

Role of Artificial Intelligence in the Criminal Justice System: A Critical Legal Study of Investigation and Judicial Processes

Bikash Kumar Pandey¹ and Dr. Sanjay Kumar Singh²

Research Scholar¹, Assistant Professor²

Department of Law¹²

YBN University, Ranchi¹²

Abstract: *Artificial Intelligence (AI) has moved from the margins of legal administration to the very centre of contemporary criminal justice reform. From predictive-policing platforms and facial-recognition surveillance networks used in criminal investigation, to risk-assessment algorithms such as the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) deployed at the sentencing stage, and to court-assistance tools such as India's Supreme Court Portal for Assistance in Court's Efficiency (SUPACE) and the Supreme Court Vidhik Anuvaad Software (SUVAS), AI now performs functions that were, until recently, the exclusive preserve of human legal actors (Berk, 2021; Kaur & Kaur, 2024). This article undertakes a critical legal study of the role of AI across the two principal stages of the criminal justice process — investigation and adjudication — situating the analysis within constitutional guarantees of due process, equality, privacy and protection against self-incrimination (Articles 14, 20(3) and 21 of the Constitution of India), and within comparable due-process jurisprudence abroad, most notably *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016) and *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. Employing a doctrinal, analytical and comparative methodology, the study examines statutory and constitutional provisions, judicial pronouncements, and institutional policies governing the use of AI in evidence collection, forensic analysis, bail and sentencing prediction, and judicial case management. The analysis is organised around three research objectives concerning investigation, judicial decision-making, and the legal-ethical implications of algorithmic governance. The study finds that while AI offers demonstrable gains in efficiency, case-clearance rates and access to justice, its unregulated deployment carries a serious risk of eroding due process, entrenching discriminatory bias, and diluting the accountability structures on which criminal justice legitimacy depends. The article concludes by recommending a graduated, rights-based regulatory framework for AI in the Indian criminal justice system, drawing on the risk-based model of the European Union's Artificial Intelligence Act and on emerging Indian data-protection jurisprudence.*

Keywords: Artificial Intelligence; Criminal Justice System; Due Process; Predictive Policing; Algorithmic Sentencing; Right to Privacy; Judicial Automation

I. INTRODUCTION

The emergence of Artificial Intelligence as an instrument of State power represents one of the most consequential legal developments of the twenty-first century. What began as a set of statistical tools for administrative convenience has, within a decade, penetrated the core functions of the criminal justice system — from the moment a First Information Report (FIR) is registered and CCTV footage is analysed, to the moment a sentencing judge weighs a recidivism-risk score, to the moment a High Court uses a translation engine to render a judgment intelligible to a vernacular litigant (Kaur & Kaur, 2024; Ministry of Law and Justice, e-Courts Project, 2023). The term "Artificial Intelligence" is used in this article, consistently with the working definition adopted by the Organisation for Economic Co-operation and Development and echoed in Indian policy literature, to denote a machine-based system that, for a given set of human-defined objectives, generates outputs such as predictions, recommendations, or decisions influencing real or virtual



environments, and that may operate with varying degrees of autonomy (Laksito, 2024, as cited in Artificial Intelligence in Predictive Policing, 2025).

The importance of studying AI in the criminal justice system at the present moment arises from a confluence of three developments. First, the scale of institutional adoption has crossed a threshold: the United States Department of Justice's December 2024 report on AI catalogued its use across forensic science, predictive policing, and correctional administration as a settled feature of the criminal justice landscape rather than an experimental one (Council on Criminal Justice, 2026). Second, in India, the judiciary itself has become an institutional adopter, with the Supreme Court's SUPACE and SUVAS platforms, and an allocation of ₹53.57 crore under Phase III of the e-Courts Mission Mode Project (2023–2027), signalling that AI adoption is no longer confined to policing but extends to the adjudicatory function (Dr. Syama Prasad Mookerjee Research Foundation, 2026; NextIAS, 2025). Third, the constitutional stakes of this adoption have crystallised through litigation: the Wisconsin Supreme Court's decision in *State v. Loomis* (2016) and the pending Indian litigation on facial-recognition deployment at protest sites illustrate that AI in criminal justice is no longer a policy question alone but a live constitutional one, implicating Articles 14, 19, 20(3) and 21 of the Constitution of India (Legal Service India, 2026).

1.1 The Conceptual Framework

For the purposes of this study, the role of AI in the criminal justice system is analysed along four principal dimensions, each of which carries distinct legal consequences and is treated as a lens of analysis throughout the article.

