INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE: A SOCIO-LEGAL AND COMPARATIVE ANALYSIS OF INDIA AND THE EUROPEAN UNION

AUTHORED BY - RUCHI HITESH PATEL,
SNEHA NARENDRA BHANUSHALI & JIGISHA SURESH PATEL

1. Abstract

Artificial intelligence has moved from an auxiliary tool to a structural feature of contemporary criminal justice administration, reshaping policing, evidence-gathering, risk assessment, and even adjudicatory support. This paper undertakes a socio-legal and comparative examination of how India and the European Union have responded to this transformation. It situates the discussion within a conceptual framework connecting due process, the rule of law, and algorithmic accountability, before mapping the concrete uses of AI in criminal justice, from predictive policing and facial recognition to automated evidence analysis. The Indian framework — comprising the Bharatiya Nagarik Suraksha Sanhita 2023, the Digital Personal Data Protection Act 2023, and constitutional privacy jurisprudence following Puttaswamy — is examined against the European Union's Artificial Intelligence Act and Law Enforcement Directive, alongside the Court of Justice's jurisprudence in Ligue des droits humains. The comparative analysis reveals that while both jurisdictions share underlying human rights commitments, they diverge sharply in regulatory maturity, with the EU operating a codified risk-based regime and India relying on fragmented procedural provisions and judicially derived safeguards. The paper concludes with recommendations for India, arguing for dedicated legislation governing algorithmic policing tools, mandatory human oversight, and independent audit mechanisms to reconcile technological efficiency with constitutional due process.

2. Keywords

Artificial Intelligence; Criminal Justice; Facial Recognition; Predictive Policing; Data Protection; Due Process; Comparative Law; India; European Union.

ISSN: 2582-6433

3. Introduction

Artificial intelligence ("AI") has moved from the margins of criminal justice administration to its operational core. Police departments increasingly deploy predictive analytics to allocate patrol resources, facial recognition systems to identify suspects, and automated tools to sift through digital evidence, while judicial and correctional institutions experiment with risk-assessment algorithms for bail and sentencing. This shift promises efficiency gains in systems long burdened by case backlogs and resource constraints, but it also imports the well-documented risks of algorithmic opacity, embedded bias, and diminished human oversight into a domain where the state's coercive power over the individual is at its most direct.

The regulatory responses to this transformation have varied sharply across jurisdictions. The European Union has enacted the world's first comprehensive, horizontally applicable law on artificial intelligence, the Artificial Intelligence Act, which designates most law-enforcement uses of AI as inherently high-risk and subjects them to a codified regime of pre-deployment assessment, documentation, and human oversight.[1] This sits atop an already mature data-protection architecture built around the General Data Protection Regulation and, specifically for policing and criminal justice, the Law Enforcement Directive. India, by contrast, has no dedicated statute governing artificial intelligence. Its criminal procedure has nonetheless been substantially rewritten through the Bharatiya Nagarik Suraksha Sanhita 2023,[2] which embeds technology and forensic science at the heart of investigation, while the Digital Personal Data Protection Act 2023 supplies India's first general data-protection statute[3] — one that, notably, exempts most law-enforcement processing from the Act's core obligations.

This divergence is not merely technical; it reflects contrasting constitutional and institutional trajectories. The European Union's approach is anticipatory and rights-driven, built on decades of jurisprudence from the Court of Justice and the European Court of Human Rights. India's approach is comparatively reactive, characterised by rapid operational adoption of AI-enabled policing tools at the state level ahead of any dedicated legal architecture, leaving courts and civil society organisations to test the legality of specific deployments after the fact.

This paper undertakes a socio-legal and comparative analysis of these two frameworks. It begins by situating the discussion within a conceptual framework connecting the rule of law, due process, and algorithmic accountability. It then surveys the concrete forms AI has taken

[1]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L1689.
[2]Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023).
[3]Digital Personal Data Protection Act 2023 (Act 22 of 2023).

