

Ethical and Legal Dimensions of Artificial Intelligence in Criminal Investigation and Judicial Processes

Bikash Kumar Pandey¹ and Dr. Sanjay Kumar Singh²

Research Scholar¹, Assistant Professor²

Department of Law¹²

YBN University, Ranchi¹²

Abstract: *The rapid diffusion of Artificial Intelligence (AI) into criminal investigation and judicial administration has generated a profound re-ordering of the relationship between the citizen, the State, and the machine. Predictive policing algorithms, automated facial and biometric recognition systems, risk-assessment instruments such as COMPAS, digital forensic tools, and AI-assisted case-management and sentencing-support systems are being deployed across common-law and civil-law jurisdictions alike, promising efficiency, consistency, and the alleviation of chronic case backlogs. Yet this promise is shadowed by grave ethical and constitutional anxieties: algorithmic opacity, discriminatory bias encoded in historical crime data, erosion of the presumption of innocence, dilution of due process and the right to a fair hearing, and the weakening of accountability structures when decisions of liberty are mediated by proprietary code. This article undertakes a doctrinal and analytical study of the ethical and legal dimensions of AI in criminal investigation and judicial processes, situating the inquiry within constitutional guarantees of equality (Article 14), personal liberty (Article 21) and the recognised fundamental right to privacy under the Constitution of India, alongside comparative developments including the European Union's Artificial Intelligence Act, 2024, the United States due-process jurisprudence exemplified in *State v. Loomis* (2016), and evidentiary standards under the *Bharatiya Sakshya Adhinyam*, 2023 and its predecessor, the Indian Evidence Act, 1872. Employing doctrinal legal research supplemented by comparative case analysis, the study examines three research questions concerning the ethical dimensions, legal implications, and adequacy of the existing legal framework governing AI in criminal justice. The findings indicate that while AI offers demonstrable investigative and administrative efficiencies, the prevailing legal architecture — both in India and internationally — remains fragmented, reactive, and insufficiently calibrated to the distinctive risks that autonomous and semi-autonomous decision-systems pose to liberty, dignity, and the rule of law. The article concludes with a call for a rights-based, proportionality-anchored statutory framework for AI governance in criminal justice, drawing on the risk-tiered model of the EU AI Act and the constitutional proportionality doctrine articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).*

Keywords: Artificial Intelligence; Criminal Investigation; Judicial Process; Due Process; Algorithmic Bias; Right to Privacy; AI Governance.

I. INTRODUCTION

The twenty-first-century criminal justice system stands at an inflection point defined not by the discovery of a new substantive crime or procedural code, but by the arrival of a new class of decision-making actor: the algorithm. The emergence of this field of study can be traced to the convergence of three developments — the exponential growth of digital and biometric data generated by modern policing (CCTV networks, mobile forensics, digital communications), advances in machine learning capable of pattern recognition at a scale unattainable by human investigators, and chronic institutional pressures of case backlog, under-staffed police forces, and demands for "smart policing" and "smart courts." What began, in the early 2010s, as isolated experiments — actuarial risk instruments in American sentencing, crime-mapping software in metropolitan police departments — has, by the mid-2020s, matured into a global infrastructure of AI-enabled criminal justice: automated facial recognition systems (AFRS) deployed by the National



Crime Records Bureau in India, the Supreme Court Portal for Assistance in Court's Efficiency (SUPACE) and the Supreme Court Vidhik Anuvaad Software (SUVAS) for judicial translation and research assistance, predictive-policing software in the United Kingdom and the United States, and risk-assessment tools such as Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) used in American sentencing courts.

Artificial Intelligence, for the purposes of this study, is understood as a constellation of computational techniques — principally machine learning, natural language processing, and computer vision — that enable a system to perform tasks conventionally requiring human cognition: pattern recognition, prediction, classification, and, in limited but growing measure, recommendation. In the criminal justice context, AI operates across the entire procedural continuum: at the investigative stage (facial recognition, predictive policing, digital forensics, DNA-matching algorithms), the prosecutorial stage (case-prioritisation and evidence-analytics tools), the adjudicatory stage (bail and sentencing risk-assessment instruments, AI-assisted legal research and drafting), and the correctional stage (recidivism prediction for parole determinations). Each of these applications reallocates a measure of discretion — traditionally the exclusive preserve of the police officer, the prosecutor, or the judge — to a statistical model trained on historical data.

The importance of studying this phenomenon at the present juncture is threefold. First, doctrinally, criminal procedure and evidence law in India have recently been re-codified through the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, all of which took effect from 1 July 2024, offering an unprecedented statutory window within which to examine whether the new codes adequately anticipate AI-mediated investigation and adjudication. Second, constitutionally, the Supreme Court's nine-judge recognition of privacy as a fundamental right under Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, has fundamentally altered the standard against which State deployment of surveillance and biometric technologies must be tested — namely, the tripartite proportionality standard of legality, necessity, and proportionality. Third, globally, the entry into force of the prohibitions under Article 5 of the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) from 2 February 2025 has, for the first time, produced a binding supranational instrument that expressly prohibits certain law-enforcement uses of AI (such as purely profiling-based predictive policing and untargeted facial-image scraping), thereby setting a comparative benchmark against which the adequacy of domestic frameworks — including India's — may be assessed. It is this confluence of technological capability, constitutional re-articulation, and comparative regulatory innovation that renders the ethical and legal study of AI in criminal investigation and judicial process both timely and necessary.

