INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 1 | 2026 Art. 17

Artificial Intelligence in the Criminal Justice System: Opportunities, Challenges, and Legal Imperatives

Gargi Verma
Law Student,
Army Institute of Law, Mohali

Recommended Citation
Gargi Verma, *Artificial Intelligence in the Criminal Justice System: Opportunities, Challenges, and Legal Imperatives*, 5 IJHRLR 255-264 (2026).
Available at www.humanrightlawreview.in/archives/.

Artificial Intelligence in the Criminal Justice System: Opportunities, Challenges, and Legal Imperatives

Gargi Verma
Law Student,
Army Institute of Law, Mohali

Manuscript Received	Manuscript Accepted	Manuscript Published
30 Jan. 2026	05 Feb. 2026	08 Feb. 2026

ABSTRACT

The integration of artificial intelligence (AI) into the criminal justice system represents a transformative shift, promising enhanced efficiency in law enforcement while raising profound legal and ethical concerns. This paper explores the multifaceted role of AI in policing, predictive analytics, and judicial processes, drawing on global and Indian contexts to assess its potential to revolutionize crime prevention and investigation. Key applications include facial recognition for identification, anomaly detection for real-time surveillance, and predictive models to forecast crime hotspots, which enable proactive resource allocation and deter criminal activities. However, these advancements are shadowed by critical challenges: pervasive privacy invasions through unchecked data collection, algorithmic biases that perpetuate systemic discrimination, and accountability deficits in opaque "black box" systems. These issues intersect with fundamental human rights, including the right to privacy under Article 21 of the Indian Constitution , as affirmed in landmark judgments like Justice K.S. Puttaswamy (Retd.) v. Union of India . The paper argues for a balanced regulatory framework that harnesses AI's benefits while mitigating risks, emphasizing transparency, bias audits, and judicial oversight. Through an analysis of real-world implementations, such as the Los Angeles Police Department's use of PredPol and India's Bureau of Police Research and Development's predictive policing initiative for women's safety, it underscores the need for context-specific legal reforms. Ultimately, AI must serve justice as a tool for equity, not exacerbating inequalities. This study contributes to the discourse on technology-driven jurisprudence, advocating for interdisciplinary approaches to ensure AI aligns with constitutional mandates and international human rights standards.

KEYWORDS

Artificial Intelligence, Criminal Justice, Predictive Policing, Privacy Rights, Algorithmic Bias, Human Rights, Indian Constitution.

INTRODUCTION

The criminal justice system, as the bedrock of societal order, has long grappled with the dual imperatives of deterrence and fairness. In an era defined by rapid technological evolution, artificial intelligence (AI) emerges as a potent instrument to augment these functions. AI, encompassing machine learning algorithms capable of processing vast datasets to identify patterns and make predictions, is increasingly embedded in law enforcement practices worldwide. From automated facial recognition to predictive crime mapping, AI promises to streamline investigations, optimize resource deployment, and preempt offenses, thereby fostering a more responsive justice apparatus. Yet, this infusion is not without peril. The opacity of AI decision-making processes, coupled with its reliance on historical data fraught with societal biases, poses existential threats to core legal principles such as due process, equality before the law, and the presumption of innocence[1].

In India, where the criminal justice ecosystem—comprising law enforcement, judiciary, and correctional services—strains under resource constraints and mounting caseloads, AI adoption holds particular promise. The National Crime Records Bureau's digitization efforts and initiatives like the e-Courts project signal a readiness to leverage technology for efficiency. However, the absence of comprehensive regulatory frameworks amplifies risks, as evidenced by concerns over surveillance under the Information Technology Act, 2000, and constitutional safeguards[2]. Globally, precedents like the United States' COMPAS recidivism tool highlight how AI can entrench racial disparities, prompting judicial scrutiny in cases such as *State v. Loomis*[3]. This paper delves into AI's applications within the criminal justice paradigm, with a focus on policing, while interrogating attendant legal challenges. It posits that while AI can enhance preventive justice, its deployment must be circumscribed by robust legal guardrails to uphold human dignity and equity.

THE CRIMINAL JUSTICE SYSTEM: FOUNDATIONS AND

[1] V.R. Krishna Iyer, Justice at Crossroads: A View from the Bench 150 (Excel Books, New Delhi, 2003).
[2] Information Technology Act, 2000 s 69.
[3] 881 NW 2d 749 (Wis 2016).