ISSN: 2582-6433

within criminal justice administration, before examining the Indian and European Union legal frameworks in turn. A comparative socio-legal analysis follows, focusing on regulatory philosophy, oversight mechanisms, and the demographic effects of algorithmic policing. The paper closes by examining the implications for human rights — privacy, equality, and due process — before offering recommendations for India's future legal architecture.

4. Conceptual and Theoretical Framework

For the purposes of this paper, 'artificial intelligence' refers to applied, narrow AI systems — principally machine-learning classifiers and pattern-recognition tools — used to support or automate specific criminal justice functions, rather than any speculative general intelligence. Three theoretical anchors structure the analysis that follows.

The first is the rule of law in its Diceyan, formal sense: state action, including the deployment of technological tools against individuals, must rest on clear, prospective, and publicly accessible legal authority. An algorithmic tool operated under an internal administrative circular or a cabinet approval, rather than a statute, sits uneasily with this requirement, however efficient it may be in operational terms.

The second anchor is due process, understood in both its procedural sense — notice, an opportunity to be heard, and a right to contest adverse determinations — and its substantive sense, which asks whether the underlying rule or practice is itself fair and non-arbitrary. Automated decision-making complicates both dimensions: procedurally, a person may not know that an algorithm, rather than a human officer, generated the suspicion against them; substantively, an algorithm trained on historically skewed policing data can reproduce and entrench the very biases due process is meant to guard against.

The third anchor is the proportionality principle, the dominant analytical tool for testing state intrusions into fundamental rights across both jurisdictions studied here. In India, the Supreme Court in Justice K.S. Puttaswamy v Union of India read a threefold test into Article 21 of the Constitution: any restriction on the right to privacy must have a legal basis, must pursue a legitimate state aim, and must be proportionate to that aim.[4] The Court of Justice of the European Union applies a structurally similar test under the Charter of Fundamental Rights, calibrated to the severity of the interference and the reliability of the technology used.

A recurring theme across both frameworks is the so-called 'black box' problem: the opacity

[4]Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1, paras 310, 325 (Chandrachud J), read together with the concurring opinions applying the threefold test of legality, legitimate aim, and proportionality to restrictions on the right to privacy.

ISSN: 2582-6433

that characterises machine-learning systems, particularly those capable of self-modification, makes it difficult for affected individuals to understand, and therefore to meaningfully contest, an adverse outcome. The Court of Justice addressed this directly in Ligue des droits humains, holding that self-learning systems capable of altering their own assessment criteria without human review are especially difficult to reconcile with the right to an effective remedy.[5] This concern underlies much of the regulatory design examined below: whether through the European Union's risk-based classification or through demands for statutory anchoring and human oversight in the Indian context, the object is the same — to keep a human, and a reviewable legal standard, in the loop wherever AI mediates the coercive power of the state.

5. AI and the Transformation of Criminal Justice

AI-enabled tools have entered criminal justice administration through several distinct channels, each carrying its own rights implications.

Predictive policing and hotspot mapping represent the earliest and most widespread application. Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS), developed with the Indian Space Research Organisation from 2015, draws on emergency helpline data and historical crime records to generate real-time crime 'hotspots' and suspect-behaviour patterns.[6] Comparable systems have proliferated across Indian states: the Punjab Artificial Intelligence System, Uttar Pradesh's Trinetra and CrimeGPT, Telangana's TSCOP, and Rajasthan's Artificial-Intelligence Based Human Efface Detection system illustrate a rapid, state-by-state adoption of algorithmic policing tools, largely without a common regulatory template.