1.1. The Conceptual Framework

For analytical clarity, this study organises the ethical and legal terrain of AI in criminal justice around four major dimensions, each of which recurs, in varying configurations, throughout the literature and case law surveyed below.

Investigative Dimension: the use of AI in detection, surveillance, and evidence-gathering — including facial recognition technology (FRT), predictive policing, automated fingerprint identification systems (AFIS), and digital/forensic AI tools that analyse call-data records, financial transactions, and social-media content.

Adjudicatory Dimension: the use of AI to support or influence judicial and quasi-judicial decision-making — including bail and sentencing risk-assessment tools (e.g., COMPAS), AI-assisted legal research and case-management platforms (e.g., SUPACE, SUVAS, the National Judicial Data Grid), and, prospectively, AI-generated drafting of judicial orders.

Evidentiary Dimension: the epistemic and procedural status of AI-generated or AI-processed material as evidence — engaging Sections 61 to 63 (documentary evidence) and the special regime for electronic records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (successor to Section 65B of the Indian Evidence Act, 1872), and the chain-of-custody, authentication, and reliability standards applicable to algorithmic outputs.

Rights and Accountability Dimension: the constitutional and human-rights framework within which AI is deployed — engaging the right to equality (Article 14), the right to life and personal liberty including privacy and due process (Article 21), protection against arbitrary State action, and the accountability mechanisms (judicial review, data-protection law, algorithmic audit, and legislative oversight) available to contest or remedy AI-driven harm.

These four dimensions are not hermetically sealed; a single technology — facial recognition, for instance — simultaneously implicates the investigative dimension (as a detection tool), the evidentiary dimension (as a source of

identification evidence), and the rights dimension (as a form of biometric surveillance engaging Article 21). The framework's importance in the current scenario lies precisely in this interlocking character: policy and doctrinal responses that address only one dimension — for instance, technical accuracy standards for FRT without corresponding evidentiary or constitutional safeguards — will necessarily remain incomplete. The framework therefore also structures the Analysis and Interpretation in Section 4 of this study.

1.2. The Need of the Study

There is a demonstrable and growing gap between the pace of technological adoption in Indian and comparative criminal justice systems and the pace of corresponding legal regulation. India currently has no dedicated statute governing facial recognition or predictive-policing technologies; the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, introduced as a private member's bill, remains pending and, as such private bills are rarely enacted, is unlikely to become law in its present form. The Digital Personal Data Protection Act, 2023 (DPDP Act), India's principal data-protection statute, contains broad exemptions under Section 17(1)(c) for processing "in the interests of prevention, detection, investigation or prosecution of any offence," substantially limiting its applicability to State surveillance infrastructure. This regulatory vacuum, combined with the accelerating deployment of AI tools such as the National Automated Facial Recognition System (AFRS), Delhi Police's real-time facial-recognition and biometric surveillance apparatus, and AI-assisted case-management platforms in the higher judiciary, creates a pressing need for systematic doctrinal study of the ethical and legal adequacy of the existing framework — a need this study directly addresses.

1.3. The Significance of the Study

Rationale. The rationale for this study rests on the proposition that criminal justice is the domain in which the coercive power of the State is at its most concentrated — bearing directly on liberty, bodily integrity, and, in extreme cases, life itself. Errors or biases introduced by AI systems in this domain are therefore qualitatively distinct from, and more consequential than, comparable errors in commercial or administrative contexts. A wrongly flagged transaction can be reversed; a wrongful arrest, a denial of bail on the basis of an opaque risk score, or a mistaken facial-recognition identification carries costs to liberty and dignity that cannot be fully undone.

Purpose. The purpose of this study is threefold: (i) to map, with reference to primary legal materials, constitutional provisions, and case law, the ethical dimensions of AI deployment across the investigative and adjudicatory continuum; (ii) to analyse the legal implications — statutory, evidentiary, and constitutional — that arise from such deployment in both the Indian and comparative context; and (iii) to assess, through doctrinal and comparative analysis, whether the existing legal framework is adequate to the task, and, where it is found wanting, to identify the specific normative and institutional gaps that require legislative or judicial attention. In doing so, the study aims to contribute to the emerging but still nascent Indian legal scholarship on AI governance in criminal justice, and to inform policy discourse surrounding the pending Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, and any future comprehensive AI legislation.

1.4. The Delimitations of the Study

The study is doctrinal and analytical in method; it does not undertake primary empirical fieldwork (such as surveys of police officers, judges, or affected litigants), relying instead on secondary data, reported judgments, statutory text, and existing empirical literature.

The study focuses primarily on the Indian legal framework, with comparative reference to the United States and the European Union limited to those doctrines and instruments (due process jurisprudence, the EU AI Act, GDPR) that illuminate or benchmark the Indian position; a comprehensive multi-jurisdictional survey is beyond its scope.

The study addresses AI in criminal investigation and judicial process; it does not extend to the use of AI in civil litigation, administrative tribunals, or purely regulatory/compliance contexts, save where such use bears directly on criminal justice.

Given the fast-evolving nature of both AI technology and its regulation, the legal and policy position is stated as of the position current in 2026; subsequent legislative or judicial developments are outside the scope of this analysis.

