJS Law Review* (2022), available at <https://nujlawreview.org/wp-content/uploads/2022/08/15.1-Edn-note.pdf> (last visited 4 August 2026).

¹¹“Questioning the Feasibility of the Criminal Procedure (Identification) Act, 2022”, SCC OnLine Blog, 31 May 2022, available at <https://www.sconline.com/blog/post/2022/05/31/questioning-the-feasibility-of-the-criminal-procedure-identification-act-2022/> (last visited 4 August 2026).

¹²“Examining the Constitutionality of the Criminal Procedure (Identification) Act, 2022”, Constitutional Law Society, NLUO (2023), available at <https://clsnuo.com/2022/08/01/examining-the-constitutionality-of-the-criminal-procedure-identification-act-2022/> (last visited 4 August 2026).

¹³Pulitzer Center, “As AI Took Over Policing in Delhi, Who Bore the Brunt?” (2023), available at <https://pulitzercenter.org/stories/ai-took-over-policing-delhi-who-bore-brunt> (last visited 4 August 2026); “Unquestioned Use of AI-Based Facial Recognition Technology”, *supra* note 2.

private member's bill and never taken up for substantive debate.¹⁴

A third strand addresses the law of evidence. Following the replacement of Section 65B of the Indian Evidence Act, 1872 by Section 63 of the BSA — which retained the dual-certification requirement of the earlier provision while adding a mandatory hash-value disclosure¹⁵ — scholars have begun to interrogate whether a provision drafted to authenticate conventional electronic records (call data, CCTV footage, e-mail) can meaningfully accommodate AI-generated or AI-enhanced content, where the “computer output” is itself the product of a probabilistic model rather than a mechanical reproduction of an underlying fact. A 2025 study specifically re-examines Section 63 in light of AI-generated content and concludes that existing standards of proof are inadequate to guarantee the impartiality and reliability that AI-produced evidence demands, recommending judicial and legislative reform to align evidentiary standards with the distinct epistemic status of algorithmically generated material.¹⁶

A fourth and more recent strand engages with India's emerging soft-law governance architecture. The MeitY India AI Governance Guidelines, unveiled on 5 November 2025 following a drafting process led by a subcommittee under Professor Balaraman Ravindran, adopt a deliberately “light-touch”, sector-agnostic approach built on seven guiding principles (“sutras”) and six governance pillars, explicitly declining to propose an omnibus AI statute in favour of working through and amending existing sectoral laws.¹⁷ Commentators broadly welcome the Guidelines' recognition of law-enforcement capacity-building as a governance priority, while cautioning that a non-binding, principles-based instrument cannot by itself discharge the state's constitutional obligation under Article 21 to prescribe a “procedure established by law” that is fair, just and reasonable before AI tools are deployed in a manner that curtails liberty.¹⁸

¹⁴Kavya Kurup, “A Comparative Analysis of AI Surveillance, Predictive Policing, Facial Recognition and Criminal Justice Laws in India and Europe”, Legal Service India, 27 May 2026, available at <https://www.legalserviceindia.com/Legal-Articles/artificial-intelligence-criminal-investigation-india-eu-laws/> (last visited 4 August 2026); Prasad, *supra* note 5.

¹⁵Bharatiya Sakshya Adhiniyam, 2023, s. 63(4); see “Section 63 BSA 2023: Admissibility of Electronic Evidence”, K.S. & K. (2026), available at <https://ksandk.com/litigation/section-63-bharatiya-sakshya-adhiniyam-2023/> (last visited 4 August 2026).

¹⁶“Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content” (2025), available at <https://zenodo.org/records/15872096> (last visited 4 August 2026).

¹⁷Ministry of Electronics and Information Technology, India AI Governance Guidelines (5 November 2025); Saikrishna & Associates, “Decoding the India AI Governance Guidelines” (2025), available at <https://www.saikrishnaassociates.com/decoding-the-india-ai-governance-guidelines/> (last visited 4 August 2026).