Biometric identification, principally facial recognition technology, forms the second major category. The National Crime Records Bureau's proposed Automated Facial Recognition System is intended to match images captured in the field or from CCTV feeds against a centralised database drawing on passport, prison, and other government records. Investigative reporting has documented instances in Delhi where individuals were arrested on the strength of a facial-recognition match with little independent corroboration.[7]

A third category concerns evidence processing and forensic analytics: the increasing use of digital forensic tools to process seized devices, automate transcription, and support electronic evidence chains, an area the Indian legislature has itself prioritised through the mandatory-

[5]Case C-817/19 Ligue des droits humains v Conseil des ministres ECLI:EU:C:2022:491, paras 194–195.
[6]SFLC.in, 'Tracing the Rise of Predictive Policing in India' (2026); see also Vidhi Centre for Legal Policy, 'India's Tryst With Predictive Policing'.
[7]The Wire and Pulitzer Center, 'As AI Took Over Policing in Delhi, Who Bore the Brunt?' (2025).

ISSN: 2582-6433

forensics provisions discussed below.

A fourth category, prominent in the European Union framework, comprises risk-assessment and evidence-reliability tools used directly within judicial or quasi-judicial processes: systems assessing an individual's likelihood of reoffending or of becoming a victim of crime, polygraph-style tools, and systems evaluating the reliability of evidence during investigation or prosecution. The Artificial Intelligence Act treats each of these as presumptively high-risk precisely because of their direct bearing on liberty and the presumption of innocence.[8]

The common thread across these categories is a shift in the locus of discretion. Decisions once made by an investigating officer or a magistrate, subject to the ordinary safeguards of accountability attaching to identifiable human decision-makers, are increasingly pre-structured, if not effectively made, by a statistical model whose internal logic is rarely disclosed to the affected individual, defence counsel, or even the court. This transformation is not inherently objectionable — AI tools can, in principle, reduce arbitrary and biased human decision-making as much as replicate it — but it fundamentally changes what 'due process' must guarantee: not merely a fair hearing before a human decision-maker, but meaningful information about, and a genuine opportunity to contest, the algorithmic process that generated the suspicion, the risk score, or the evidentiary inference in the first place. The same infrastructure that traced thousands of missing children in a Delhi High Court–sanctioned pilot can, without adequate safeguards, misidentify an innocent adult as a criminal suspect; the remainder of this paper is concerned with how each jurisdiction's legal framework mediates precisely this trade-off.

6. Indian Legal Framework

India has no dedicated statute governing artificial intelligence. Instead, the legal architecture bearing on AI in criminal justice is assembled from constitutional doctrine, general criminal procedure, evidence law, and a recently enacted data-protection statute.

The constitutional foundation rests on Article 21's guarantee of life and personal liberty. In K.S. Puttaswamy, the Supreme Court unanimously recognised privacy as intrinsic to Article 21 and read into it a threefold test for any state intrusion: legality (a valid law authorising the action), legitimate aim, and proportionality.[9] This test has become the default constitutional lens through which the legality of any AI-enabled surveillance or identification tool must be assessed, even though the Court has not yet applied it directly to a specific facial-recognition

[8]Artificial Intelligence Act (n 1) Annex III, paras 6–8.
[9]Constitution of India 1950, art 21; Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

or predictive-policing deployment.

At the level of ordinary legislation, the Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS), which replaced the Code of Criminal Procedure 1973 with effect from 1 July 2024, embeds technology at multiple stages of the investigative process. Section 105 mandates audio-video recording of search and seizure proceedings,[10] a requirement courts have already treated as substantive rather than merely directory: at least one High Court has granted bail partly because the prosecution failed to demonstrate compliance with the videography requirement. Section 176(3) makes forensic investigation mandatory for offences punishable with seven years' imprisonment or more, requiring a forensic expert to visit the crime scene and collect evidence under videographic record.[11] The statute further permits electronic filing of first information reports, video-conferenced witness examination, and, under section 530, conduct of trials, inquiries, and proceedings in electronic mode generally. Read alongside the Bharatiya Sakshya Adhiniyam 2023, which broadened the definitional scope of electronic and digital records for admissibility purposes, the BNSS reflects a legislative embrace of technology as a tool of criminal procedure — but one focused on documentation and evidentiary integrity rather than on regulating the predictive or biometric-identification tools discussed above.