1.5 Research Questions

RQ1: What are the ethical dimensions of Artificial Intelligence (AI) in criminal investigation and judicial processes?

RQ2: What are the legal implications of using Artificial Intelligence (AI) in criminal investigation and judicial processes?

RQ3: How adequate is the existing legal framework governing the use of AI in criminal investigation and judicial processes?

1.6 Research Objectives

O1: To examine the ethical dimensions of Artificial Intelligence (AI) in criminal investigation and judicial processes.

O2: To analyse the legal implications of using Artificial Intelligence (AI) in criminal investigation and judicial processes.

O3: To assess the adequacy of the existing legal framework governing the use of Artificial Intelligence (AI) in criminal investigation and judicial processes.

II. REVIEW OF RELATED LITERATURE

International Literature

Rodrigues (2020) undertakes an early and influential mapping of the legal and human-rights gaps opened up by AI deployment, arguing that existing human-rights instruments — framed around individual, human decision-makers — struggle to attribute responsibility and afford remedy when harm is mediated by an autonomous or semi-autonomous system. The study identifies vulnerabilities in due process, non-discrimination, and privacy protections, and calls for rights-based AI governance frameworks capable of anticipating algorithmic harm before, rather than after, deployment. For the present study, Rodrigues's framework directly informs the ethical dimension (RQ1), particularly the argument that AI's opacity structurally undermines the individualised scrutiny that due process demands.

Fazel et al. (2022) conduct a systematic review of validation studies for criminal recidivism risk-assessment tools of the kind used in Western sentencing courts, including COMPAS-type instruments. The review finds considerable heterogeneity in predictive accuracy across tools and jurisdictions, and cautions that many instruments have not been independently validated on the populations to which they are subsequently applied — a finding with direct bearing on the due-process reasoning in *State v. Loomis* (2016), discussed in Section 4 below. The study's central contribution to the present research lies in its empirical substantiation of the legal-implications question (RQ2): if risk instruments are of uncertain external validity, their use to inform decisions of liberty raises the evidentiary and constitutional concern of sentencing on the basis of unreliable or non-individualised information.

Engel, Linhardt, and Schubert (2025), drawing on the Lessig aphorism that "code is law," empirically examine how the introduction of the COMPAS instrument altered judicial reasoning and sentencing patterns in practice, finding that risk scores exert an anchoring effect on judicial discretion even where courts formally treat the score as merely one factor among many — echoing, and empirically testing, the *Loomis* court's own caution that COMPAS must not become "determinative." This 2025 study is the most recent of the three international sources reviewed and is directly relevant to RQ3, since it demonstrates that formal legal safeguards (such as the *Loomis* limitations) may be insufficient, in practice, to prevent algorithmic outputs from displacing individualised human judgment — a systemic adequacy concern central to this study's third objective.

National Literature

Jauhar, A., Misra, M., Sengupta, A., Chakrabarti, P. P., Ghosh, S., & Ghosh, S. (2021) produced by the Vidhi Centre for Legal Policy in collaboration with the Indian Institute of Technology Kharagpur's TCG-CREST, offers the most comprehensive Indian policy-oriented treatment of AI in the justice system to date. It surveys existing and prospective AI applications in Indian courts (translation, case triage, legal research) and articulates seven principles for "responsible AI" — safety, equality, inclusivity, non-discrimination, privacy protection, transparency, and accountability. The paper

explicitly cautions against premature adoption of AI in adjudicatory decision-making (as opposed to administrative support functions) absent robust safeguards. For the present study, this source substantially informs the analysis of RQ3, providing an Indian-specific benchmark of what an adequate governance framework would require, against which the current statutory position (discussed in Section 4.3) can be measured.

Narayanan, Agarwal, and Bansal (2023) examine the practical inroads AI has made into the Indian judiciary — including SUPACE, SUVAS, and AI-assisted transcription of Supreme Court proceedings — while cautioning against the risk of embedded bias and the absence of a statutory framework specifically addressing judicial AI use. Their analysis emphasises that Indian judicial AI tools have, to date, been confined to administrative and research-support functions rather than outcome-determinative decision-making, a distinction the authors argue is constitutionally significant but institutionally fragile absent codified limits. This 2023 study is the most recent Indian source in the chronological sequence and directly supports this study's analysis of the evidentiary and adjudicatory dimensions in Section 4.

Synthesis of the Literature

Read together, these five studies — spanning 2020 to 2025 and both international and Indian contexts — reveal a consistent pattern: technical and empirical scholarship (Fazel et al., 2022; Engel et al., 2025) demonstrates that AI risk-assessment and decision-support tools carry real and measurable limitations in accuracy, validity, and their effect on human discretion, while doctrinal and policy scholarship (Rodrigues, 2020; Jauhar et al., 2021; Narayanan et al., 2023) converges on the conclusion that legal and constitutional safeguards have not kept pace with technological deployment. This convergence directly substantiates the need for, and the research questions animating, the present study.

3. Methodology of the Study

This study adopts a *doctrinal legal research methodology*, supplemented by comparative and analytical techniques, appropriate to a normative inquiry into the adequacy of law. The methodology proceeds along the following lines.