COMPONENTS

At its core, the criminal justice system constitutes an interconnected matrix of institutions designed to uphold the rule of law, mitigate deviance, and safeguard communal welfare. Encompassing law enforcement agencies, adjudicatory bodies, and rehabilitative mechanisms, it orchestrates the continuum from crime detection to offender reintegration. In India, this triad—police, courts, and prisons—operates under constitutional imperatives, with the Directive Principles of State Policy underscoring preventive strategies against crime[4]. The police, as the frontline sentinel, enforce penal statutes like the Indian Penal Code, 1860, while courts interpret and apply justice through adversarial proceedings. Correctional institutions, governed by the Prisons Act, 1894, emphasize reform over retribution, aligning with rehabilitative ideals enshrined in *Sunil Batra v. Delhi Administration* [5]

This system's efficacy hinges on collaborative synergy, yet inefficiencies—such as investigative delays and judicial backlogs—persist. AI's ingress offers remedial potential by automating routine tasks and augmenting analytical capacities. For instance, AI-driven case management tools can triage dockets, expediting resolutions in line with the right to speedy trial under Article 21[6]. Nonetheless, integration demands fidelity to procedural safeguards, lest it erode the human element central to justice administration. As the Supreme Court observed in *Hussainara Khatoon v. Home Secretary, State of Bihar*, justice delayed is justice denied; AI, if judiciously harnessed, could invert this axiom.[7]

AI IN POLICING: TECHNOLOGICAL AUGMENTATIONS

Policing, the vanguard of criminal justice, entails vigilant enforcement to preserve order and avert infractions. AI's permeation herein manifests through sophisticated tools that transcend traditional methodologies, enabling nuanced interventions. Globally, law enforcement entities deploy AI for multifaceted purposes: discerning identities, monitoring trajectories, flagging aberrations, forecasting threats, scrutinizing affective cues, and delineating relational networks. These applications, while bolstering operational prowess, necessitate vigilant oversight to avert overreach[8].

[4] Constitution of India arts 38-39.
[5] (1978) 4 SCC 494.
[6] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 para 267.
[7] (1979) 1 SCC 81.
[8] Council on Criminal Justice, The Implications of AI for Criminal Justice

Identification technologies exemplify AI's precision-enhancing role. Facial recognition algorithms, leveraging convolutional neural networks, corroborate identities by juxtaposing biometric markers against databases, as in verifying credentials at checkpoints. In India, the Aadhaar-enabled biometric system integrates such capabilities, though tempered by *Puttaswamy* case, mandates against disproportionate surveillance[9]. Automated fingerprint analysis, impervious to partial impressions, accelerates matches in forensic labs, while gait recognition deciphers ambulatory idiosyncrasies for non-intrusive profiling. Voice biometrics and AI-optimized DNA sequencing further expedite evidentiary linkages, reducing human error in high-stakes probes.

Tracking mechanisms extend this vigilance into spatiotemporal domains. Computer vision algorithms parse video feeds to pursue subjects across surveillance grids, factoring velocity and morphology for continuity. Vehicular oversight, via license plate readers and drone analytics, chronicles mobility patterns, aiding pursuits or abductions inquiries. In urban India, initiatives like Delhi's Integrated Traffic Management System employ AI to monitor flows, preempting disruptions while raising positional privacy queries under the Telegraph Act, 1885[10].

Detection paradigms harness AI's acuity for anomaly discernment. Machine learning models, trained on baseline norms, isolate deviations—be it anomalous financial trails signaling laundering or acoustic sensors pinpointing gunfire via networks like ShotSpotter. Weapons detection at perimeters employs terahertz imaging augmented by AI, curtailing threats at public venues. These tools, by furnishing instantaneous alerts, empower preemptive responses, yet their deployment must conform to reasonableness under Article 14, as judicially expounded in *Maneka Gandhi v. Union of India*[11]

Associational mapping unveils covert affiliations, pivotal in organized crime dismantlement. Convoy detection in vehicular data clusters co-traveling units, inferring conspiracies, while social network analytics visualize interpersonal webs from digital footprints. In counter-terrorism, such as post-26/11 reforms, AI sifts communication intercepts, though bounded by the Unlawful Activities (Prevention) Act, 1967's procedural rigor.[12] Collectively, these integrations amplify policing's prophylactic efficacy, yet they

(2023), available at https://councilоncj.org/the-implications-of-ai-for-criminal-justice/, (last visited on November 17, 2025).

[9] (2017) 10 SCC 1.

[10] Indian Telegraph Act, 1885 s 5.

[11] (1978) 1 SCC 248.

[12] Unlawful Activities (Prevention) Act, 1967 s 4.

imperil civil liberties if unmoored from legal anchors.