¹⁸MediaNama, “MeitY's AI Governance Guidelines on Liability and Innovation” (2025), available at

Taken together, the literature converges on a shared diagnosis — statutory fragmentation, absent purpose-limitation, weak retention and deletion safeguards, and an evidentiary regime not designed for algorithmically generated proof — but has not yet produced an integrated analysis that reads the CPIA, the BNSS/BSA trilogy, the DPDPA, the pending FRT Bill and the 2025 Governance Guidelines together against the Puttaswamy proportionality standard specifically in the context of criminal investigation. This paper seeks to fill that gap.

3. ANALYSIS AND DISCUSSION

3.1 The Constitutional Foundation: Privacy, Proportionality and Self-Incrimination

The constitutional starting point for any assessment of AI-enabled investigation is the recognition of informational privacy as a facet of the right to life and personal liberty under Article 21. In *Justice K.S. Puttaswamy v. Union of India*, a nine-judge bench unanimously held that privacy is intrinsic to Article 21 and to the freedoms in Part III generally, and prescribed a structured proportionality enquiry — legality, legitimate state aim, necessity (the least restrictive alternative) and a balancing of the measure's proportionality to the right infringed — as the test for any state action, including surveillance and biometric-collection measures, that intrudes upon it.¹⁹ Every AI-enabled investigative tool considered in this paper — automated facial matching against a police database, algorithmic risk-scoring for bail or preventive detention, AI-assisted forensic enhancement of images or audio — is, on its face, a form of surveillance or biometric processing that must clear this four-fold bar. The difficulty, examined further in Part 3.2, is that neither the CPIA nor the BNSS/BSA framework was drafted with this test explicitly in view, so that legality is frequently satisfied only in the thinnest formal sense (a statute or rule exists) without the necessity and proportionality limbs having been legislatively engaged at all.

A second, distinct constitutional concern is the guarantee against testimonial self-incrimination under Article 20(3). In *State of Bombay v. Kathi Kalu Oghad*, the Supreme Court drew a line between “testimonial” compulsion, which Article 20(3) prohibits, and the compelled production of “non-communicative” physical evidence such as fingerprints or handwriting exemplars, which it does not.²⁰ That distinction was refined in *Selvi v. State of Karnataka*,

<https://www.medianama.com/2025/11/223-meity-ai-governance-liability-regulation-innovation/> (last visited 4 August 2026).

¹⁹Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; the four-fold proportionality standard was further elaborated in the Aadhaar judgment, Justice K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.

²⁰State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.

where the Court held narco-analysis, polygraph examination and brain-electrical-activation profiling to be testimonial in substance — because they extract information from the subject's mental processes — and therefore impermissible without free and informed consent, even where the underlying technique is scientific rather than a traditional interrogation.²¹ The CPIA's definition of “measurements” extends to undefined “behavioural attributes” captured under Sections 53 and 53A of the erstwhile Code of Criminal Procedure (now BNSS Sections 51 and 52), a category that commentators warn could be read to sweep in AI-derived behavioural or psychological profiling of the sort *Selvi* treated as testimonial and therefore constitutionally protected, notwithstanding the CPIA's silence on the point.²²

3.2 The Statutory Architecture: CPIA, BNSS and the Retention Problem

The Criminal Procedure (Identification) Act, 2022 repealed the Identification of Prisoners Act, 1920 and substantially widened the categories of “measurements” that police and prison authorities may lawfully collect from arrested, convicted and even certain categories of detained persons, extending beyond fingerprints and footprints to iris and retina scans, biological samples and behavioural attributes, with the NCRB designated as the central repository.²³ Three features of the Act are of particular concern when read against the Puttaswamy standard. First, Section 4 permits retention of records for seventy-five years, and — through a proviso with retrospective effect — permits continued retention even where the person concerned is subsequently acquitted or discharged, subject only to a discretionary order of deletion by a court or magistrate; there is no default obligation to purge records upon acquittal.²⁴ Second, the Act permits inter-agency sharing and dissemination of biometric records without a defined regulatory framework governing onward transfer, storage security or purpose limitation, leaving these matters to executive Standard Operating Procedures issued outside the ordinary rule-making process. Third, and most significant for present purposes, the Act says nothing about the algorithmic processing of the measurements it authorises the State to collect — it regulates capture, not analysis — leaving CrPI's underlying facial-matching, iris-matching and DNA-matching algorithms entirely outside any statutory accuracy, bias-

²¹*Selvi v. State of Karnataka*, (2010) 7 SCC 263.