Research Design

The study is qualitative and doctrinal in design, involving the systematic collection, analysis, and synthesis of primary legal sources (constitutional provisions, statutes, delegated legislation, and judicial decisions) and secondary sources (peer-reviewed literature, government and institutional reports, and policy papers) bearing on AI in criminal investigation and judicial process.

Sources of Data

Primary sources: the Constitution of India (Articles 14, 19, and 21); the Bharatiya Nyaya Sanhita, 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023; the Bharatiya Sakshya Adhiniyam, 2023; the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 (pending); the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689); reported judgments including *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), *Anvar P.V. v. P.K. Basheer* (2014), *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), and *State v. Loomis* (2016).

Secondary sources: peer-reviewed articles, systematic reviews, government reports (including the United States Department of Justice's 2024 report on AI and criminal justice), and institutional policy papers (Vidhi Centre for Legal Policy, 2021).

Method of Analysis

The study employs (i) *doctrinal analysis*, involving close textual reading of constitutional provisions and statutory sections to determine their scope and applicability to AI-mediated investigation and adjudication; (ii) *case-law analysis*, tracing the ratio decidendi of landmark judgments to derive applicable constitutional standards (such as the proportionality test articulated in *Puttaswamy*); and (iii) *comparative legal analysis*, juxtaposing the Indian position against the regulatory model adopted under the EU AI Act and the due-process jurisprudence of the United States, in order to benchmark adequacy under Objective 3 (O3).

Scope of Analysis

The analysis in Section 4 is organised around the three research questions and the four-dimension conceptual framework articulated in Section 1.1, ensuring that ethical, legal, and adequacy considerations are examined both independently and in their interrelation.

Limitations of the Methodology

As a doctrinal study, this research does not generate new empirical data on the actual operation of AI tools within Indian police stations or courts; its findings on real-world impact are necessarily mediated through existing empirical literature and reported case law, which may lag behind the pace of technological deployment on the ground.

III. ANALYSIS AND INTERPRETATION

This section presents the substantive analysis of the study, organised around the three research questions and the four-dimension conceptual framework set out in Section 1.1.

3.1 The Ethical Dimensions of Artificial Intelligence in Criminal Investigation and Judicial Processes

Addressing RQ1 and Objective O1, this sub-section examines five interlocking ethical concerns that recur across the literature and case law surveyed: algorithmic bias and discrimination; opacity and the "black box" problem; erosion of the presumption of innocence; automation bias and de-skilling of human judgment; and the ethics of biometric surveillance.

3.1.1 Algorithmic Bias and Discrimination

AI systems trained on historical crime data risk encoding and amplifying pre-existing patterns of discriminatory policing. The best-documented instance is the COMPAS recidivism instrument, which an investigative analysis by Larson, Mattu, Kirchner, and Angwin (2016) for ProPublica found was more likely to falsely flag Black defendants as high-risk for future crime, and more likely to falsely flag white defendants as low-risk, than actual recidivism outcomes justified. Although the vendor disputed the statistical methodology, the finding crystallised what has since become a foundational concern in AI-ethics scholarship: that facial-neutral algorithms, trained on data reflecting historically unequal enforcement patterns, can reproduce that inequality under a veneer of statistical objectivity. Daka et al. (2022), in a systematic review of AI and crime-prediction literature, similarly find that predictive-policing tools risk creating feedback loops in which over-policed neighbourhoods generate more recorded crime data, which in turn directs further policing resources to those neighbourhoods — a self-reinforcing cycle of disproportionate surveillance.

In the Indian context, the ethical stakes of bias are compounded by the absence of disaggregated data on how facial recognition and predictive tools perform across India's own social fault-lines of caste, religion, and region — a gap noted in Indian scholarship (Talukder & Shompa, 2024) and by civil-society organisations examining the deployment of the National Automated Facial Recognition System (AFRS) and Delhi Police's real-time surveillance apparatus, which has drawn a pending Public Interest Litigation before the Delhi High Court and scrutiny by the Supreme Court of India concerning biometric surveillance at public protests.

3.1.2 Opacity and the "Black Box" Problem

A second ethical concern is epistemic: many AI systems, particularly those relying on proprietary machine-learning models, do not disclose the weighting of input variables or the internal logic by which an output (a risk score, a facial match, a crime-hotspot prediction) is generated. This was central to Eric Loomis's due-process challenge in *State v. Loomis*, 2016 WI 68, 881 N.W.2d 749 (Wis. 2016), where the defendant argued that reliance on a COMPAS score whose "methodology used to make the reports is a trade secret" infringed his right to be sentenced on accurate, individually verifiable information. The Wisconsin Supreme Court did not accept that proprietary opacity per se violated due process, reasoning that the defendant had access to the score itself and the inputs he had provided, even if not the underlying algorithm — but it required that any presentence investigation report using COMPAS include specific written advisories as to the tool's limitations. The case illustrates the ethical tension between commercial confidentiality (protecting a vendor's intellectual property) and the individual's interest in contesting the basis of a decision affecting liberty.