- **Investigative and Evidentiary Dimension:** the use of AI in surveillance, facial recognition, digital forensics, DNA profiling, predictive policing, and the generation of electronic evidence governed by Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (formerly Section 65B of the Indian Evidence Act, 1872) (*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1).
- **Adjudicatory and Sentencing Dimension:** the deployment of risk-assessment and decision-support algorithms such as COMPAS in the United States and analogous case-management tools in Indian courts, raising due-process and equal-protection concerns (*State v. Loomis*, 2016; Berk, 2021).
- **Administrative and Access-to-Justice Dimension:** the use of AI for case listing, translation (SUVAS), legal research assistance (SUPACE), and reduction of pendency, situated within the e-Courts Mission Mode Project (National Judicial Data Grid, 2025).
- **Constitutional and Ethical Dimension:** the interaction of AI with fundamental rights, namely the right to privacy under Article 21 (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017), the protection against self-incrimination under Article 20(3) (*Selvi v. State of Karnataka*, (2010) 7 SCC 263), and the guarantee of equality under Article 14, together with the transparency and accountability principles embedded in India's Digital Personal Data Protection Act, 2023 and the European Union's Artificial Intelligence Act, 2024.

These four dimensions are treated as majorly relevant to the present study because they map directly onto the institutional architecture of the criminal justice system — investigation, adjudication, administration and constitutional oversight — and because, taken together, they illuminate why the current moment demands sustained legal scrutiny rather than purely technological or managerial evaluation.

1.2 The Need of the Study

India's criminal justice system continues to labour under a pendency of over 5.4 crore cases nationwide, with over 87,000 matters pending before the Supreme Court alone as of mid-2025 (Dr. Syama Prasad Mookerjee Research Foundation, 2026). This chronic backlog has made the promise of AI-assisted efficiency politically and administratively attractive, yet the legal community has not kept pace in producing a rigorous doctrinal account of what such automation does to constitutional guarantees of fair trial, non-discrimination and due process. Comparative experience, particularly the COMPAS controversy in the United States and the expanding use of facial-recognition



technology (FRT) by Indian police forces without a dedicated statutory framework, demonstrates that the absence of timely legal scrutiny allows technological infrastructure to outpace the safeguards meant to govern it (Legal Service India, 2026). There is, therefore, a pressing need for a study that integrates constitutional doctrine, statutory interpretation, comparative case law and empirical policy data into a single critical account of AI's role in criminal investigation and adjudication.

1.3 The Significance of the Study

The rationale for this study lies in the widening gap between the pace of AI deployment by law-enforcement and judicial institutions and the pace of legal-regulatory response. Unlike sectors such as banking or telecommunications, where statutory regulators have moved to govern algorithmic decision-making, the criminal justice sector in India continues to operate largely on administrative circulars and institutional discretion rather than a dedicated legislative framework for algorithmic accountability. The purpose of this study is threefold: (a) to map, with precision, the actual and emerging uses of AI across the investigative and adjudicatory stages of the Indian and comparative criminal justice systems; (b) to test these uses against established constitutional and evidentiary doctrine, including the due-process standard articulated in *Maneka Gandhi v. Union of India*, AIR 1978 SC 597, and the privacy doctrine of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017); and (c) to generate policy-relevant recommendations capable of informing a future statutory or regulatory framework for AI in criminal justice. The significance of the study, accordingly, lies not merely in academic description but in its contribution to an urgently needed legal-regulatory conversation.

1.4 The Delimitations of the Study

This study is doctrinal and analytical in nature and does not involve primary empirical data collection such as surveys of police officers, judges or litigants; its findings are accordingly limited to what can be established from statutes, judicial decisions, government reports and peer-reviewed secondary literature. The study focuses primarily on the Indian criminal justice system, with comparative reference to the United States, the United Kingdom and the European Union, and does not purport to offer an exhaustive survey of AI adoption in every jurisdiction. Fast-moving technological and regulatory developments mean that the study reflects the state of law and policy as available up to the time of writing, and later legislative or judicial developments may qualify some of its conclusions. Finally, the study is confined to the criminal justice system and does not extend its analysis to AI in civil litigation, arbitration, or regulatory adjudication, except where such material sheds comparative light on the criminal process.

1.5 Research Questions

RQ1: What is the role of Artificial Intelligence (AI) in criminal investigation and evidence collection?