²²“The Viewpoint] Does the Criminal Procedure (Identification) Act, 2022 Impinge on the Privacy of Accused?”, Bar & Bench, 6 May 2022, available at <https://www.barandbench.com/view-point/the-viewpoint-does-the-criminal-procedure-identification-act-2022-impinge-on-the-privacy-of-accused> (last visited 4 August 2026).

²³Criminal Procedure (Identification) Act, 2022 (Act 11 of 2022), ss. 2(1)(b) and 4; Criminal Procedure (Identification) Rules, 2022.

²⁴“The Criminal Procedure (Identification) Act, 2022 and the Right to Privacy”, Lexology, 27 May 2022, available at <https://www.lexology.com/library/detail.aspx?g=b80efba0-72e4-4fc0-9e06-0f6b066e1b19> (last visited 4 August 2026).

testing or audit requirement.

The BNSS, which replaced the Code of Criminal Procedure, 1973 with effect from 1 July 2024, likewise modernised procedural provisions — for instance by permitting audio-video recording of search and seizure and electronic service of summons — without directly addressing AI-assisted identification or algorithmic risk assessment. The consequence is that CrPI and AFRS operate today on the strength of executive notification and the CPIA's general “measurements” power, rather than under any provision that specifically contemplates, and therefore specifically constrains, automated biometric matching. This is precisely the species of executive action — technically “lawful” in form but insufficiently anchored in a specific, foreseeable and proportionate statutory mandate — that the Delhi High Court petition and the pending Supreme Court protest-surveillance matter both put in issue.²⁵

3.3 The Data Protection Overlay: DPDPA, 2023 and its Law-Enforcement Exemption

The Digital Personal Data Protection Act, 2023 was, in principle, positioned to close some of the gaps identified above, by imposing purpose-limitation, notice, consent and data-minimisation obligations on any “data fiduciary” processing personal data, including biometric and facial data. The Digital Personal Data Protection Rules, 2025, notified on 14 November 2025 after an eighteen-month transition period running to May 2027, operationalised these obligations through detailed consent-notice, breach-reporting and data-principal-rights procedures.²⁶ However, Section 17(2) of the DPDPA exempts processing of personal data by, or on behalf of, government instrumentalities for purposes including “prevention, detection, investigation or prosecution of any offence” from most of the Act's substantive obligations, provided the processing is carried out in accordance with a law for the time being in force. This exemption is broadly drawn and does not, on its own terms, require the exempted processing to satisfy data-minimisation or purpose-specification requirements equivalent to those imposed on private fiduciaries, effectively leaving investigative AI processing to be governed by whatever safeguards — often minimal — exist in the underlying sectoral statute, such as the CPIA. The practical result is that the DPDPA's most protective provisions apply with full force to a private company's use of facial recognition for building access control, but apply only in attenuated form to the police's use of a materially similar algorithm for suspect identification — an asymmetry in obvious tension with the proportionality logic of *Puttaswamy*, under which state coercive power ordinarily calls for more, not less, procedural protection than private

²⁵Internet Freedom Foundation, *supra* note 8; Choudhury, *supra* note 10.

²⁶“The 2026 Guide to Facial Recognition and Privacy in India”, *supra* note 6.

commercial processing.

3.4 Evidentiary Challenges: Section 63 BSA and AI-Generated Proof

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 replaced Section 65B of the Indian Evidence Act, 1872 with effect from 1 July 2024, retaining the underlying architecture — an electronic record is admissible without production of the original device provided the conditions in the section are satisfied — while introducing a mandatory dual-certificate requirement (from the person in charge of the device and an independent expert) and, for the first time, requiring the certificate to disclose the record's hash value.²⁷ The Supreme Court had earlier clarified, under the predecessor provision, that the certificate requirement is mandatory wherever secondary electronic evidence is sought to be proved, subject to a narrow exception where the party is unable to secure the certificate for reasons beyond its control and the trial court permits production of the certificate at a later stage;²⁸ video and image records generated during investigation have separately been held to constitute “documents” rather than material objects, attracting the electronic-evidence regime rather than the ordinary rules for physical exhibits.²⁹