3.1.3 Erosion of the Presumption of Innocence and Individualised Justice

Predictive and risk-assessment tools operate on group-level statistical correlations, whereas criminal justice — doctrinally and ethically — demands individualised assessment of guilt and culpability. Fazel et al. (2022), in their systematic review of recidivism-tool validation studies, caution that many instruments have not been externally validated on the specific populations to which they are applied, meaning that a defendant may be scored against a reference population that does not reflect their actual circumstances. Ethically, this raises the spectre of a person being

subjected to a more severe outcome (a longer remand, a harsher sentence) not because of anything they have individually done, but because of the statistical behaviour of a demographic or geographic category to which an algorithm assigns them.

3.1.4 Automation Bias and the De-skilling of Human Judgment

A related but distinct concern is *automation bias* — the well-documented human tendency to over-trust automated recommendations, even when contrary evidence is available (Goddard, Roudsari, & Wyatt, 2012, cited in comparative empirical-legal scholarship on judicial decision-making). Engel, Linhardt, and Schubert (2025) find that the introduction of COMPAS scores measurably altered judicial sentencing behaviour, suggesting that even where courts formally treat an algorithmic score as advisory, it exerts an anchoring effect on discretion. The ethical risk here is the gradual transfer of substantive decision-making authority from the accountable human judge or investigating officer to an unaccountable statistical artefact, undermining the judicial oath and constitutional role of independent adjudication.

3.1.5 The Ethics of Biometric Surveillance

Finally, the deployment of facial recognition and other biometric identification technologies in public spaces raises distinct ethical concerns regarding consent, proportionality, and the chilling effect on constitutionally protected activity such as protest and assembly. The case of human-rights activist S.Q. Masood, who was stopped by Hyderabad police, made to remove his COVID-19 face mask, and photographed without stated reason — later the subject of a legal notice and public-interest challenge — has become a widely cited Indian illustration of the ethical hazard of unregulated biometric policing. Researcher Vidushi Marda's observation, made in this context, that "AI is not a silver bullet" for underlying societal problems captures the ethical caution that technological solutionism can substitute for, rather than support, substantive policing reform.

Table 1: Ethical Dimensions of AI in Criminal Justice — Summary Matrix

Ethical Concern	Illustrative Technology / Case	Constitutional Value Implicated
Algorithmic bias and discrimination	COMPAS (Larson et al., 2016); predictive policing (Dakalbab et al., 2022)	Right to equality (Article 14)
Opacity / "black box" reasoning	<i>State v. Loomis</i> (2016)	Due process; right to be heard
Erosion of individualised justice	Recidivism risk tools (Fazel et al., 2022)	Presumption of innocence; Article 21
Automation bias / de-skilling	Judicial reliance on risk scores (Engel et al., 2025)	Independence of judicial discretion
Unregulated biometric surveillance	AFRS; Delhi Police FRT deployment	Right to privacy (Article 21); Article 19

3.2 The Legal Implications of Using Artificial Intelligence in Criminal Investigation and Judicial Processes

Addressing RQ2 and Objective O2, this sub-section analyses the legal implications of AI deployment across three registers: constitutional law, evidentiary law, and statutory/regulatory law.

3.2.1 Constitutional Implications: Article 14, Article 21, and the Proportionality Standard

The starting point for constitutional analysis in India is *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; AIR 2017 SC 4161, in which a nine-judge Bench of the Supreme Court unanimously held that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21, and as part of the freedoms guaranteed by Part III of the Constitution, thereby overruling the contrary observations in *M.P. Sharma v.*



Satish Chandra (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962). The Court held that any State action restricting privacy must satisfy a tripartite test: (i) legality, requiring the existence of a validly enacted law; (ii) legitimate State aim; and (iii) proportionality, requiring a rational nexus between the objects sought and the means adopted, with the least restrictive means being preferred. This proportionality standard is the primary constitutional lens through which AI-enabled investigative technologies — facial recognition, predictive policing, communications interception — must now be assessed in India.

Applying this standard, a significant legal implication follows: because India currently possesses no statute specifically authorising or regulating the police use of facial recognition technology, deployments such as the National AFRS and Delhi Police's real-time surveillance network arguably fail the threshold requirement of *legality* under the *Puttaswamy* test, since they proceed on the basis of executive notifications, administrative tenders, and internal police manuals rather than a validly enacted law. This is the central argument advanced in recent Indian legal scholarship examining the constitutional validity of facial recognition under Article 21, and is presently the subject of live litigation, including a Public Interest Litigation concerning Delhi Police's use of facial recognition, mobile biometric applications, and AI-enabled surveillance vehicles at public protests, which the Supreme Court of India has indicated it will examine on its merits rather than refer solely to an administrative committee.

Article 14's guarantee of equality before the law and equal protection of the laws is separately implicated wherever an AI system's outputs disproportionately burden a particular class of persons — whether through biased predictive-policing allocation or discriminatory risk-scoring — without a rational nexus to a legitimate classification, potentially rendering such deployment vulnerable to challenge as manifestly arbitrary State action.

3.2.2 Evidentiary Implications: Electronic and Algorithmic Evidence

The evidentiary status of AI-generated or AI-processed material is governed, in India, by the special regime for electronic records first established under Section 65B of the Indian Evidence Act, 1872, and now carried forward in substantially similar form under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. In *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, a three-judge Bench of the Supreme Court held that secondary electronic evidence is admissible only upon production of a certificate under Section 65B(4), overruling the earlier, more permissive position in *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600. Subsequent uncertainty introduced by *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 — which suggested the certificate requirement could be relaxed in the interest of justice — was authoritatively resolved by a three-judge Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), which held that the Section 65B(4) certificate is a mandatory condition precedent to the admissibility of electronic evidence (save where the original device itself is produced before the court).

