LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:441-449, July 2025

ARTIFICIAL INTELLIGENCE AND CRIME PREDICTION: ETHICAL AND LEGAL CONCERNS

By- Sushmitha. S[1]

ABSTRACT

Artificial Intelligence (AI) is transforming modern law enforcement by enabling crime prediction, risk assessment, and targeted policing. AI-driven tools, such as facial recognition, predictive algorithms, and recidivism scoring systems, offer data-driven efficiencies that promise safer communities. However, their growing adoption raises serious ethical and legal concerns. This paper critically examines issues including algorithmic bias, opaque decision-making, mass surveillance, and violations of due process. Such tools as COMPAS in the U.S. have uncovered racially biased outputs, and predictive policing tends to disproportionately target marginalized groups. The article discusses salient constitutional safeguards under Indian and global law, surveys pertinent judicial precedents, and evaluates regulatory proposals such as the EU Artificial Intelligence Act and ethics frameworks such as the Menlo Report. It advocates enhanced oversight, fairness audits, and human-in-the-loop checks to guard against abuse. Finally, AI in criminal justice needs to be balanced with civil liberties, so that it promotes democratic principles and does not erode them.

KEYWORDS: Predictive Policing, Algorithmic Bias, Civil Liberties, Artificial Intelligence in Law Enforcement, Regulatory Frameworks

[1]**Intern, Lex Lumen Research Journal.**

1. INTRODUCTION

Artificial Intelligence (AI) is transforming the criminal justice system at a speed that is unprecedented. From anticipating crime and flagging potential offenders to more efficient deployment of police resources, AI technologies are being employed for proactive crime prevention. Facial recognition, predictive policing software, and risk assessment algorithms such as COMPAS hold out the promise of greater accuracy, cost savings, and quicker decision-making. But all this transformation has a cost. The application of AI for law enforcement is fraught with grave legal, ethical, and constitutional issues. They include algorithmic bias, un transparency, infringement of due process rights, mass surveillance, and profound privacy invasions. In India, the implications cut across basic rights ensured under Part III of the Constitution, notably Articles 14, 19, and 21. This essay examines how AI, with its lofty potential, can perpetuate discrimination and undermine civil rights. It presents international case studies and presents legal and policy changes to make crime prediction technologies used in a fair and responsible fashion.

2. DISCRIMINATION AND BIAS

2.1 Algorithmic Bias

Many AI applications in criminal justice are modelled on past experiences. These data commonly exhibit the effects of decades of discriminatory policing, underreporting, and racial profiling. Predictive policing models, for example, disproportionately single out minority communities because of the pattern of past arrests. One famous example is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), a tool employed in US courts to assess recidivism risk. In 2016, an investigation by ProPublica found that COMPAS over-predicted recidivism risk among Black defendants but under-predicted it among white defendants, even when their criminal histories were the same [Angwin et al., 2016].

2.2 Dirty Data and Feedback Loops

The "dirty data" idea data collected through practices that violate civil rights poses significant ethical issues. Data collected from biased practices contributes to biased predictions, creating

feedback cycles of injustice. Academics contend that such loops complicate efforts to uproot structural inequality (Richardson et al., 2019).

3. CONSTITUTIONAL AND LEGAL CONCERNS

3.1 Due Process and Equal Protection

In the U.S., the Fifth and Fourteenth Amendments guarantee due process and equal protection. In India, similar protections are enshrined in Article 14 (equality before the law) and Article 21 (right to life and personal liberty). Using opaque AI models to determine bail, sentencing, or surveillance decisions risks breaching these constitutional protections. In Maneka Gandhi v. Union of India [(1978) 1 SCC 248], it was held by the Supreme Court that any "procedure" denying personal liberty has to be just, fair, and reasonable. Automated black-box decisions by AI systems do not pass this test, particularly when defendants are not able to challenge or understand the rationale of the decisions.

3.2 Opacity and Accountability

Most AI algorithms employed in policing are trade-secreted and proprietary. Courts and defendants therefore cannot assess how a risk score or prediction is produced. Such unexplained computation contravenes natural justice principles, especially the audi alteram partem rule. Legal scholar Aziz Z. Huq contends that machine-learning systems render accountability and judicial review all but impossible, threatening democratic governance (Huq, 2020).