Section 63, however, was conceived to authenticate the *chain of custody and technical provenance* of an electronic record — that it was produced by a properly functioning device in the regular course of its use — not to test the *substantive reliability* of an inferential output generated by a probabilistic model. When Delhi Police tenders an AFRS-generated “match”, or when a forensic laboratory tenders an AI-enhanced version of degraded CCTV footage, or when an audio clip is subjected to AI-based speaker identification, the certificate contemplated by Section 63(4) can confirm that the computer or device operated regularly and produced the output in question — but it cannot, on its own terms, speak to the accuracy, error rate, training-data bias or confidence threshold of the underlying algorithm. A 2025 study on this precise question concludes that the current standards of proof are insufficiently calibrated to the distinct epistemic status of AI-generated content and recommends judicial and legislative reform to require disclosure of model accuracy, validation methodology and confidence scores as a precondition of admissibility, particularly given the emerging problem of deep-fake and AI-

²⁷Bharatiya Sakshya Adhiniyam, 2023, s. 63(1) and (4); see “Electronic Evidence Under the BSA, 2023”, iPleaders (2026), available at <https://blog.ipleaders.in/electronic-evidence-under-the-bsa-2023/> (last visited 4 August 2026).

²⁸Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (clarifying and partially modifying the position on the mandatory nature of the certificate requirement).

²⁹P. Gopalkrishnan v. State of Kerala, (2020) 9 SCC 161.

manipulated evidence being introduced into criminal proceedings.³⁰ Absent such reform, an accused faces the practical difficulty of contesting an AI-derived identification without any statutory right to obtain the algorithm's error-rate data, source code or training methodology, in circumstances where such material is typically treated by vendors and by the State as proprietary or classified — a due-process asymmetry with few analogues in conventional forensic evidence, where cross-examination of a human expert witness remains available as a check on reliability.

3.5 Ethical Concerns: Bias, Opacity and Function Creep

Beyond formal legality, three ethical concerns recur across the literature and the reported experience of AFRS deployment. The first is *algorithmic bias*: facial recognition systems trained predominantly on datasets that under-represent particular skin tones, genders and age groups exhibit materially higher false-positive rates for those groups, a pattern documented internationally and mirrored in the composition of those wrongly implicated in the Delhi riots prosecutions.³¹ Because CrPI and AFRS operate as investigative-lead generators rather than as evidence subjected to adversarial testing at the point of generation, this bias risks translating directly into disproportionate rates of arrest, detention and prosecution of already marginalised communities, without any statutory requirement for periodic, independent bias auditing of the underlying model.

The second concern is *opacity or the “black box” problem*: machine-learning classifiers of the kind used in facial and voice matching typically cannot furnish a human-intelligible explanation of why a particular match was returned, which sits uneasily with the reasoned-decision requirements embedded throughout Indian criminal procedure, from the recording of grounds of arrest to the requirement of a reasoned judgment. The MeitY India AI Governance Guidelines expressly acknowledge this difficulty, identifying the opacity of AI decision-making in sensitive domains including law enforcement as a governance risk requiring “understandable by design” systems and clear audit mechanisms, though the Guidelines stop short of prescribing binding explainability standards for investigative AI.³²

The third concern is *function creep*: tools justified publicly by reference to serious or organised crime have, in practice, migrated toward broader surveillance uses, most visibly in the

³⁰“Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam”, supra note 15.

³¹“Unquestioned Use of AI-Based Facial Recognition Technology”, supra note 2.

³²Ministry of Electronics and Information Technology, India AI Governance Guidelines (2025); Vision IAS, “India AI Governance Guidelines” (2026), available at <https://visionias.in/current-affairs/monthly-magazine/2025-12-23/polity-and-governance/india-ai-governance-guidelines> (last visited 4 August 2026).

deployment of facial recognition at sites of public protest — the subject of the Article 32 petition described in Part 1 — which implicates not merely privacy under Article 21 but the freedoms of speech, assembly and movement under Article 19(1)(a), (b) and (d). Once a national biometric-matching infrastructure of CrPI's scale exists, the marginal institutional cost of repurposing it for a use beyond its original justification is low, while the constitutional harm of doing so — particularly the chilling effect of identifiable surveillance on political expression — is high, a dynamic the current legal framework does not squarely confront because no statute defines, in advance, the permissible universe of purposes for which CrPI-linked systems may be queried.