This settled evidentiary architecture was designed principally for conventional digital records (call-data records, CCTV footage, emails) and does not squarely address the distinct evidentiary questions raised by *algorithmic outputs* — a facial-recognition match, a predictive-policing risk score, or an AI-generated forensic inference. Such outputs are not merely records of past events but probabilistic inferences generated by a model, raising unresolved questions of: (i) whether the "certificate" mechanism under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (requiring attestation that a computer was "operating properly") is a meaningful proxy for the reliability of a machine-learning model's output; (ii) whether a defendant has a corresponding right to interrogate the training data, error rates, and validation methodology behind an algorithmic identification or score, analogous to the right to cross-examine a human witness; and (iii) how chain-of-custody principles apply to cloud-processed or continuously-retrained models. None of these questions has yet received authoritative judicial resolution in India, constituting a significant evidentiary gap identified by this study.

3.2.3 Statutory and Regulatory Implications

At the statutory level, the Digital Personal Data Protection Act, 2023 is India's principal data-protection instrument, but its Section 17(1)(c) exempts processing undertaken "in the interests of prevention, detection, investigation or prosecution of any offence" from the obligations otherwise imposed on data fiduciaries, and Section 17(2) permits the Central Government to exempt State instrumentalities altogether on grounds of sovereignty, security, and public order. The consequence, noted in recent Indian scholarship analysing the FRT-enabled surveillance landscape, is that the

DPDP Act provides negligible practical constraint on law-enforcement biometric processing, leaving the *Puttaswamy* proportionality standard as the primary — and, absent implementing legislation, largely aspirational — safeguard. Comparatively, the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) adopts a materially more prescriptive approach. Article 5 of the Act, whose prohibitions have applied since 2 February 2025, categorically bans, among other practices: (a) AI systems used by or on behalf of law enforcement to predict the likelihood of an individual committing a crime based solely on profiling or personality-trait assessment rather than objective, verifiable facts linked to criminal activity; (b) the untargeted scraping of facial images from the internet or CCTV footage to build or expand facial-recognition databases; and (c) "real-time" remote biometric identification in publicly accessible spaces for law-enforcement purposes, subject only to three narrowly defined exceptions (targeted search for victims of trafficking or missing persons, prevention of an imminent and specific terrorist threat, or the search for a suspect in specified serious crimes), each requiring prior judicial or independent administrative authorisation and a mandatory fundamental-rights impact assessment under Article 27. This risk-tiered, ex-ante prohibition model stands in sharp contrast to the Indian position, which relies on post-facto constitutional litigation rather than statutory prohibition, and is discussed further as a comparative benchmark in Section 4.3.

Table 2: Comparative Legal Framework for AI in Criminal Justice — India, United States, and European Union

Jurisdiction	Governing Instrument(s)	Core Standard Applied	Key Case / Provision
India	Constitution of India (Arts. 14, 19, 21); Bharatiya Sakshya Adhiniyam, 2023; DPDP Act, 2023	Proportionality test (legality, legitimate aim, proportionality)	<i>Puttaswamy v. Union of India</i> (2017); <i>Anvar P.V. v. P.K. Basheer</i> (2014)
United States	Fourteenth Amendment Due Process Clause; state evidence law	Due process with disclosed limitations; no per se bar on proprietary tools	<i>State v. Loomis</i> , 2016 WI 68, 881 N.W.2d 749
European Union	Artificial Intelligence Act, Regulation (EU) 2024/1689	Risk-tiered ex-ante prohibition and impact assessment	Article 5 (prohibited practices); Article 27 (fundamental rights impact assessment)

4.3 The Adequacy of the Existing Legal Framework Governing AI in Criminal Investigation and Judicial Processes
Addressing RQ3 and Objective O3, this sub-section assesses whether the legal framework identified in Section 4.2 is adequate to govern the ethical risks identified in Section 4.1. The assessment proceeds against four criteria drawn from the conceptual framework in Section 1.1: (i) statutory specificity, (ii) evidentiary preparedness, (iii) proportionality enforcement, and (iv) institutional accountability.

3.3.1 Statutory Specificity: A Persistent Regulatory Vacuum

On the criterion of statutory specificity, the existing Indian framework is found to be markedly inadequate. Unlike the European Union's AI Act, India has no binding statute directly regulating facial recognition, predictive policing, or algorithmic risk-assessment in criminal investigation. The Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 — which would have required prior magistrate approval for FRT deployment, distinguished FRT from "measurements" under the Criminal Procedure (Identification) Act, 2022, and imposed retention limits — remains a pending private member's bill with a low probability of enactment. In its absence, the Criminal Procedure (Identification) Act, 2022, which authorises the collection of "measurements" including biometric and behavioural data of arrested and convicted persons for periods of up to seventy-five years, is the closest analogous statutory instrument, but its text does not expressly contemplate AI-driven facial recognition or predictive analytics, leaving significant interpretive uncertainty.

