WHEN JUSTICE MEETS THE MACHINE: LEGAL AND ETHICAL IMPLICATIONS OF AI IN CRIMINAL JUSTICE

Saptarshi Saharay[1]

VOLUME 1, ISSUE 2 (JULY- DECEMBER 2025)

ABSTRACT

In an age of data and technology, artificial intelligence (AI) and its influence cannot be disputed—it is revolutionizing sectors, reengineering government, and even seeping into the corridors of justice. In the criminal justice system, AI is becoming increasingly utilized in predictive policing, risk assessment, facial recognition, and even sentencing. Though this digitization holds the promise of efficiency and objectivity, it also poses quite serious legal and ethical issues. Can a machine ever really comprehend justice? Is AI fair, or merely quick?

This article examines the legal structures, ethical challenges, and practical implications of applying AI in criminal justice systems worldwide, with a particular focus on India and the United States. It also examines how the courts, legislatures, and civil society are responding to this AI driven upheaval.

[1] Saptarshi Saharay, *Sister Nivedita University*

AI IN CRIMINAL JUSTICE: WHAT'S AT STAKE?

Key Applications of AI in the System

- AI is applied at nearly all levels of the criminal justice pipeline:
- Predictive policing: Software such as PredPol and India's CMAPS digests crime data to predict criminal hotspots.
- Risk assessment tools: COMPAS in the United States makes estimates about recidivism likelihood to inform parole and bail determinations.
- Facial recognition software: Law enforcement uses it to identify suspects from CCTV or social media photos.
- Digital forensics: AI-enabled software can sift through vast amounts of data from phones, hard drives, or the dark web.
- Lie detection and emotional assessment: Experiential equipment such as EyeDetect purports to read "truth" from eye behaviour.

These applications, although effective, are not controversy-free.

THE LEGAL CHALLENGES OF AI IN CRIMINAL JUSTICE

Violation of Due Process and Fair Trial

The "black box" nature of AI—its inability to make transparent decisions—undermines the constitutional provision for a fair trial. In State v. Loomis, 881 N.W.2d 749 (Wis. 2016), the defendant objected to the use of the COMPAS algorithm for sentencing, claiming it was against due process because the methodology was proprietary and transparent. The Wisconsin Supreme Court affirmed the sentence but warned against "determinative" application of AI tools. Denial of access to the logic of the algorithm is contrary to Brady v. Maryland, 373 U.S. 83 (1963), which mandates disclosure of exculpatory evidence. In India, the use of such impenetrable tools will conflict with Article 21 of the Constitution of India ensuring life and liberty with "procedure established by law."

Data Privacy and Surveillance

Facial recognition and predictive policing tools raise concerns under:

- Right to Privacy: Established as a fundamental right in Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- The Personal Data Protection Bill, 2019 (India), although pending, seeks to oversee AI-based processing of data.

- Case Example: The Delhi Police allegedly used facial recognition technology during protests without adequate protections, a practice criticized by civil rights organizations.

Ethical Implications: The Morality of Machine Justice

Bias in, Bias Out

- AI learns from data—but if the data is biased, so will the AI.
- Example: COMPAS was found in studies to over flag Black defendants as high-risk when compared to white defendants.
- Academic Criticism: "Machine Bias," by Julia Angwin and colleagues, ProPublica (May 23, 2016).

This creates ethical concerns of:

- Equal treatment before law (Article 14, Indian Constitution)
- Non-discrimination under international human rights instruments

Dehumanization of Justice

- AI decisions are binary, whereas human existence is complex. Ethical jurisprudence requires empathy, discretion, and context—characteristics lacking in machines.
- Can an AI take into account remorse or social circumstances?
- Does entrusting decision-making to machines take away from the human dignity that justice is required to uphold?

PREDICTIVE POLICING: INNOVATION OR INJUSTICE

Predictive Policing Tools in India

India has been testing AI technologies such as:

- To predict crime hotspots, Uttar Pradesh and Delhi implemented the Crime Mapping Analytics and Predictive System (CMAPS).
- Trinetra: Employed by the Rajasthan Police to track the online activities of criminals.
- Though well-intentioned, such systems raise several serious concerns:
- Transparency: Are these systems audited?
- Consent: Do citizens know they are under surveillance?
- Oversight: Is there any legislative oversight?

International Example: PredPol in the U.S.

- PredPol was withdrawn from some U.S. cities following reports of:
- Excessive policing in minority communities

- Enforcement of racial stereotyping in past data
- Legal Issues:
- Equal Protection Clause of the 14th Amendment (U.S. Constitution)
- Abuse of police authority under Article 246 of the Indian Constitution in conjunction with Entry 2 of List II (State List)

The Constitutional and Statutory Vacuum in India

India does not have laws that deal specifically with the use of AI in criminal justice. This regulatory gap beckons:

- Misuse of power
- Lack of accountability
- No right to appeal AI driven decisions.
- Need for Legislative Action
- Incorporate algorithmic transparency in law enforcement.
- Establish a Regulatory Authority on AI.
- Mandate impact assessments before deploying AI tools.
- Global Models to Consider

EU AI Act (2021): Classifies AI tools by risk, bans unacceptable use cases.