RQ2: How is Artificial Intelligence (AI) used in judicial decision-making and case management?

RQ3: What are the legal and ethical implications of using Artificial Intelligence (AI) in the criminal justice system?

1.6 Research Objectives

O1: To examine the role of Artificial Intelligence (AI) in criminal investigation and evidence collection.

O2: To analyze the use of AI in judicial decision-making and case management.

O3: To evaluate the legal and ethical implications of AI in the criminal justice system.

II. REVIEW OF RELATED LITERATURE

Council of Europe. (2020). This report of the Council of Europe's Committee on Legal Affairs and Human Rights was among the earliest institutional documents to frame AI in policing and criminal justice explicitly as a human-rights issue rather than a purely technical one, recommending that member states establish independent oversight mechanisms before deploying predictive-policing and risk-assessment tools (as cited in Predictive Policing or Predictive Prejudice?,



2025). Its significance for this study lies in establishing the analytical baseline that algorithmic tools in criminal justice must be evaluated against binding human-rights standards, a premise carried forward throughout the present article's constitutional analysis.

Berk, R. A. (2021) cited review disaggregates the loose popular category of "AI" into its constituent statistical operations, arguing that predictive policing is substantially an exercise in spatial statistics while criminal justice risk assessment is an exercise in adaptive, non-parametric regression. Berk (2021) contends that concerns about accuracy, fairness and transparency are genuine but involve irreducible trade-offs that cannot be resolved by technical fixes alone and instead require political and legal choices. This article draws on Berk's framework to distinguish, throughout the analysis, between the investigative use of AI (predictive policing) and the adjudicatory use of AI (risk assessment at sentencing and bail), treating each as raising distinct legal questions.

Kaur, N., & Kaur, M. (2024) surveys the introduction of SUVAS and SUPACE by the Supreme Court of India and situates them within the broader modernisation of court administration, noting that SUVAS was the first formal step taken by the Indian judiciary toward AI adoption and that SUPACE is designed to collect relevant facts and legal provisions for a judge without itself pronouncing judgment (Kaur & Kaur, 2024). The study also flags an emerging judicial expectation of algorithmic transparency, observing that users of algorithms are increasingly expected to disclose their underlying data and assumptions. This source anchors the present article's discussion of the administrative and access-to-justice dimension of AI in the Indian context.

Lin, L. (2025) examines predictive-policing algorithms as a case study in the legal implications of automated law enforcement, arguing that although proponents present such tools as sources of objectivity and efficiency, the historical crime data on which they are trained often reflects pre-existing patterns of disproportionate policing in minority communities, producing a self-reinforcing cycle of discriminatory enforcement. The study situates this critique within the equal-protection guarantee of the Fourteenth Amendment to the United States Constitution. This source informs the present article's treatment, under Objective 3, of algorithmic bias as a constitutional equality problem rather than a merely technical defect.

Anbarasi, G., & Sankar, D. (2025) examines AI adoption in Indian courts through the specific lens of environmental sustainability, documenting that SUVAS had translated more than 36,271 Supreme Court judgments into Hindi and 17,142 into other regional languages by 2024, and that virtual hearings between 2020 and 2023 are estimated to have prevented approximately 50,000 metric tons of carbon emissions through reduced travel (Anbarasi & Sankar, 2025). While its central concern is environmental, the study is significant for this article because it provides verifiable, government-linked implementation data on the scale of AI adoption in Indian courts, and because it identifies the absence of comprehensive legislation governing AI in the judiciary as a continuing structural gap — a gap this article addresses directly under Objective 3.

III. THE METHODOLOGY OF THE STUDY

This study adopts a doctrinal legal research methodology, supplemented by an analytical and comparative approach. The doctrinal method involves the systematic identification, interpretation and critical analysis of primary legal sources, including the Constitution of India, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, together with judicial pronouncements of the Supreme Court of India and comparative courts.

Secondary sources consulted include peer-reviewed journal articles, government and institutional reports (including the United States Department of Justice's December 2024 report on AI in criminal justice, reports of the Council of Europe, and Indian e-Courts Project documentation), and law-review commentary, all collected through a purposive, non-random search strategy targeting literature published between 2020 and 2026, in keeping with the recency required by the subject-matter.