3.3.2 Evidentiary Preparedness: An Unaddressed Frontier

On the criterion of evidentiary preparedness, the framework is partially adequate. The certificate-based regime under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, as clarified by *Arjun Panditrao Khotkar* (2020), provides a workable, judicially settled mechanism for authenticating conventional electronic records. However, as identified in Section 4.2.2, this mechanism does not extend to the distinctive reliability and explainability questions posed by probabilistic algorithmic outputs, and no Indian appellate authority has yet articulated standards analogous to the *Daubert*-style scientific-reliability scrutiny developed in other forensic-evidence contexts for AI-generated identifications or predictions. This represents a significant adequacy gap.

3.3.3 Proportionality Enforcement: Strong in Principle, Weak in Practice

On the criterion of proportionality enforcement, the *Puttaswamy* framework is doctrinally robust but institutionally under-enforced. The proportionality test requires, at minimum, a valid law authorising any privacy-infringing State action; yet, as demonstrated by ongoing litigation concerning Delhi Police's deployment of real-time facial recognition, biometric identification applications, and AI-enabled surveillance vehicles at public gatherings, State agencies have in practice proceeded with large-scale biometric surveillance in the continued absence of such a law, with judicial scrutiny occurring reactively, years after deployment, and typically only where public-interest litigation is brought. The doctrinal strength of *Puttaswamy* is therefore not matched by ex-ante institutional mechanisms (of the kind the EU AI Act's Article 27 fundamental-rights impact assessment and prior-authorisation requirements provide) capable of preventing rights violations before they occur, rather than remedying them after the fact.

3.3.4 Institutional Accountability: Fragmented Oversight

On the criterion of institutional accountability, the framework is fragmented across multiple statutes and institutions — the Information Technology Act, 2000 and its 2011 Rules (applicable only to body corporates, not government surveillance instrumentalities), the DPDP Act, 2023 (substantially exempting law-enforcement processing), the Bharatiya Nagarik Suraksha Sanhita, 2023 (governing search, seizure, and investigative procedure generally, without AI-specific provisions), and constitutional judicial review (available only post-facto and subject to the delays inherent in Indian litigation). No single regulator possesses either the mandate or the technical capacity to audit algorithmic tools deployed in criminal investigation for accuracy, bias, or compliance with the *Puttaswamy* proportionality standard — a structural deficiency also identified in the Vidhi Centre for Legal Policy's 2021 strategy paper on responsible AI in the Indian justice system.

Table 3: Adequacy Assessment of the Existing Legal Framework

Adequacy Criterion	Current Indian Position	Adequacy Rating
Statutory specificity	No dedicated AI/FRT statute; Bill pending since 2023	Inadequate
Evidentiary preparedness	Settled regime for electronic records; silent on algorithmic reliability	Partially adequate
Proportionality enforcement	Strong constitutional doctrine (<i>Puttaswamy</i>); weak ex-ante enforcement	Partially adequate
Institutional accountability	Fragmented across IT Act, DPDP Act, BNSS; no dedicated AI regulator	Inadequate

Taken together, the four-criterion assessment indicates that the existing Indian legal framework governing AI in criminal investigation and judicial process is *inadequate* on two of four criteria and only *partially adequate* on the remaining two, substantiating the study's central finding — elaborated in Section 5 below — that legislative intervention, rather than continued reliance on constitutional litigation alone, is necessary to close the identified gaps.

IV. MAJOR FINDINGS

Finding 1 (Ethical): AI deployment in Indian and comparative criminal justice systems is attended by five recurrent ethical risks — algorithmic bias, opacity, erosion of individualised justice, automation bias, and unregulated biometric surveillance — each of which is empirically documented in the literature reviewed (Larson et al., 2016; Dakalbab et al., 2022; Fazel et al., 2022; Engel et al., 2025) and doctrinally recognised, at least implicitly, in *State v. Loomis* (2016).

Finding 2 (Legal — Constitutional): The proportionality standard articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) provides India with a doctrinally sound constitutional test for evaluating AI-enabled surveillance, but its threshold requirement of a valid authorising law is not presently satisfied by major deployments such as the National AFRS and Delhi Police's biometric-surveillance infrastructure, rendering such deployments constitutionally vulnerable.

Finding 3 (Legal — Evidentiary): The settled electronic-evidence regime under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (as clarified by *Arjun Panditrao Khotkar*, 2020, in respect of its predecessor Section 65B) is well-adapted to conventional digital records but does not address the distinct reliability, explainability, and contestability questions raised by AI-generated probabilistic outputs such as facial-recognition matches or predictive-policing risk scores.

Finding 4 (Legal — Statutory): India's principal data-protection statute, the Digital Personal Data Protection Act, 2023, substantially exempts law-enforcement processing under Section 17, leaving a regulatory vacuum that the pending Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 was designed, but has so far failed, to fill.

Finding 5 (Adequacy): Measured against the four-criterion framework applied in Section 4.3, the existing Indian legal framework is inadequate on statutory specificity and institutional accountability, and only partially adequate on evidentiary preparedness and proportionality enforcement — indicating that constitutional litigation alone, however doctrinally robust, cannot substitute for comprehensive ex-ante legislative regulation.

Finding 6 (Comparative): The European Union's risk-tiered, ex-ante regulatory model under Article 5 of the AI Act — which categorically prohibits purely profiling-based predictive policing and unauthorised real-time biometric identification, and mandates fundamental-rights impact assessments before deployment — offers a workable comparative template that Indian AI-governance reform could adapt, subject to contextualisation for India's distinct constitutional and institutional architecture.