3.6 The Soft-Law Response: MeitY's 2025 Governance Guidelines

The most recent institutional response is the MeitY India AI Governance Guidelines, unveiled on 5 November 2025 under the IndiaAI Mission after a drafting process led by a subcommittee under Professor Balaraman Ravindran and informed by more than 2,500 public submissions on an earlier January 2025 draft.³³ The Guidelines articulate seven guiding “sutras” — trust, people-first design, innovation over restraint, fairness and equity, accountability, understandability by design, and safety, resilience and sustainability — and propose an institutional architecture comprising an AI Governance Group, a supporting Technology and Policy Expert Committee, and a dedicated AI Safety Institute, alongside a specific recommendation to build the capacity of law-enforcement agencies, including the Enforcement Directorate, the Central Bureau of Investigation and police cyber-crime units, to detect and respond to AI-related crime.³⁴ Significantly, the Guidelines deliberately eschew a horizontal, binding AI statute in favour of “closing legal gaps” through targeted amendments to existing sectoral laws — a philosophy IT Secretary S. Krishnan articulated at the launch as a choice to “rely on existing laws and frameworks rather than rush into new legislation.”³⁵

This approach has evident advantages of flexibility and speed, but it also means that, as of the date of this paper, none of the specific gaps identified in Parts 3.2 to 3.5 — the CPIA's silence on algorithmic processing, the DPDPA's broad law-enforcement exemption, Section 63 BSA's inadequacy for AI-generated evidence, and the absence of any bias-audit or explainability mandate for investigative AI — has been closed by binding legislative amendment. The Guidelines are, on their own terms, a policy framework addressed to future law-making rather

³³Saikrishna & Associates, *supra* note 17; MediaNama, *supra* note 18.

³⁴MediaNama, *supra* note 18.

³⁵“Decoding the India AI Governance Guidelines”, *supra* note 17.

than a source of enforceable rights for a person whose liberty is presently at stake in an AI-assisted investigation, and they cannot substitute for the “procedure established by law” that Article 21 demands before the coercive power of the State is exercised.

4. FINDINGS

(1) India's AI-enabled criminal investigation apparatus, exemplified by the NCRB's CrPI platform and the Delhi Police's AFRS, has scaled nationally without a dedicated statute governing the algorithmic processing of biometric data, leaving the CPIA's undifferentiated “measurements” power as the principal — and inadequate — statutory foundation.

(2) The CPIA fails each limb of the Puttaswamy proportionality test in material respects: its seventy-five-year and functionally indefinite retention scheme is disproportionate to its stated investigative purpose; its inter-agency data-sharing provisions lack a defined regulatory framework; and its delegation of core safeguards to executive Standard Operating Procedures raises an unresolved excessive-delegation concern.

(3) The Digital Personal Data Protection Act, 2023, notwithstanding its Rules of 2025, provides materially weaker protection for AI-driven biometric processing conducted by law-enforcement agencies than for equivalent private-sector processing, owing to the broad law-enforcement exemption in Section 17(2), producing an asymmetry inconsistent with the heightened scrutiny ordinarily warranted by coercive state action.

(4) Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 was designed to authenticate the technical provenance of electronic records and is doctrinally ill-suited, without judicial or legislative gloss, to test the substantive reliability of AI-generated or AI-enhanced investigative material, leaving accused persons without a clear statutory mechanism to interrogate algorithmic error rates, bias or training methodology.

(5) Documented deployment of AFRS in the Delhi riots prosecutions demonstrates real-world harm from unaudited facial recognition, including a high rate of subsequent acquittal or discharge, evidencing that the bias and opacity concerns raised in the literature are not merely speculative.

(6) The pending Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 remains the only legislative proposal squarely addressing facial recognition in policing, and its continued non-passage leaves the single most invasive current AI investigative tool without dedicated statutory regulation.