The comparative method is employed to juxtapose Indian constitutional doctrine with foreign case law, principally the due-process jurisprudence of the Wisconsin Supreme Court in *State v. Loomis* (2016) and the risk-based regulatory model of the European Union's Artificial Intelligence Act, 2024, in order to test the adequacy of the existing Indian legal framework and to identify transplantable regulatory principles. The analytical method is applied in Section 4 to interpret the collected material against the three research objectives, using a thematic framework organised around investigation, adjudication, and legal-ethical implications. As the study is doctrinal, no primary data was collected from human subjects, and consequently no institutional ethical clearance was required; all secondary material is cited and attributed in accordance with the American Psychological Association's (APA) seventh-edition referencing style.

IV. ANALYSIS AND INTERPRETATION

The Role of Artificial Intelligence in Criminal Investigation and Evidence Collection

AI has transformed the investigative stage of the criminal process most visibly through predictive policing, facial-recognition technology (FRT), digital forensics, and automated evidence generation. Predictive policing systems apply statistical and machine-learning models to historical crime data in order to forecast the times, locations and, in some deployments, the individuals associated with heightened risk of criminal activity (Ji-min & Mi-geon, 2024, as cited in *Predictive Policing or Predictive Prejudice?*, 2025). In India, AI is increasingly used by law enforcement for data analysis, crime detection, surveillance and predictive policing, with tools such as AI-enhanced CCTV analysis software supporting investigation and evidence handling, while prosecutors employ AI to assist in filing First Information Reports and analysing witness testimony (Oxford Institute of Technology and Justice, 2026).

The constitutional significance of these tools lies chiefly in their intersection with the right to privacy. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, a nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21, and is further protected as an element of the freedoms guaranteed under Part III of the Constitution. The Court laid down a three-fold test for any State action restricting privacy — legality, legitimate aim, and proportionality — a test that applies with particular force to AI-enabled surveillance and facial-recognition deployment, since such systems collect and process biometric data typically without the specific, informed consent of the individuals concerned (*Right to Privacy Under Article 21 Versus AI Surveillance*, 2026).

The absence of a dedicated statute governing police use of FRT in India has itself become the subject of constitutional litigation. Recent proceedings before the Supreme Court concerning the deployment of facial-recognition technology at protest sites raise questions squarely under Article 21 (privacy), Article 19(1)(a) (freedom of speech and expression), Article 19(1)(b) (freedom of peaceful assembly), and Article 14 (protection against arbitrary State action), and commentators have suggested that the resulting judgment may become, for AI-based surveillance, what *Puttaswamy* became for informational privacy generally (*Legal Service India*, 2026).

A second investigative concern involves self-incrimination. In *Selvi v. State of Karnataka*, (2010) 7 SCC 263, the Supreme Court held that the involuntary administration of narco-analysis, polygraph and brain-electrical-activation-profile tests violates both Article 20(3) (the right against self-incrimination) and Article 21 (the right to personal liberty and privacy), and that such techniques may be used only with the subject's informed consent, administered in accordance with guidelines framed by the National Human Rights Commission. Although *Selvi* predates the current generation of AI-driven investigative tools, its reasoning — that the State may not extract or infer testimonial material from an unwilling mind through technological means — provides a directly applicable constitutional template for evaluating AI systems that purport to infer intent, deception or culpability from biometric or behavioural data.

A third dimension concerns the admissibility of AI-generated and other electronic evidence. Under Section 63 of the *Bharatiya Sakshya Adhiniyam*, 2023 (the successor, with effect from 1 July 2024, to Section 65B of the Indian Evidence Act, 1872), electronic records are admissible only upon compliance with prescribed certification requirements. The Supreme Court's decisions in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, established that a certificate under the electronic-evidence



provision is a mandatory pre-condition for the admissibility of electronic records, including, by extension, records or outputs generated or processed by AI-based forensic tools such as AMPED FIVE video-analysis software (Oxford Institute of Technology and Justice, 2026). This body of doctrine means that AI-generated investigative outputs cannot simply be presented as self-proving; they must be authenticated through the same statutory chain-of-custody discipline applied to conventional electronic evidence, and their probative weight remains subject to judicial scrutiny of the underlying algorithm's reliability.

Comparatively, the United States has confronted analogous questions in the context of digital-location evidence, most notably in *Carpenter v. United States*, 585 U.S. 296 (2018), where the Supreme Court held that the government's acquisition of historical cell-site location information constitutes a Fourth Amendment search requiring a warrant, recognising that the aggregation and analytic processing of digital data by automated systems raises privacy concerns qualitatively different from isolated pieces of evidence. Although *Carpenter* did not directly concern AI, its underlying logic — that automated, continuous, retrospective analysis of personal data implicates constitutional protections in a manner that occasional human observation does not — has been influential in subsequent debates about AI-enabled investigative surveillance.