Algorithmic Accountability Act (USA, 2022): Requires entities to assess the impacts of automated decision systems.

India could model its AI laws around these standards while preserving constitutional rights.

ROLE OF JUDICIARY IN REGULATING AI

Indian Judicial Approach

- While courts have not directly adjudicated the use of AI in criminal justice, they have acknowledged it.
- Right to privacy as an essential part of dignity (Puttaswamy case)
- Algorithmic accountability as a future legal issue (implied indirectly in Aadhaar-related judgments)
- Judicial Proposals:
- Courts must require disclosure of source codes when AI technologies are presented as evidence.

- Appoint technical amici curiae to examine algorithmic systems.

U.S. Judicial Reactions

- People v. Wakefield, No. B293953 (Cal. Ct. App. 2020): Expressed concerns regarding facial recognition mistakes.
- Demands the Daubert standard for AI instruments to be allowed as evidence.

STRIKING A BALANCE: IS THERE A THIRD WAY?

AI in criminal justice must be addressed from a rights-based perspective.:

- Be transparent: Open-source code and plain language.
- Be accountable: Offer mechanisms of appeal for AI decisions.
- Be fair: Eliminate biased data sets and track outcomes.
- Be proportional: Utilize AI where human examination is feasible.
- Role of Legal Professionals
- Judges and lawyers should be trained in:
- AI ethics
- Algorithmic thinking
- Cyber forensics and data protection

THE ROAD AHEAD

- AI offers great potential in criminal justice—from speeding up investigations to improving public safety.
- But unchecked AI can compromise due process, equality, and individual liberty.
- India urgently needs a robust legal framework and judiciary-led oversight to align AI with constitutional values.

CASE STUDIES AND REAL-WORLD OUTCOMES: LESSONS FROM THE FIELD

India: Delhi's Use of Facial Recognition

The Delhi Police began using face recognition software (FRS) in 2019 in an effort to find missing people and suspects. Crowds were monitored using the same technology in 2020 during the anti-CAA demonstrations in Delhi. However, civil liberties activists criticized this as a form of unapproved mass surveillance.

Legal Concerns Raised:

- Under the Information Technology Act of 2000, there is no enabling act.

- Potential contravention of the Supreme Court's decision in Puttaswamy, which requires tests of necessity, legality, and proportionality for surveillance.

Expert Opinion:

As per the Internet Freedom Foundation, the system was only 2% accurate when utilized for the detection of missing children, questioning reliability and wrongful profiling.

- In 2020, a Black man named Robert Williams in Detroit was unjustly arrested based on a mistaken match by facial recognition software. His case has become the hallmark of algorithmic bias
- Violation of Constitutional Rights:
- Fourth Amendment: Unreasonable search and seizure.
- Fourteenth Amendment: Equal protection clause, as facial recognition technology exhibits increased error rates with Black faces.

Policy Impact:

- San Francisco, Boston, and a number of other cities prohibited police from using facial recognition.
- Prompted the U.S. Congress to approve the 2020 Facial Recognition and Biometric Technology Moratorium Act.

COMPARATIVE LEGAL ANALYSIS: GLOBAL RESPONSES TO AI REGULATION IN CRIMINAL JUSTICE

European Union: Risk-Based Framework

- The EU Artificial Intelligence Act (currently still in legislative process as of 2025) categorizes AI applications into:
- Unacceptable Risk: Social scoring, mass surveillance—categorically prohibited.
- High Risk: Covers AI in policing, border control, and judiciary—requires transparency, human oversight, and impact assessment.
- Limited/Minimal Risk: Automated responses and chatbots—disclosure only.
- This risk-based framework may be a universal standard.

China: Leading but Controversial

China has implemented AI heavily in the judiciary and policing (e.g., "One Person, One File" mechanism and "Smart Courts"). Although it has enhanced disposal rates in cases, it has faced criticism over:

- Lack of transparency.
- Facilitating state surveillance.
- Lack of legal recourse against AI mistakes.
- While being technologically sophisticated, it highlights the ethical peril of AI in the hands of authoritarian governments.

India: A Reactive as Opposed to a Proactive Approach

- India does not have today:
- A robust AI policy of regulation.
- The 2019 Data Protection Act is still pending as of 2025.
- An autonomous AI Ethics Review Board.
- This fragmented, sectoral regulation is insufficient for handling AI in sensitive spheres such as criminal justice.