(7) The MeitY India AI Governance Guidelines of November 2025 constitute a significant policy development and correctly identify law-enforcement capacity-building, explainability and bias mitigation as governance priorities, but as non-binding soft law they cannot discharge the State's Article 21 obligation to act only through fair, just and reasonable procedure established by law.

(8) Ongoing litigation before the Delhi High Court and the Supreme Court's pending consideration of facial recognition deployment at protest sites indicate that the judiciary, rather than the legislature, is currently the primary forum in which the constitutional limits of AI-enabled investigation are being tested — an inversion of the ordinarily preferable sequence in which Parliament first legislates proportionate safeguards.

5. RECOMMENDATIONS

1. Enact a dedicated algorithmic policing statute. Parliament should prioritise and pass a comprehensive Facial Recognition and Algorithmic Policing Act, building on but substantially strengthening the pending 2023 private member's Bill, to specifically regulate the acquisition, deployment and audit of facial recognition, predictive-policing and other AI investigative tools, rather than continuing to rely on the CPIA's generic “measurements” power.

2. Introduce judicial pre-authorisation for high-intrusion AI tools. Deployment of real-time or retrospective facial recognition against public spaces, and any AI-based risk-scoring used to inform arrest, bail or preventive-detention decisions, should require prior judicial or magisterial authorisation on a showing of reasonable suspicion tied to a specific, identified offence, mirroring the safeguards that already govern interception of communications under Section 5(2) of the Telegraph Act and Section 69 of the Information Technology Act, 2000.

3. Mandate periodic algorithmic audit and bias testing. Any AI system used in criminal investigation, including CrPI's constituent matching algorithms, should be subject to

independent, periodic accuracy and bias auditing by a body such as the proposed AI Safety Institute, with disaggregated error-rate disclosure by demographic category and mandatory suspension of deployment where error rates exceed a prescribed threshold.

4. Amend Section 63 BSA (or introduce a dedicated provision) for AI-generated evidence.

The certification regime under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 should be supplemented by a specific sub-provision or judicial guideline requiring disclosure of the algorithm's validated accuracy rate, confidence score for the specific output tendered, and a summary of training-data provenance, as a precondition to the admissibility of AI-generated or AI-enhanced evidence, building on the reform proposals already advanced in the literature.

5. Narrow the DPDPA's law-enforcement exemption. Section 17(2) of the Digital Personal Data Protection Act, 2023 should be amended, or implementing rules issued, to require that law-enforcement processing of biometric and facial data remain subject to purpose limitation, necessity and proportionate retention safeguards materially equivalent to those applicable to private data fiduciaries, consistent with the reasoning in Puttaswamy that state coercive power warrants heightened, not diminished, protection.

6. Institute a statutory exclusionary rule. Evidence obtained through AI investigative tools deployed in violation of statutory or constitutional safeguards — including facial recognition used without judicial authorisation, or biometric data retained beyond the statutorily prescribed period — should be rendered presumptively inadmissible, to create a meaningful compliance incentive that the current framework, which imposes no direct evidentiary consequence for procedural non-compliance, presently lacks.

7. Codify a right to algorithmic disclosure for the accused. An accused person against whom AI-generated identification or profiling evidence is tendered should have a statutory right, enforceable at the pre-trial stage, to obtain the algorithm's documented error rate, validation methodology and the specific confidence score generated in their case, subject to reasonable safeguards for trade-secret protection that do not defeat meaningful cross-examination.

8. Translate the MeitY Guidelines' law-enforcement recommendations into binding rules.

The capacity-building, explainability and incident-reporting recommendations directed at law-enforcement agencies in the November 2025 India AI Governance Guidelines should be

operationalised through binding rules issued under the CPIA, the BNSS or a new statute, rather than left as aspirational guidance, so that the proposed AI Governance Group's oversight extends in practice, and not merely in principle, to criminal investigation.