The Digital Personal Data Protection Act 2023 (DPDP Act) is India's first comprehensive data-protection statute, but its application to law-enforcement AI is markedly narrower than its European counterpart. Section 17(1)(c) exempts the processing of personal data from most of the Act's core obligations — including consent and notice requirements — where such processing is in the interest of the prevention, detection, investigation, or prosecution of any offence.[12] Unlike the position under comparable overseas frameworks, this exemption is not textually confined to processing by a defined class of 'competent authorities' nor conditioned on independent oversight, leaving considerable latitude for law-enforcement agencies deploying AI-enabled surveillance tools.

The most significant regulatory gap concerns biometric identification technology specifically. The National Crime Records Bureau's Automated Facial Recognition System rests not on statute but on a 2009 cabinet notification approving the Bureau's modernisation mandate, invoked to justify a 2019 Request for Proposal — later withdrawn and reissued in substantially similar form — for a nationwide facial-recognition database.[13] Digital rights organisations have

[10]Bharatiya Nagarik Suraksha Sanhita 2023, s 105.
[11]Bharatiya Nagarik Suraksha Sanhita 2023, s 176(3).
[12]Digital Personal Data Protection Act 2023, s 17(1)(c).
[13]National Crime Records Bureau, Request for Proposal for National Automated Facial Recognition System (2019, revised 2020).

ISSN: 2582-6433

argued that this notification cannot satisfy the 'law' requirement of the Puttaswamy test, since a cabinet approval is neither a statute nor a rule made under statutory delegation, and offers no defined safeguards, retention limits, or independent oversight mechanism comparable to those found in the EU framework.[14]

Judicial engagement with AI-specific tools has so far been narrow and largely permissive. The Delhi High Court's order in Sadhan Haldar v State (NCT of Delhi) authorised use of an automated facial-recognition trial specifically for tracing missing children, a purpose-limited authorisation that has nonetheless been cited more broadly to lend legitimacy to facial-recognition deployment generally.[15] No Indian constitutional court has yet ruled squarely on the legality of predictive-policing software, risk-assessment tools, or general-purpose facial recognition used for ordinary criminal investigation, leaving the field to operate largely outside curial scrutiny.

7. European Union Legal Framework

The European Union's regulatory architecture for AI in criminal justice is considerably more layered and codified than India's, resting on four connected instruments.

At the level of primary law, the Charter of Fundamental Rights of the European Union guarantees respect for private life and the protection of personal data as distinct fundamental rights.[16] These Charter guarantees inform the interpretation of all secondary legislation discussed below and supply the standard against which the Court of Justice tests specific AI deployments.

The General Data Protection Regulation governs personal-data processing generally but expressly excludes processing by competent authorities for law-enforcement purposes from its scope.[17] That gap is filled by the Law Enforcement Directive, the first horizontally binding EU instrument specifically regulating personal-data processing by police and criminal justice authorities.[18] The Directive applies wherever a competent authority processes data for the prevention, investigation, detection, or prosecution of criminal offences, and imposes obligations tailored to that context: data-protection-by-design requirements, mandatory

[14]Internet Freedom Foundation, Legal Notice to the National Crime Records Bureau (2019); Panoptic, 'NCRB's National Automated Facial Recognition System' (case study).
[15]Sadhan Haldar v State (NCT of Delhi) (Delhi High Court, order of 2018 authorising a facial-recognition trial for tracing missing children).
[16]Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7–8.
[17]Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 2(2)(d).
[18]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive) [2016] OJ L119/89, arts 1, 11, 25.

ISSN: 2582-6433

logging of processing operations, and, most significantly for AI purposes, a restriction on automated individual decision-making that requires adverse decisions based solely on automated processing to be subject to appropriate safeguards, including a right to obtain human intervention.