In summary, the investigative role of AI spans predictive policing, biometric surveillance, forensic analytics and the generation of digital evidence, and each application must be tested not merely for operational efficiency but against the constitutional triad of privacy (Article 21), protection from arbitrary State action (Article 14), and protection against self-incrimination (Article 20(3)), together with the statutory evidentiary safeguards of the *Bharatiya Sakshya Adhiniyam*, 2023.

The Use of Artificial Intelligence in Judicial Decision-Making and Case Management

At the adjudicatory stage, AI performs two analytically distinct functions: (i) substantive decision-support, where algorithmic outputs inform decisions on bail, sentencing or risk of recidivism; and (ii) administrative case management, where AI supports research, translation, listing and pendency reduction without directly influencing the merits of a case.

The leading illustration of the first function is the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) risk-assessment tool considered in *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016). In that case, a sentencing court considered a COMPAS-generated risk score, contained in a Presentence Investigation Report, as one factor in denying the defendant probation. The defendant challenged the use of the tool on due-process grounds, arguing that its proprietary, "black-box" nature prevented him from challenging its scientific validity, and that its consideration of gender as an input variable was constitutionally impermissible (Studicata, 2026). The Supreme Court of Wisconsin held that the use of a COMPAS risk assessment at sentencing does not violate due process provided that it is not the determinative factor in the sentencing decision and is accompanied by defined cautions and disclosures, including a written advisement alerting the sentencing court to the proprietary nature of the tool, its use of group-based rather than individualised data, and the absence of cross-validation on the local offender population (*State v. Loomis*, 2016, ¶¶ 98–101; Justia, 2026). The United States Supreme Court subsequently denied certiorari in the related petition, *Loomis v. Wisconsin*, 137 S. Ct. 2290 (2017), leaving the Wisconsin court's reasoning as the most authoritative judicial treatment of algorithmic sentencing to date (Wikipedia, 2026).

Loomis is significant for this study because it establishes a judicially workable, if contested, middle path between wholesale prohibition and unregulated use of algorithmic decision-support in adjudication: courts may consider such tools, but only as one input among several, and only where procedural safeguards preserve the defendant's ability to contextualise and challenge the algorithmic output. Whether an equivalent safeguard structure would satisfy the stricter due-process standard articulated by the Indian Supreme Court in *Maneka Gandhi v. Union of India*, AIR 1978 SC 597 — under which any procedure depriving a person of life or personal liberty must be fair, just and reasonable, and not arbitrary or oppressive — remains an open and, in the present author's assessment, doctrinally significant question,



since Maneka Gandhi's insistence on substantive fairness arguably demands a more exacting standard of algorithmic transparency than Loomis required.

In the Indian context, AI has so far been deployed almost exclusively in the second, administrative function. SUPACE (Supreme Court Portal for Assistance in Court's Efficiency) is designed to assist judges by scanning large volumes of case files and surfacing relevant precedents, statutes and legal principles; it does not itself pronounce judgment, and the former Chief Justice of India has publicly confirmed that the tool is not intended to spill over into judicial decision-making (Oxford Institute of Technology and Justice, 2026; Medicaps University, 2025). As of early 2026, SUPACE's deployment has been limited primarily to select criminal matters before judges of the Bombay and Delhi High Courts, with wider rollout constrained less by software capability than by the hardware infrastructure — high-grade GPUs and TPUs — required for deep-learning models to operate efficiently at scale (Dr. Syama Prasad Mookerjee Research Foundation, 2026).

SUVAS (Supreme Court Vidhik Anuvaad Software), the companion translation tool, addresses a distinct constitutional concern: Article 348(1)(a) of the Constitution of India mandates that English remain the authoritative language of proceedings and judgments of the Supreme Court and the High Courts, a rule that can operate as a practical barrier to access to justice for litigants unfamiliar with English. SUVAS mitigates this barrier by producing translated versions of judgments for informational purposes, and had translated more than 31,000 judgments by the end of 2023, with volumes continuing to rise through 2025, particularly in Hindi, Punjabi and Kannada across the Allahabad, Delhi and Kerala High Courts (Dr. Syama Prasad Mookerjee Research Foundation, 2026).