3.3 Judicial Scrutiny and Case Law

In LAPD v. Community Coalition, community Organisations challenged Los Angeles Police Department's use of predictive policing, alleging racial targeting and lack of oversight. Although courts have not uniformly ruled against such programs, these cases signal rising concern about AI's incompatibility with constitutional rights.

3.4 Procedural Fairness and the Audi Alteram Partem Principle

Procedural fairness requires that no one should be condemned unheard. Predictive algorithms, when used to make decisions without leaving understandable reasoning behind them, offend this requirement. In Swadeshi Cotton Mills Co. Ltd. v. Union of India [(1981) 1 SCC 664], the Supreme Court highlighted the necessity of hearing the party concerned before administrative action. Black-box AI systems, with their largely proprietary algorithms, essentially do away with this protection, cutting off the right of impacted individuals to respond or even know how they were categorized or scored.

4. PRIVACY AND SURVEILLANCE THREATS

4.1 Data Harvesting

AI systems are dependent on huge inputs of data from CCTV, GPS, social media, and public records. In most cases, this information is gathered without permission, violating the privacy right. The Right to Privacy was enshrined as a constitutional right in Justice K.S. Puttaswamy v. Union of India [(2017) 10 SCC 1], which read much into informational self-determination and safeguard against arbitrary state surveillance. Most AI applications, such as facial recognition and predictive algorithms, function with insufficient data protection legislation. India's Digital Personal Data Protection Act, 2023 still does not have strong provisions governing the use of the law enforcement.

4.2 Chilling Effects on Democratic Freedoms

AI. -driven mass surveillance can creep in to stifle dissent and discourage political engagement. When the people believe that they are constantly under surveillance, they may censor themselves. This is indicated in literature (Selinger & Hartzog, 2009) and contravenes Article 19(1)(a) (freedom of speech) and 19(1)(b) (freedom of peaceful assembly).

4.3 Surveillance Creep and Function Creep

In addition to its original intent of crime avoidance, AI technologies can apply to increasingly wider targets, often called surveillance creep. Function creep is when technology is designed to fulfil one purpose (e.g. counter-terrorism) and subsequently used for another unanticipated purpose

(e.g. student activity in schools), making extreme surveillance a normalized part of daily life. These cases of blind escalation move the uses of technology beyond the proportionality principle that was established in the Puttaswamy case.

5. PUBLIC TRUST AND HUMAN RIGHTS

If we rely too much on these new AI systems in criminal justice, it makes the law less trustworthy for the public. When a dangerous markup is placed on minorities who experience fewer cooperative interactions with the police, placing trust in corporations like Pinkerton is socially irresponsible and detrimental; Net benefit places less value on community policing. The issues with low error rates regarding facial recognition technology create a deeper concern for dark skin/female identifiers. These errors place people in jail for false arrests, misplaced/employed identifiers related to people walking, labelled as guilty, and resulted in tremendous psychological harm. Social advances can undertone and trivialize human dignity, this goes to the heart of Article 21 in the Indian Constitution.

5.1 The Psychological and Social Effects on Targeted Communities

Declaring entire neighborhoods as "high-crime" areas stigmatizes, alienates, and creates a felt sense of structural injustice. It has a similar impact on career advancement, inability to advance on education, and housing sameness, thus compounding disadvantage for already marginalised communities. Ruha Benjamin (2019), in Race After Technology, challenges such as "automated inequities" and calls for dismantling technology systems that retrench racial and social inequalities. Moreover, globally, non-protected AI uses also violate human rights conventions like the International Covenant on Civil and Political Rights (ICCPR), particularly Article 17 (privacy) and Article 14 (fair trial).

6. ETHICAL PRINCIPLES AND REGULATORY FRAMEWORK

6.1 European Union AI Act.

The proposed EU Artificial Intelligence Act of 2021 and now adopted in 2024, identifies predictive policing technologies as "high-risk," which conditions formal use on transparency, risk assessments, and human control; The consequence for failing to comply is a considerable fine, thereby ensuring accountability.

6.2 U.S. Municipal Regulations.

San Francisco and Boston governments have banned facial recognition technology because of claims of racial bias and violations of civil liberties, as local municipalities are showing opposition to unregulated surveillance regardless of the absence of federal law.

6.3 The Menlo Report

The Menlo Report (2012) of the U.S. Department of Homeland Security has defined four ethical principles - Respect for Persons, Beneficence, Justice, and Respect for Law and Public Interest. The report facilitates transparency and accountability in public-sector research on emerging technologies, like AI.