6. CONCLUSION

Artificial intelligence offers Indian law enforcement genuine and legitimate investigative advantages — faster identification of suspects, more efficient forensic analysis and, if properly governed, the capacity to solve cases that would otherwise remain intractable. The Government's stated ambition of a “future-ready” justice system is not, in itself, constitutionally objectionable. What this paper has sought to demonstrate is that the manner and pace of that ambition's implementation have significantly outrun the constitutional and statutory safeguards that must accompany any exercise of coercive state power. The CPIA, drafted before the current generation of AI-driven biometric matching was operationally mature, regulates the capture of biometric data but not its algorithmic analysis; the DPDPA's law-enforcement exemption inverts the proportionality logic of *Puttaswamy* by protecting private commercial data processing more robustly than state investigative processing; and Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, though a meaningful modernisation of the electronic-evidence regime, was not built to test the distinct reliability problems that AI-generated proof presents. The documented consequences — most starkly, the high rate of acquittal and discharge following AFRS-assisted identification in the Delhi riots prosecutions — are not abstract or theoretical, but a lived demonstration of the costs of deploying algorithmic tools ahead of the legal framework needed to discipline them.

The judiciary has begun, through the pending Delhi High Court challenge to the CPIA and the Supreme Court's forthcoming consideration of facial recognition at protest sites, to test these tools against constitutional first principles. But litigation is, by its nature, retrospective and piecemeal, resolving the legality of a challenged practice only after it has already been deployed and, frequently, already caused harm. The more durable and constitutionally appropriate path is legislative: a dedicated statute governing algorithmic policing, judicial pre-authorisation for high-intrusion tools, mandatory bias auditing, a recalibrated evidentiary standard for AI-generated proof, and a narrowed law-enforcement exemption under the DPDPA. The MeitY India AI Governance Guidelines of November 2025 correctly diagnose many of these problems and offer a promising institutional architecture — the AI Governance

Group, the Technology and Policy Expert Committee and the AI Safety Institute — through which reform could be channelled. Whether that architecture in fact translates aspiration into binding, enforceable safeguards for criminal investigation specifically, rather than for the AI economy more generally, will determine whether India's justice system becomes not merely “future-ready” in name, but genuinely fair, accountable and constitutionally sound in the exercise of its newest and most powerful investigative tools.

REFERENCES

Constitution and Statutes

1. *The Constitution of India, 1950, arts. 14, 19, 20(3), 21, 32, 226.*
2. *The Identification of Prisoners Act, 1920 (repealed).*
3. *The Indian Evidence Act, 1872 (repealed w.e.f. 1 July 2024), s. 65B.*
4. *The Information Technology Act, 2000, ss. 69, 69B.*
5. *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.*
6. *The Criminal Procedure (Identification) Act, 2022 (Act 11 of 2022).*
7. *The Criminal Procedure (Identification) Rules, 2022.*
8. *The Bharatiya Nyaya Sanhita, 2023.*
9. *The Bharatiya Nagarik Suraksha Sanhita, 2023.*
10. *The Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63.*
11. *The Digital Personal Data Protection Act, 2023, s. 17(2).*
12. *The Digital Personal Data Protection Rules, 2025 (notified 14 November 2025).*
13. *Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 (Private Member's Bill, pending).*

B. Cases

14. *Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
15. *Justice K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.*
16. *Selvi v. State of Karnataka, (2010) 7 SCC 263.*
17. *State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.*
18. *State of U.P. v. Ram Babu Misra, AIR 1980 SC 791.*
19. *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.*
20. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.*

21. *P. Gopalkrishnan v. State of Kerala*, (2020) 9 SCC 161.
22. *In re: The Delhi Laws Act, 1912*, AIR 1951 SC 332.
23. *Internet Freedom Foundation v. Union of India*, W.P. (Crl.) Diary No. 53491 of 2023 (SC).
24. Writ petition challenging the Criminal Procedure (Identification) Act, 2022, pending before the Delhi High Court (2026).
25. Writ petition on facial recognition and AI surveillance at protest sites, pending before the Supreme Court under Article 32 (2026).