These initiatives sit within the broader e-Courts Mission Mode Project, under whose Phase III (2023–2027) the Union Government has allocated approximately ₹7,210 crore, of which ₹53.57 crore is earmarked specifically for the integration of AI and blockchain technologies across High Courts (NextIAS, 2025). The scale of institutional pendency that motivates this investment is considerable: the National Judicial Data Grid recorded approximately 3.89 crore cases pending at the district and taluka level and 58.43 lakh cases pending before the High Courts, alongside over 87,000 matters before the Supreme Court as of mid-2025 (IndiaAI, 2026; Dr. Syama Prasad Mookerjee Research Foundation, 2026).

Comparative experience illustrates a spectrum of adjudicatory AI adoption considerably broader than the Indian model: the United Kingdom has deployed HART (Harm Assessment Risk Tool) to inform custody decisions, China's "Smart Court" system draws on stored case data to expedite decisions in similar matters, and Estonia has piloted an automated adjudicator for certain small-claims disputes (Drishti IAS, 2025; IndiaAI, 2026). This spectrum underscores that the Indian judiciary's current posture — confining AI strictly to research assistance and translation while withholding it from substantive decision-making — reflects a deliberate and comparatively cautious institutional choice, one broadly consistent with the due-process concerns identified in Loomis and with the heightened protection Indian constitutional doctrine affords to personal liberty.

The Legal and Ethical Implications of Artificial Intelligence in the Criminal Justice System

The legal and ethical implications of AI in criminal justice can be organised around four recurring concerns identified throughout the preceding analysis: algorithmic bias and the guarantee of equality; transparency and the right to a reasoned, challengeable decision; privacy and data protection; and the absence of a dedicated regulatory framework.

First, algorithmic bias implicates the guarantee of equality before the law under Article 14 of the Constitution of India and its comparative analogue, the Equal Protection Clause of the Fourteenth Amendment to the United States Constitution. Because predictive-policing and risk-assessment algorithms are trained on historical crime and arrest data, they risk encoding and perpetuating pre-existing patterns of disproportionate enforcement against particular communities, producing what critics describe as a self-reinforcing cycle of algorithmically legitimised discrimination (Lin, 2025). This concern was expressly before the Wisconsin Supreme Court in Loomis, where the defendant argued that COMPAS's consideration of gender was constitutionally impermissible; the court's acceptance of gender as a permissible input, provided it served a non-discriminatory, accuracy-enhancing purpose and was not the sole basis for



the decision, illustrates the difficulty of translating anti-discrimination doctrine, developed for individualised human decision-making, into the register of statistical group-based prediction (Harvard Law Review, 2026).

Second, transparency concerns arise from the frequently proprietary, "black-box" architecture of AI tools used in criminal justice. The core due-process objection sustained (though ultimately not accepted) in Loomis — that a defendant cannot meaningfully contest a sentencing factor whose internal logic is a trade secret — remains, in the present author's assessment, only partially resolved by disclosure of aggregate validation statistics, since such disclosure does not permit challenge to the specific weighting applied in an individual case. Indian commentary has begun to articulate an emerging expectation that users of algorithms in legal processes must publicly disclose their choices, data and assumptions in a comprehensive, timely and accessible manner (Kaur & Kaur, 2024), though this expectation has not yet crystallised into binding statutory obligation in the criminal justice context specifically.

Third, privacy and data protection concerns are addressed only partially by existing Indian law. The Digital Personal Data Protection Act, 2023 establishes general principles of purpose limitation, data minimisation and accountability for the processing of personal data, and grants individuals a right to seek information about data collected from them (IndiaAI, 2026); however, the Act contains broad exemptions for processing undertaken by the State in the interests of the security of the State and the prevention, detection, investigation or prosecution of offences, which risks placing precisely the AI-enabled investigative tools discussed under Objective 1 — predictive policing and facial recognition — largely outside the Act's operative discipline. This gap leaves the constitutional proportionality test articulated in Puttaswamy (2017) as the primary, and in practice the only readily invocable, safeguard against disproportionate AI-enabled surveillance in the investigative context.