6.4 The Indian Legal Vacuum and Regulatory Delay.

While India currently lacks comprehensive legislation analogous to the EU AI Act, the Digital Personal Data Protection Act, 2023 provides some improvements in the area of private data use, however it does not mention initiatives such as predictive policing, algorithm auditing, or discuss the liability of the state. On top of this, Indians have no formal classification of high-risk AI, accountability for explainability and impact assessments, and ultimately remains open for abuse.

7. POLICY RECOMMENDATIONS

To safeguard constitutional rights and establish some parameters for the ethical implementation of Internet and AI-based technologies in policing, the following policies are urged:

1. Legislation on Algorithmic Transparency: Courts should have the authority to scrutinise AI systems consistent with Article 21 and the principles of natural justice.

2. Fairness audits: Legislative enforcement of independent audits on predictive models, on a regular schedule, to determine conformance with Article 14.

3. Human-in-the-loop design: If a decision affects liberty, a human must always be involved in the review of the decision to preserve elements of judicial discretion and procedural fairness.

4. Right to redress: Individuals who suffer harm from AI-driven decisions that adversely impact them without justification require declared legal routes to redress, to include compensation and review processes, consistent with Article 32 of the Constitution, and Article 2(3) of the ICCPR.

5. Community Oversight Boards: Citizen oversight boards should evaluate AI applications in policing to ensure accountability and transparency.

6. Public Awareness and Digital Literacy: Communities must be able to fight back against the excesses of technology through awareness campaigns that create communities that are aware of their rights and are able to understand AI systems in order to promote democratic engagement.

8. CONCLUSION

AI has enormous potential to enhance policing and public safety. However, in the absence of rigorous legal and ethical safeguards, these technologies can also increase discrimination, violate civil liberties, and decrease public trust. Courts, legislatures, and communities must work to develop crime forecasting tools that promote justice rather than jeopardise it. We will need legal reforms, public oversight, and ethical frameworks to help ensure that AI allows us to promote democratic values and the rule of law

REFERENCES

1. Richardson, R., Schultz, J., & Crawford, K. (2019). An exploration of how civil rights breaches can distort police databases, influence predictive policing tools, and hinder justice. NYU Law Review Online, 94, p.15.

2. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). A critical investigation into bias in criminal risk assessment software, revealing racial disparities in its outcomes. ProPublica. Retrieved from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
3. Ferguson, A. G. (2017). A comprehensive account of how data-driven surveillance technologies reshape policing and disproportionately affect communities of color. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York University Press.
4. Huq, A. Z. (2020). Examines the compatibility of machine learning technologies with constitutional safeguards in a modern governance framework. Cornell Law Review, 105, 579.
5. Selinger, E., & Hartzog, W. (2009). Discusses the tensions between widespread surveillance mechanisms and the core principles of democratic governance. Washington & Lee Law Review, 66, 1507.
6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 – A seminal Indian Supreme Court verdict recognizing privacy as an essential constitutional right under Article 21.
7. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 – A pivotal case that broadened the scope of the right to life and liberty in Indian constitutional law.
8. The Digital Personal Data Protection Act, 2023 – Indian legislation focusing on the protection and lawful processing of personal data in the digital era.
9. European Union Artificial Intelligence Act, 2024 – A landmark EU statute setting out ethical and regulatory standards for the deployment of artificial intelligence systems.
10. U.S. Department of Homeland Security. (2012). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research – Establishes ethical norms for ICT research, emphasizing transparency, fairness, and harm reduction.
11. International Covenant on Civil and Political Rights (ICCPR), 1966 – A global treaty guaranteeing key civil and political rights to individuals across ratifying nations.

12. Benjamin, R. (2019). Provides a critical race analysis of emerging technologies and calls for structural reforms in tech development. Race After Technology: Abolitionist Tools for the New Jim Code. Polity Press.
13. Swadeshi Cotton Mills Co. Ltd. v. Union of India, (1981) 1 SCC 664 – An important Indian case addressing state intervention in private enterprises and due process concerns.
14. Chander, A. (2017). A scholarly critique of how automated decision-making systems can reinforce racial inequalities. Michigan Law Review, 115(6).
15. Nayak, S. C. (2022). Analyzes constitutional challenges posed by artificial intelligence and recommends a human-rights-driven approach. Indian Journal of Law and Technology, 18.
16. Privacy International. Function Creep: The Expansion of Surveillance Capabilities. Retrieved from: https://privacyinternational.org