THEORETICAL FOUNDATIONS: ALGORITHMIC JUSTICE VS HUMAN JUSTICE

Retributive vs Predictive Justice

- Traditional criminal justice models are founded on concepts of culpability, deterrence, and rehabilitation. AI is predictive and statistical, though. That creates philosophical implications:
- AI punishes for what a person may do rather than for what they did.
- That puts mens rea (guilty mind) as a central tenet of criminal law under threat.

Procedural Justice

- Tom Tyler's theory emphasizes that people comply with the law when the process is fair, transparent, and respectful. AI's opacity disrupts this:
- Citizens can't contest or understand algorithmic decisions.
- Loss of trust in judicial systems

PROBLEMS IN DATA QUALITY AND ACCOUNTABILITY

Garbage In, Garbage Out

- AI is only as good as the training data. If datasets contain:
- Historical bias (e.g., over policing in minority areas),
- Incomplete records (e.g., underreported crimes against women),
- or doctored entries (e.g., planted evidence),
- Then the AI replicates and amplifies injustice.

Lack of Clear Liability Frameworks

- When AI tools fail, who is responsible?
- The developer?
- The police department?
- The government?
- This "accountability gap" is perilous in criminal law, where lives and liberties are at risk.

Suggested Reforms:

- Introduce Algorithmic Impact Assessments (AIAs).
- Require human-in-the-loop review.
- Establish civil liability regimes for AI mistakes.

AI IN COURTS: AUTOMATION OF JUDICIAL DECISIONS

Smart Courts in China and UA

- China's AI judges have disposed of over 3 million cases using robotic assistance, including:
- Traffic ticketing.
- E-filing and remote hearings.
- UAE launched an AI judge to handle small claims under AED 20,000.

Should India Follow Suit?

Pros:

- Accelerate outstanding cases (There are more than 4 crore cases outstanding in India.).
- Assist the overburdened lower judiciary.

Cons:

- Risk of undermining judicial discretion.
- Low digital literacy among litigants.
- Rural-urban tech divide.
- Conclusion: AI should be used as a supplement, not as a substitute.

AI ETHICS IN LAW ENFORCEMENT: A NEW CODE OF CONDUCT

Main Principles for Ethical Use

- Take up the OECD AI Principles, which are:
- Transparency: Clear explanation of AI decisions.
- Accountability: Impose legal responsibility

- Fairness: Avoid bias and provide fair outcomes.
- Robustness: Maintain accuracy, security, and resilience.

Training for Stakeholders

- Judges: Have to be trained in algorithmic reasoning and AI forensics.
- Lawyers: Need to learn how to cross-examine AI-generated evidence.
- Police: Need ethical training and AI literacy to prevent misuse.

RECOMMENDATIONS FOR THE INDIAN LEGAL FRAMEWORK

Pass a Comprehensive AI and Data Protection Law

- Include transparency, consent, storage, and grievance redress.
- Make criminal justice a "sensitive sector."

Set up an AI Ethics Committee under NHRC

- Examine tools such as CMAPS and Trinetra.
- Listen to citizen grievances.

Make Algorithmic Disclosure in Court Mandatory - Take a cue from the Daubert Standard (USA) for admissibility.

Public Awareness and Debate

- Promote digital literacy about AI's role in justice.
- Enable civil society to track the abuse of AI.

Pilot Projects and Independent Audits

- Audit AI systems before national release.
- Test in lower courts, not capital punishment.

WHAT LEGAL SCHOLARS ARE SAYING

- Shoshana Zuboff (Surveillance Capitalism) warns against private corporations using AI for policing abuse.
- Cathy O'Neil (Weapons of Math Destruction): Suggests that algorithms tend to generate new discrimination.
- Usha Ramanathan (Indian expert on privacy): AI applications without legal support facilitate "technological tyranny."

These views underscore the fact that AI, if left unregulated, poses a legal and ethical risk.

COUNTERARGUMENTS AND RESPONSES

"AI is more objective than humans."

Response: AI mirrors human prejudice in data. Unlike humans, it can't adjust contextually.

B. "AI can decrease case backlogs."

Response: True, but haste without justice equals injustice. Efficient and equitable practices must be balanced.

C. "We can't stop technological progress."

The law should guide, not pursue, technology. Regulation allows for safe progress.

The justice system is not only about convictions or clearances—it is about fairness, human dignity, and trust in society. While AI has great power to help solve crime and provide rapid justice, it can never be a substitute for the fundamental human values that underpin law.

If criminal justice becomes too dependent on secret, biased, and unaccountable algorithms, it will become less just and more mechanical.

CONCLUSION

AI is already being applied in predictive policing, facial recognition, and judicial decision-making. It has serious implications for due process, privacy, bias, and accountability. India and most countries do not have adequate legal protections. World best practices highlight transparency, ethics, and regulatory oversight. India has to move with caution and foresight, learning from global successes and failures. At the end of it all, we have to ensure that in pursuit of efficiency, we do not lose the heart of justice: humanity.