The most recent and most consequential addition is the Artificial Intelligence Act, adopted in 2024 as the world's first comprehensive, cross-sectoral AI statute. The Act adopts a risk-based classification: systems posing 'unacceptable risk' are prohibited outright, including AI systems that create or expand facial-recognition databases through untargeted scraping of images from the internet or CCTV footage, and biometric-categorisation systems that infer race, political opinion, trade-union membership, religion, or sexual orientation from biometric data.[19] A defined list of law-enforcement applications is classified as 'high-risk' by default: tools assessing the risk of an individual becoming a victim of crime or reoffending, polygraphs and similar tools, systems evaluating the reliability of evidence in investigation or prosecution, and biometric identification and categorisation systems generally. High-risk classification triggers a demanding compliance regime: providers must maintain technical documentation, conduct risk assessments, ensure human oversight and a defined accuracy threshold, and log operations, while deployers face registration, monitoring, and incident-reporting duties, with serious breaches attracting fines of up to six per cent of global turnover.[20] 'Real-time' remote biometric identification in publicly accessible spaces for law-enforcement purposes is not banned outright but is subject to some of the Act's tightest restrictions, permitted only in narrowly defined circumstances and generally subject to prior judicial or independent administrative authorisation.[21]

The Court of Justice of the European Union has already begun to give concrete content to these statutory standards. In Ligue des droits humains, decided under the earlier Passenger Name Record Directive rather than the Artificial Intelligence Act itself, the Court upheld the validity of an EU-wide automated passenger-screening regime but imposed significant limits on its operation. It held that the system could not employ self-learning artificial intelligence capable of modifying its own assessment criteria without human review, since the resulting opacity would deprive affected individuals of an effective remedy. The Court further linked the severity of a rights interference to the technology's reliability, holding that a higher false-positive rate corresponds to a more serious interference with fundamental rights, and flagged the

[19]Artificial Intelligence Act (n 1) art 5.
[20]Artificial Intelligence Act (n 1) arts 11, 19 and Annex IV; art 99 (penalties).
[21]Artificial Intelligence Act (n 1) art 5(1)(h) and related recitals.

ISSN: 2582-6433

discrimination risks inherent in automated profiling notwithstanding the Directive's own prohibition on using protected characteristics as assessment criteria. Although the case predates the Artificial Intelligence Act, its reasoning — mandatory human review of self-learning systems, and reliability-linked proportionality — anticipates and reinforces the Act's own design.

Taken together, the European Union framework exhibits three structural features largely absent from the Indian position: an unambiguous statutory basis for every category of AI use in law enforcement, defined ex ante compliance obligations attaching before deployment rather than being tested only after harm has occurred, and an active constitutional court willing to adjudicate the legality of specific automated-processing regimes.

8. Comparative Socio-Legal Analysis

Placed side by side, the Indian and European Union frameworks diverge along four principal axes.

The first is regulatory philosophy. The European Union operates an anticipatory, codified model: the Artificial Intelligence Act and the Law Enforcement Directive define categories of permissible and prohibited use before deployment, backed by binding compliance obligations and significant financial penalties. India's approach is reactive and procedural: the BNSS and Bharatiya Sakshya Adhiniyam regulate the documentation and admissibility of evidence gathered using technology, but no equivalent instrument defines, in advance, which categories of AI-enabled policing tool are permissible, prohibited, or subject to heightened scrutiny.

The second axis is the sufficiency of legal basis. Both jurisdictions nominally require a valid legal basis for state intrusions into privacy — the Charter and secondary legislation in the EU, and the Puttaswamy threefold test in India. In practice, however, the EU's requirement is satisfied through primary legislation enacted by the European Parliament and Council, whereas India's most consequential biometric-surveillance initiative, the NCRB's proposed facial-recognition system, rests on a cabinet notification rather than a statute — an arrangement digital-rights groups argue fails Puttaswamy's own legality threshold.[22]

The third axis concerns independent oversight and transparency. The EU framework layers national data-protection authorities, the European Data Protection Board, and dedicated Artificial Intelligence Act market-surveillance authorities atop mandatory technical documentation and logging obligations. India's Data Protection Board, established under the

[22]Puttaswamy (n 4) para 325; cf Panoptic, 'NCRB's National Automated Facial Recognition System' (case study) (n 14).