PREDICTIVE POLICING: FORECASTING CRIME AND ALLOCATING RESOURCES

Predictive policing epitomizes AI's prognostic prowess, employing statistical inference and machine learning to anticipate criminal occurrences. By ingesting historical offenses, geospatial metrics, climatic variables, and socioeconomic indices, algorithms delineate propensity zones and temporal spikes. This foresight, akin to meteorology's predictive models, empowers strategic deployments, mitigating reactive paradigms' limitations[13].

Three archetypal models delineate this domain. Place-centric systems dissect locales for elevated risk, channeling patrols to nascent hotspots via kernel density estimations. Person-oriented frameworks profile at-risk actors—perpetrators or victims—drawing on actuarial data like prior convictions or vulnerability indices. Resource optimization synthesizes these, dynamically routing assets to maximize deterrence, often via graph theory for patrol graphing.

Advantages abound: proactive interdiction curtails incidents, as evidenced by a 12% property crime dip in PredPol trials.[14] Fiscal prudence accrues from judicious allocations, while real-time adaptability via continual retraining sustains relevance amid evolving threats. In India, the Bureau of Police Research and Development's "Predictive Policing for Women Safety" prototype exemplifies this, fusing multi-source inputs into geospatial advisories for dynamic patrols, addressing gendered violence under the Protection of Women from Domestic Violence Act, 2005[15].

NAVIGATING CHALLENGES: PRIVACY, BIAS, AND ACCOUNTABILITY IN AI DEPLOYMENT

AI's justice foray is encumbered by tripartite perils: privacy erosion, entrenched biases, and evasive accountability, each demanding juridical remediation. Privacy, enshrined as a fundamental right post- Puttaswamy, confronts "surveillance capitalism's" specter, wherein indiscriminate data harvests—sans

[13] Brennan Center for Justice, Predictive Policing Explained (2020), available at https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained/, (last visited on November 17, 2025).

[14] PredPol Inc, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations 45 (PredPol Inc, Santa Cruz, 2018).

[15]Bureau of Police Research and Development, Project Report on Predictive Policing for Women Safety 12 (Ministry of Home Affairs, New Delhi, 2020), available at https://bprd.nic.in/uploads/pdf/Predictive%20Policing%20for%20Women.pdf/, (last visited on November 17, 2025).

informed consent—forge panoptic profiles[16]. Facial tracking and locational pings, while investigative boons, vitiate autonomy, chilling expression under Article 19(1)(a). Remedies entail data minimization and anonymization, aligned with the Personal Data Protection Bill's contours. Bias, an algorithmic inheritance from prejudiced archives, manifests as disparate impacts. The COMPAS tool's racial skew, 45% false positives for Black recidivists versus 23% for whites mirrors Amazon's gendered hiring rebuff, where male-dominated resumes inculcated misogyny[17]. In India, caste-inflected policing data could exacerbate untouchability vestiges, contravening Article 17. Mitigation via diverse datasets and equity audits is imperative, as urged in *Indra Sawhney v. Union of India* for affirmative calibrations.[18]

REAL-LIFE APPLICATIONS: LESSONS FROM GLOBAL AND INDIAN IMPLEMENTATIONS

Empirical vignettes illuminate AI's tangible imprint, offering pragmatic insights into its scalability and pitfalls. The LAPD's PredPol deployment slashed burglaries by 12%, optimizing beats via risk terrains derived from historical data, though subsequent audits revealed over-policing in minority neighborhoods, prompting ethical recalibrations and eventual program suspension amid civil rights concerns[19]. UK's West Midlands digitized reports, trimming processing by 40% through Capita's AI, which automated incident logging and pattern recognition, thereby enhancing officer mobility and investigative throughput while integrating GDPR-compliant data protocols to safeguard privacy[20]. NYPD's BriefCam analytics expedited subway responses by sifting hours of footage in minutes, identifying anomalies like crowd surges or abandoned packages, which supported rapid interventions during events like the 2021 Times Square incident; yet, it faced lawsuits over biased facial matching, underscoring the need for diverse training datasets. Singapore's Azure chatbot,

[16] Federal Trade Commission, FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance (2024), available at https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance/,(last visited on November 17, 2025).

[17] ProPublica, "Machine Bias", available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing/, (last visited on November 17, 2025).

[18] (1992) Supp (3) SCC 217.

[19] The Guardian, LAPD ended predictive policing programs amid public outcry. A new study shows how they validated existing patterns of policing (2021), available at https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform/, (last visited on November 17, 2025).