Fourth, and consequently, the absence of a dedicated legislative framework governing AI in criminal justice remains the central structural deficiency identified across the literature reviewed in Section 2. Anbarasi and Sankar (2025) explicitly identify the need for comprehensive legislation governing AI use in the judiciary as a continuing challenge, notwithstanding the operational successes of SUVAS and SUPACE, while the Legal Service India commentary on the pending facial-recognition litigation observes that India "presently lacks a dedicated law comprehensively regulating police deployment of facial recognition technology" (Legal Service India, 2026). By contrast, the European Union's Artificial Intelligence Act, which entered into force in 2024, adopts an explicitly risk-tiered regulatory architecture that classifies certain law-enforcement uses of AI — including specific forms of biometric categorisation and individual risk-assessment profiling — as "high-risk" or, in narrowly defined circumstances, prohibited outright, subject to conformity assessment, human oversight and fundamental-rights impact assessment obligations. This risk-tiered model offers a transplantable template for a future Indian statutory framework, one capable of reconciling the efficiency gains documented under Objectives 1 and 2 with the constitutional safeguards demanded by Puttaswamy, Selvi and Maneka Gandhi.

Taken together, these four implications demonstrate that the legal challenge posed by AI in criminal justice is not a challenge of technological capability but of institutional accountability: existing constitutional doctrine supplies the normative standards — proportionality, fairness, non-arbitrariness, and protection against self-incrimination — but India currently lacks the statutory and institutional infrastructure required to operationalise those standards specifically against algorithmic decision-making.

V. MAJOR FINDINGS

AI's investigative role in India is substantial and expanding, encompassing predictive policing, facial-recognition surveillance, and AI-assisted forensic and digital-evidence analysis, yet it operates without a dedicated statute and relies instead on the general constitutional proportionality test laid down in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).

The Indian judiciary has, to date, confined AI adoption to the administrative and research-assistance function (SUPACE, SUVAS) and has consciously withheld it from substantive adjudicatory decision-making, a posture that is more cautious than several comparative jurisdictions but is not yet backed by binding statutory limits.



Comparative jurisprudence, principally *State v. Loomis* (2016), demonstrates that even where courts permit algorithmic risk assessment at sentencing, they do so only subject to significant procedural safeguards — non-determinativeness, disclosure of validation limitations, and periodic re-norming — safeguards not yet mirrored in binding Indian doctrine or statute.

Electronic and AI-generated evidence remains subject to the strict certification discipline established under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, and the Supreme Court's rulings in *Anvar P.V.* (2014) and *Arjun Panditrao Khotkar* (2020), meaning AI outputs cannot bypass conventional standards of evidentiary authentication.

Algorithmic bias, opacity, and gaps in India's Digital Personal Data Protection Act, 2023 (particularly its law-enforcement exemptions) together constitute the most significant unresolved legal and ethical risks identified in this study, echoing concerns raised in comparative literature on predictive policing (Lin, 2025; Berk, 2021).

India presently lacks a dedicated, risk-tiered statutory framework for AI in criminal justice comparable to the European Union's Artificial Intelligence Act, 2024, and this legislative gap is the central structural finding of the study.

VI. CONCLUSION

This study set out to examine, through a doctrinal and comparative legal lens, the role of Artificial Intelligence across the investigative and adjudicatory stages of the criminal justice system. The analysis confirms that AI has already become deeply embedded in criminal investigation — through predictive policing, facial recognition and digital forensics — and, more cautiously, in judicial administration, through tools such as SUPACE and SUVAS. It further confirms that comparative jurisdictions, particularly the United States through *State v. Loomis* (2016), have begun to develop judicially crafted safeguards for algorithmic decision-making, while India's constitutional doctrine, anchored in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), *Selvi v. State of Karnataka* (2010), and *Maneka Gandhi v. Union of India* (1978), supplies a normatively demanding but as yet under-operationalised standard against which such tools must be tested.

The central conclusion of this study is that the principal legal deficiency in India is not an absence of applicable constitutional principle but an absence of statutory translation: the proportionality, fairness and non-arbitrariness standards developed by the Supreme Court exist in the abstract but have not been codified into binding, AI-specific obligations of transparency, auditability, and human oversight applicable to police and judicial use of algorithmic tools. Accordingly, this study recommends that any future Indian legislative response adopt a risk-tiered structure broadly comparable to the European Union's Artificial Intelligence Act, 2024, imposing heightened conformity-assessment, disclosure and human-oversight obligations on "high-risk" criminal-justice applications of AI — including predictive policing, facial recognition, and any future adoption of algorithmic sentencing or bail-risk tools — while allowing continued, lightly regulated use of purely administrative applications such as SUVAS and SUPACE. Only through such codification can the considerable efficiency gains AI offers to a chronically overburdened criminal justice system be reconciled with the constitutional guarantees of due process, equality, privacy and protection against self-incrimination that remain the irreducible foundation of criminal justice legitimacy.