ISSN: 2582-6433

DPDP Act, has a narrower enforcement mandate and no specific competence over AI-enabled policing tools; meanwhile, exemptions under the Right to Information Act for law-enforcement records have historically limited independent scrutiny of tools such as CMAPS, about whose operational effect very little is publicly known even a decade after deployment.

The fourth, and perhaps most socially significant, axis concerns demographic impact. Empirical research on Delhi's CMAPS system has found that its crime-hotspot outputs correlate with, and arguably reinforce, existing policing biases, disproportionately flagging areas with concentrations of caste and religious minorities as high-risk, thereby reproducing a discriminatory feedback loop rather than a neutral statistical output.[23] This dynamic is not unique to India: the Court of Justice's own reasoning in Ligue des droits humains was substantially concerned with the discrimination risks of automated profiling.[24] The critical difference lies in institutional response. The Court of Justice imposed binding, judicially enforceable constraints — restrictions on self-learning systems and a mandated linkage between reliability and permissible interference — directly onto the challenged instrument. No comparable judicial intervention has yet addressed India's predictive-policing tools, notwithstanding broadly similar underlying concerns.

These divergences should not obscure important commonalities. Both jurisdictions recognise privacy and non-discrimination as constitutional or quasi-constitutional values that constrain the state's use of technology; both frameworks, in their different ways, are troubled by the same 'black box' problem; and both are still working out, through legislation in one case and litigation in the other, how far human oversight must be preserved before an AI tool can properly be said to operate within the rule of law. The comparison is instructive for India less because the EU model is flawless — commentators have themselves criticised gaps in the Artificial Intelligence Act's law-enforcement transparency provisions and its reliance on vendor self-classification of risk — than because it demonstrates that a codified, ex ante framework is achievable without abandoning operational policing capability.

9. Human Rights, Equality, Privacy and Due Process

The preceding comparison can be distilled into three overlapping rights concerns.

Privacy is engaged whenever an AI system collects, matches, or infers information about an individual without their knowledge, as is inherent to facial recognition and predictive-policing

[23]Vidushi Marda and Shivangi Narayan, 'Data in New Delhi's Predictive Policing System', Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM 2020); LSE Human Rights Blog, 'Predictive Policing in India: Deterring Crime or Discriminating Minorities?' (2021).

[24]Ligue des droits humains (n 5) paras 199–200 (discrimination risk in automated PNR profiling).

ISSN: 2582-6433

tools. Both frameworks converge doctrinally: a privacy-restricting measure must have a legal basis, pursue a legitimate aim, and be proportionate, whether under Article 21 of the Constitution of India or Articles 7 and 8 of the Charter of Fundamental Rights. The practical divergence lies in the rigour with which that formal test is enforced against specific technologies — enforced through binding EU legislation in one case, and left largely to future litigation in the other.

Equality and non-discrimination form the second concern. The Artificial Intelligence Act directly prohibits biometric-categorisation systems that infer protected characteristics such as race, religion, or political opinion,[25] a recognition that AI tools trained on historical data can encode and amplify existing social biases. India has no equivalent statutory prohibition specific to AI-enabled policing tools. This is not merely a theoretical gap: empirical study of Delhi's predictive-policing system has documented a discriminatory feedback loop in which caste- and religion-associated neighbourhoods are disproportionately flagged as crime hotspots, entrenching over-policing of already marginalised communities rather than correcting for it.