[20] Capita, AI in Public Sector: Case Studies from UK Policing 22 (Capita PLC, London, 2022).

handling over 100,000 inquiries annually on crime prevention and procedural guidance, alleviated query burdens on handlers, boosting citizen satisfaction scores by 25% and exemplifying AI's role in community-oriented policing.[21]

In India, BPR&D's women-safety module dynamically maps hotspots by integrating FIRs, social media signals, and geospatial data, enabling predictive patrols that reduced reported assaults by 15% in pilot districts like Hyderabad, aligning with the Criminal Law (Amendment) Act, 2013's emphasis on gender-sensitive enforcement. This initiative, powered by a core AI engine processing multi-format inputs, not only guides vehicle routines but also flags vulnerability clusters, fostering inter-agency collaboration with NGOs for holistic interventions.

CONCLUSION

AI's foray into criminal justice heralds efficiency yet summons sagacity, demanding a paradigm shift from unchecked innovation to rights-anchored governance. A rights-resilient framework encompassing legislative codification like an AI Ethics Act mandating transparency disclosures, judicial precedents evolving Puttaswamy's proportionality lens for algorithmic scrutiny, and ethical protocols such as independent oversight boards is paramount. India, poised at this crossroads amid its digital public infrastructure boom, must legislate AI governance to harmonize innovation with justice's sanctity, perhaps drawing from the EU AI Act's risk-tiered approach while indigenizing it through caste-sensitive bias mitigations. Policymakers should prioritize pilot evaluations with sunset clauses, ensuring AI tools sunset if they fail equity benchmarks, while fostering public-private partnerships for open-source auditing tools. Judicially, courts could mandate "explainability riders" in AI-influenced decisions, akin to Loomis' advisories, empowering defendants to challenge opaque outcomes. Internationally, aligning with UN Guidelines on AI and Human Rights would bolster India's global stature in tech diplomacy.[22] Ultimately, AI's true measure lies not in predictive accuracy but in equitable outcomes; by embedding constitutional ethos equality, dignity, and accountability.

BIBLIOGRAPHY

Brennan Center for Justice, *Predictive Policing Explained* (2020),

[21] Microsoft, Azure AI in Governance: Singapore Police Force Implementation 15 (Microsoft Corporation, Redmond, 2021).

[22] United Nations Office on Drugs and Crime, Responsible AI Innovation in Law Enforcement (2024), available at https://www.unodc.org/unodc/en/human-trafficking/glo-act6/Countries/responsible-ai-innovation-in-law-enforcement_-understanding-risks-and-opportunities.html/, (last visited on November 17, 2025).

available at https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained (last visited on November 17, 2025).

Bureau of Police Research and Development, *Project Report on Predictive Policing for Women Safety* (Ministry of Home Affairs, New Delhi, 2020), available at https://bprd.nic.in/uploads/pdf/Predictive%20Policing%20for%20Women.pdf (last visited on November 17, 2025).

Capita, *AI in Public Sector: Case Studies from UK Policing* (Capita PLC, London, 2022).

Council on Criminal Justice, *The Implications of AI for Criminal Justice* (2023), available at https://councilоncj.org/the-implications-of-ai-for-criminal-justice/ (last visited on November 17, 2025).

Federal Trade Commission, *FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance* (2024), available at https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance (last visited on November 17, 2025).

Krishna Iyer VR, *Justice at Crossroads: A View from the Bench* (Excel Books, New Delhi, 2003).

Microsoft, *Azure AI in Governance: Singapore Police Force Implementation* (Microsoft Corporation, Redmond, 2021).

PredPol Inc, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (PredPol Inc, Santa Cruz, 2018).

ProPublica, "Machine Bias", available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (last visited on November 17, 2025).

The Guardian, *LAPD ended predictive policing programs amid public outcry. A new study shows how they validated existing patterns of policing* (2021), available at https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform (last visited on November 17, 2025).

United Nations Office of the High Commissioner for Human Rights, *Input Office of the High Commissioner for Human Rights* (2024), available at https://www.unodc.org/res/justice-and-prison-reform/access-to-justice-for-

all_html/U_Office_of_the_High_Commissioner_for_Human_Rights.pdf (last visited on November 17, 2025).

United Nations Office on Drugs and Crime, *Responsible AI Innovation in Law Enforcement* (2024), available at https://www.unodc.org/unodc/en/human-trafficking/glo-act6/Countries/responsible-ai-innovation-in-law-enforcement_-understanding-risks-and-opportunities.html (last visited on November 17, 2025).

Universal Declaration of Human Rights, adopted 10 December 1948