REFERENCES

1. Anbarasi, G., & Sankar, D. (2025). Greening the justice system: Assessing the legality, feasibility, and potential of artificial intelligence in advancing environmental sustainability within the Indian judiciary. *Frontiers in Political Science*. <https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1553705/pdf>
2. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
3. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
4. Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4, 209–237. <https://doi.org/10.1146/annurev-criminol-051520-012342>
5. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).



6. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
7. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
8. *Carpenter v. United States*, 585 U.S. 296 (2018).
9. Constitution of India, 1950, arts. 14, 19, 20(3), 21, 348(1)(a).
10. Council of Europe. (2020). *Justice by algorithm: The role of artificial intelligence in policing and criminal justice systems*. Committee on Legal Affairs and Human Rights, Parliamentary Assembly. <https://pace.coe.int/en/files/28723/html>
11. Council on Criminal Justice. (2026). *DOJ report on AI in criminal justice: Key takeaways*. <https://counciloncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/>
12. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
13. Dr. Syama Prasad Mookerjee Research Foundation. (2026). *Artificial intelligence in the Indian judiciary: SUPACE, SUVAS, and the limits of assistive automation*. <https://spmrf.org/artificial-intelligence-in-the-indian-judiciary-supace-suvas-and-the-limits-of-assistive-automation/>
14. Drishti IAS. (2025). *Artificial intelligence in judiciary*. <https://www.drishtias.com/daily-news-analysis/artificial-intelligence-in-judiciary>
15. European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
16. Harvard Law Review. (2026). *State v. Loomis*. <https://harvardlawreview.org/print/vol-130/state-v-loomis/>
17. IndiaAI. (2026). *Can artificial intelligence (AI) revolutionize India's judiciary system?* <https://indiaai.gov.in/article/can-artificial-intelligence-ai-revolutionize-india-s-judiciary-system>
18. Justia. (2026). *State v. Loomis, Wisconsin Supreme Court (2016)*. <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>
19. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
20. Kaur, N., & Kaur, M. (2024). Role of artificial intelligence in the Indian courts. *International Journal of Law, Policy and Social Review*, 6(1), 17–20. <https://www.lawjournals.net/assets/archives/2024/vol6issue1/5124.pdf>
21. Legal Service India. (2026). *Facial recognition technology at protest sites: Supreme Court to examine AI surveillance, privacy & protest rights*. <https://www.legalserviceindia.com/Legal-Articles/facial-recognition-technology-at-protest-sites-supreme-court-ai-surveillance-india/>
22. Lin, L. (2025). Algorithmic justice or bias: Legal implications of predictive policing algorithms in criminal justice. *Johns Hopkins Undergraduate Law Review*. <https://jhulr.org/2025/01/01/algorithmic-justice-or-bias-legal-implications-of-predictive-policing-algorithms-in-criminal-justice/>
23. *Loomis v. Wisconsin*, 137 S. Ct. 2290 (2017).
24. *Maneka Gandhi v. Union of India*, AIR 1978 SC 597 (India).
25. Mediacaps University. (2025). *How artificial intelligence is revolutionizing the Indian legal systems*. <https://www.medicaps.ac.in/blog/how-artificial-intelligence-is-revolutionizing-the-indian-legal-system>
26. NextIAS. (2025). *Integrating AI in India's judiciary and law enforcement*. <https://www.nextias.com/ca/current-affairs/27-02-2025/integrating-ai-in-india-judiciary-and-law-enforcement>
27. Oxford Institute of Technology and Justice. (2026). *India: Increasing use of AI across the justice system*. <https://www.techandjustice.bsg.ox.ac.uk/research/india>
28. Predictive policing or predictive prejudice? A study of the legal, historical and ethical implications of AI in policing. (2025). *OxJournal*. <https://www.oxjournal.org/predictive-policing-or-predictive-prejudice/>
29. Right to privacy under Article 21 versus AI surveillance. (2026). *International Journal of Enhanced Research and Development*. <https://rjwave.org/ijedr/papers/IJEDR2601236.pdf>
30. *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).
31. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).



32. Studicata. (2026). *State v. Loomis – Case brief summary*. <https://www.studicata.com/case-briefs/case/state-v-loomis>
33. Wikipedia. (2026). *Loomis v. Wisconsin*. https://en.wikipedia.org/wiki/Loomis_v._Wisconsin