Due process and the right to a fair trial constitute the third concern, and arguably the one where the two frameworks diverge most sharply in institutional design. The Law Enforcement Directive gives individuals subject to a decision based solely on automated processing a right to obtain human intervention and to contest the decision — a right explicitly extended to the criminal justice context. India's BNSS and Bharatiya Sakshya Adhiniyam contain no comparable AI-specific due-process guarantee; an individual identified through facial recognition or flagged by a predictive-policing tool has no statutory right to demand human review of, or to specifically contest, the algorithmic process that generated the suspicion against them. The consequences of this gap are not hypothetical: investigative reporting has documented cases in Delhi in which individuals were arrested on the strength of a facial-recognition match alone, without independent corroborating evidence, before the identification was later shown to be unreliable.

A closely related concern is the presumption of innocence, which is placed under particular strain by any system that generates probabilistic suspicion about individuals who have not otherwise attracted investigative attention. The Court of Justice was alive to this in Ligue des droits humains, describing the automated passenger-screening regime it reviewed as introducing a surveillance mechanism that was continuous, untargeted, and systematic in character, applied to travellers regardless of any individualised suspicion.[26] The same structural

[25]Artificial Intelligence Act (n 1) art 5(1)(g).

[26]Ligue des droits humains (n 5) para 111 (describing a surveillance regime that is continuous, untargeted, and

ISSN: 2582-6433

objection applies, with equal or greater force, to predictive-policing tools like CMAPS, which generate hotspot classifications — and by extension, elevated police attention — for entire neighbour hoods without any finding of individualised suspicion whatsoever. Reconciling the genuine efficiency gains AI can offer with these three rights — privacy, equality, and due process — is the central regulatory challenge the next section addresses for India specifically.

10. Challenges and Recommendations for India

India's engagement with AI in criminal justice faces four interlocking challenges. First, the absence of dedicated legislation means that consequential deployments, including the NCRB's national facial-recognition system, proceed on the strength of executive notifications rather than statute, an arrangement that struggles to satisfy the legality limb of the Supreme Court's own Puttaswamy test. Second, independent oversight of AI-enabled policing tools remains thin: no regulator specifically supervises algorithmic policing tools, the Data Protection Board's mandate does not extend meaningfully to law-enforcement AI, and Right to Information exemptions for police records have historically obscured basic information about how systems such as CMAPS actually function. Third, the training data underlying predictive-policing tools is drawn from historical policing records that themselves reflect decades of documented bias, risking a feedback loop in which algorithmic 'neutrality' launders pre-existing discrimination into an ostensibly objective output. Fourth, there is an accountability vacuum when AI-assisted identification proves wrong: no statutory right to contest an algorithmic identification exists, and the remedies available to a wrongly identified individual are limited to the ordinary, after-the-fact avenues of bail and trial, by which point reputational and liberty harms have already occurred.

Several recommendations follow, drawing deliberately on features of the EU model that are transferable to the Indian constitutional and institutional context without requiring wholesale adoption of its regulatory architecture.

First, Parliament should enact dedicated legislation — whether a standalone statute or a substantial amendment integrated into the DPDP Rules and the BNSS framework — that supplies an unambiguous statutory basis for each category of AI-enabled policing tool, modelled on the Artificial Intelligence Act's risk-based classification of law-enforcement applications as inherently high-risk. This would resolve the legality deficit that currently affects instruments such as the NCRB's facial-recognition system.

systematic).

ISSN: 2582-6433

Second, deployment of any high-risk policing AI tool should be conditioned on a mandatory, independently reviewed impact assessment analogous to a data protection impact assessment, examining accuracy, bias, and proportionality before, rather than after, nationwide rollout.

Third, the law should guarantee a right to meaningful human review of, and to contest, any adverse outcome generated wholly or substantially through automated processing, modelled on the Law Enforcement Directive's automated-decision safeguard, together with mandatory disclosure to the affected individual and defence counsel that an AI tool was involved in generating the suspicion or evidence relied upon.