Finding 7 (Institutional): No single Indian regulatory authority currently possesses both the legal mandate and the technical capacity to audit AI tools deployed in criminal investigation for bias, accuracy, or constitutional compliance, echoing the institutional-accountability gap identified in the Vidhi Centre for Legal Policy's (2021) strategy paper on responsible AI in the Indian justice system.

V. CONCLUSION

This study set out to examine the ethical dimensions, legal implications, and adequacy of the existing legal framework governing Artificial Intelligence in criminal investigation and judicial processes. Its findings demonstrate that the arrival of AI in criminal justice is not a peripheral technological development but a structural challenge to foundational legal principles — the presumption of innocence, the right to an individualised hearing, the constitutional guarantee of equality under Article 14, and the fundamental right to privacy and personal liberty under Article 21 as authoritatively recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). The comparative analysis undertaken in Section 4 demonstrates that while Indian constitutional doctrine — particularly the proportionality standard — is theoretically well-equipped to constrain arbitrary or disproportionate AI deployment, its practical enforcement lags considerably behind both the pace of technological adoption by Indian law-enforcement agencies and the regulatory sophistication of comparator jurisdictions such as the European Union under its Artificial Intelligence Act.

The study's central conclusion is that India requires a dedicated, rights-anchored statutory framework for AI in criminal justice — building upon, rather than abandoning, the pending Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 — that would (i) codify the *Puttaswamy* proportionality standard into specific, ex-ante procedural safeguards including prior judicial authorisation for biometric surveillance; (ii) extend the evidentiary certificate regime under the Bharatiya Sakshya Adhiniyam, 2023 to address the specific reliability and contestability requirements of

algorithmic evidence; (iii) narrow the law-enforcement exemptions presently available under Section 17 of the Digital Personal Data Protection Act, 2023, or introduce a parallel, sector-specific oversight mechanism for criminal-justice data processing; and (iv) establish a technically competent, independent oversight body empowered to audit AI tools used in investigation and adjudication for bias, accuracy, and constitutional compliance, drawing on the fundamental-rights impact assessment model found in Article 27 of the EU AI Act. Absent such reform, the promise of AI-enabled efficiency in Indian criminal justice risks being purchased at the cost of the very constitutional guarantees — equality, liberty, dignity, and due process — that the criminal justice system exists to protect. Future research building on this study might usefully undertake empirical assessment of AI tool performance within Indian policing and judicial institutions, complementing the doctrinal analysis offered here.

REFERENCES

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, 2020 SCC OnLine SC 571 (India).
3. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
4. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
5. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
6. Biju, P. R., & Gayathri, O. (2022). The Indian approach to artificial intelligence: An analysis of policy discussions, constitutional values, and regulation. *Indian Journal of Law and Technology*, 14(1), 67–89.
7. Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).
8. Dakalbab, F., Talib, M. A., Waraga, O. A., Nassif, A. B., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. *Social Sciences & Humanities Open*, 6(1), Article 100342. <https://doi.org/10.1016/j.ssaho.2022.100342>
9. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
10. Engel, C., Linhardt, L., & Schubert, M. (2025). Code is law: How COMPAS affects the way the judiciary handles the risk of recidivism. *Artificial Intelligence and Law*, 33(2), 383–404. <https://doi.org/10.1007/s10506-024-09389-8>
11. European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
12. Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, Bill No. [XX] of 2023 (India).
13. Fazel, S., Burghart, M., Fanshawe, T., Gil, S. D., Monahan, J., & Yu, R. (2022). The performance of criminal recidivism risk assessment tools used in sentencing: Systematic review of validation studies. *Journal of Criminal Justice*, 81, Article 101902. <https://doi.org/10.1016/j.jcrimjus.2022.101902>
14. Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: A systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, 19(1), 121–127. <https://doi.org/10.1136/amiajnl-2011-000089>
15. India Const. arts. 14, 19, 21.
16. Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872, § 65B (repealed 2024) (India).
17. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
18. Jauhar, A., Misra, M., Sengupta, A., Chakrabarti, P. P., Ghosh, S., & Ghosh, S. (2021). *Responsible AI in the Indian justice system: A strategy paper*. Vidhi Centre for Legal Policy.
19. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
20. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).
21. Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016, May 23). *How we analyzed the COMPAS recidivism algorithm*. ProPublica. <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>
22. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).
23. Narayanan, S., Agarwal, M., & Bansal, S. (2023). Artificial intelligence inroads into the Indian judicial system. *Indian Journal of Legal Studies*, 9(4), 200–220.

24. Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, Article 100005. <https://doi.org/10.1016/j.jrt.2020.100005>
25. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 (India).
26. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600 (India).
27. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S. Ct. 2290 (2017).
28. Talukder, K. A., & Shompa, T. F. (2024). Artificial intelligence in criminal justice management: A systematic literature review. *Journal of Machine Learning, Data Engineering and Data Science*, 1(1), 63–82. <https://doi.org/10.70008/jmldeds.v1i01.42>
29. U.S. Department of Justice, Office of Legal Policy. (2024). *Artificial intelligence and criminal justice: Final report*. U.S. Department of Justice.