C. Books, Articles, Reports and Online Sources

26. “Unquestioned Use of AI-Based Facial Recognition Technology in Criminal Investigations: Delhi Riots Lessons on Rights and Reliability”, *Eng. Proc.* 2026, 143(1), 17, DOI: 10.3390/engproc2026143017.
27. Kavya Kurup, “A Comparative Analysis of AI Surveillance, Predictive Policing, Facial Recognition and Criminal Justice Laws in India and Europe”, *Legal Service India*, 27 May 2026.
28. Oxford Institute of Technology and Justice, “India: Increasing Use of AI Across the Justice System” (2026), available at <https://www.techandjustice.bsg.ox.ac.uk/research/india>.
29. “Facial Recognition Evidence: Legal and Ethical Limits”, *Free Law* (2025), available at <https://www.freelaw.in/legalarticles/Facial-Recognition-Evidence-Legal-and-Ethical-Limits->.
30. “The 2026 Guide to Facial Recognition and Privacy in India”, *Hyperverge* (2026), available at <https://hyperverge.co/blog/facial-recognition-privacy-india/>.
31. “Facial Recognition in Indian Criminal Investigations”, *Budding Forensic Expert* (2026), available at <https://www.buddingforensicexpert.in/2026/07/facial-recognition-in-indian-criminal-investigation.html>.
32. Anmol Prasad, “Why India Must Pass the Pending Facial Recognition Technology Bill”, *Bar & Bench*, 4 April 2026.
33. Tarun Choudhury, “Facial Recognition Technology at Protest Sites: Supreme Court to Examine AI Surveillance, Privacy and Protest Rights”, *Legal Service India*, 28 July 2026.
34. Internet Freedom Foundation, “Supreme Court Dismisses Challenge to the Criminal Procedure (Identification) Act, 2022” (2024), available at <https://internetfreedom.in>.

35. *Internet Freedom Foundation, "Delhi HC Issues Notice in the Constitutional Challenge to the Criminal Procedure (Identification) Act, 2022 and Rules Thereunder" (2026), available at <https://internetfreedom.in>.*
36. *"Editorial Note: Scrutinising the Criminal Procedure (Identification) Act, 2022", NUJS Law Review (2022).*
37. *"Questioning the Feasibility of the Criminal Procedure (Identification) Act, 2022", SCC OnLine Blog, 31 May 2022.*
38. *"Examining the Constitutionality of the Criminal Procedure (Identification) Act, 2022", Constitutional Law Society, NLUO (2023).*
39. *"[The Viewpoint] Does the Criminal Procedure (Identification) Act, 2022 Impinge on the Privacy of Accused?", Bar & Bench, 6 May 2022.*
40. *Pulitzer Center, "As AI Took Over Policing in Delhi, Who Bore the Brunt?" (2023), available at <https://pulitzercenter.org/stories/ai-took-over-policing-delhi-who-bore-brunt>.*
41. *"Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content" (2025), available at <https://zenodo.org/records/15872096>.*
42. *"Electronic Evidence Under the BSA, 2023", iPleaders (2026), available at <https://blog.ipleaders.in/electronic-evidence-under-the-bsa-2023/>.*
43. *"Section 63 BSA 2023: Admissibility of Electronic Evidence", K.S. & K. (2026), available at <https://ksandk.com/litigation/section-63-bharatiya-sakshya-adhiniyam-2023/>.*
44. *Ministry of Electronics and Information Technology, India AI Governance Guidelines (5 November 2025), Government of India.*
45. *Saikrishna & Associates, "Decoding the India AI Governance Guidelines" (2025), available at <https://www.saikrishnaassociates.com/decoding-the-india-ai-governance-guidelines/>.*
46. *MediaNama, "MeitY's AI Governance Guidelines on Liability and Innovation" (2025), available at <https://www.medianama.com/2025/11/223-meity-ai-governance-liability-regulation-innovation/>.*
47. *Vision IAS, "India AI Governance Guidelines", Current Affairs (2026), available at <https://visionias.in/current-affairs/monthly-magazine/2025-12-23/polity-and-governance/india-ai-governance-guidelines>.*

48. *“Artificial Intelligence in the Criminal Justice System: Opportunities, Challenges, and Legal Imperatives”*, Zenodo (1 February 2026), available at <https://zenodo.org/records/18826639>.
49. AI Knowledge Consortium, *“Neural Network: January Edition”* Newsletter (2025), available at <https://aiknowledgeconsortium.substack.com/p/neural-network-january-edition>.