Fourth, the scope of the Section 17(1)(c) law-enforcement exemption under the DPDP Act should be narrowed and conditioned on independent oversight, rather than operating as a near-blanket carve-out, and the Data Protection Board's jurisdiction should be expressly extended to cover algorithmic tools used by law-enforcement agencies.

Fifth, given the documented correlation between predictive-policing outputs and existing caste- and religion-linked policing bias, any predictive-policing tool should be subject to mandatory, published bias-testing against demographic outcomes prior to, and periodically after, deployment, with results subject to independent audit rather than internal police review alone.

Finally, the evidentiary provisions of the Bharatiya Sakshya Adhiniyam 2023 should be supplemented with standard operating protocols specifically addressing the admissibility, chain-of-custody, and reliability standards applicable to AI-generated evidence, ensuring that the procedural rigour the BNSS has brought to physical forensic evidence is matched for algorithmic evidence.

11. Conclusion

Artificial intelligence has already reshaped the operational reality of criminal justice administration in both India and the European Union, but the legal frameworks governing that transformation remain at markedly different stages of maturity. The European Union has translated decades of privacy and data-protection jurisprudence into a codified, risk-based statutory regime that subjects law-enforcement AI to defined obligations before deployment, reinforced by an active Court of Justice willing to constrain specific technologies on rights grounds. India, despite recent and genuinely significant procedural reform through the BNSS and its first general data-protection statute, has yet to extend a comparable degree of statutory specificity to the predictive-policing and facial-recognition tools already operating across its states, leaving constitutional principles articulated in Puttaswamy to do work that, in the European Union, is done by detailed primary legislation.

ISSN: 2582-6433

This is not an argument that India should import the EU model wholesale — the Artificial Intelligence Act itself has attracted legitimate criticism for gaps in law-enforcement transparency and for allowing vendors, rather than regulators, the first say in risk classification. It is, however, an argument that India possesses a genuine window of opportunity: having just recodified its criminal procedure and enacted its first data-protection statute, it is comparatively well placed to anchor AI-specific safeguards — statutory basis, independent oversight, mandatory human review, and bias auditing — within that same legislative moment, rather than waiting, as the European Union largely did not have to, for harm to accumulate before the law catches up with the technology already in police hands.

12. References / Bibliography

Primary Legislation and Treaties

Constitution of India 1950.

Bharatiya Nagarik Suraksha Sanhita 2023 (Act 46 of 2023).

Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023).

Digital Personal Data Protection Act 2023 (Act 22 of 2023).

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Law Enforcement Directive) [2016] OJ L119/89.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L1689.

Case Law

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

Sadhan Haldar v State (NCT of Delhi) (Delhi High Court, 2018).

Case C-817/19 Ligue des droits humains v Conseil des ministres ECLI:EU:C:2022:491.

Secondary Sources

SFLC.in, ‘Tracing the Rise of Predictive Policing in India’ (2026).

Vidhi Centre for Legal Policy, ‘India’s Tryst With Predictive Policing’.

ISSN: 2582-6433

The Wire and Pulitzer Center, 'As AI Took Over Policing in Delhi, Who Bore the Brunt?' (2025).

Vidushi Marda and Shivangi Narayan, 'Data in New Delhi's Predictive Policing System', Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM 2020).

LSE Human Rights Blog, 'Predictive Policing in India: Deterring Crime or Discriminating Minorities?' (2021).

Observer Research Foundation, 'Facial Recognition in Law Enforcement is the Litmus Test for India's Commitment to "Responsible AI for All"'.

Panoptic, 'NCRB's National Automated Facial Recognition System' (case study).

Tech Policy Press, 'The Landscape of Facial Recognition Technologies in India' (2024).

Access Now, 'In a Bittersweet Ruling, EU Court of Justice Allows EU-Wide Border Surveillance Scheme but Clarifies its Limits' (2022).

Verfassungsblog, 'Automated Predictive Threat Detection after Ligue des Droits Humains: Implications for ETIAS and CSAM' (Parts I and II) (2023).