INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"FROM PREDICTION TO PREJUDICE: REGULATING ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE" (ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE)

AUTHORED BY - ANANYA PAL
B.B.A.LL.B
Amity University Lucknow

CO-AUTHOR - DR. ARVIND KUMAR SINGH
Associate Professor
Amity University Uttar Pradesh Campus, Lucknow

Abstract

The inclusion of AI in a criminal justice system has generated both hopes and fears. Predictive policing tools and algorithmic decision-making guarantee an efficient public service system where crimes can be prevented, and governance is data-driven. However, they threaten the very notion of due process, equality, and human dignity. This paper undertakes a critical assessment of AI in criminal justice, particularly concerning predictive policing and algorithmic bias.

Drawing on comparative experience, it analyses the U.S.'s reliance on what are called risk assessment instruments such as COMPAS, a system that has been severely criticised for perpetuating racial and socio-economic disparities. It further analyses the 2024 Artificial Intelligence Act of the European Union, which, applying a more precautionary principle, categorises predictive policing as a "high-risk" application, subjecting it to fairly strict transparency requirements. Conversely, India's experiments with AI- for instance, under the judiciary via the Supreme Court SUPACE system-are still in their embryonic stages but raise pressing questions on constitutional rights, especially after the Puttswamy verdict's recognition of the right to privacy.

The basic contention is that AI, while certainly a supplementary tool, does not afford the fairness, accountability, or human judgment inherent in the classical notions of rule of law. Predictive justice stands to turn into prejudiced policing due to algorithmic opacity, biases in

ISSN: 2582-6433

the data, and lack of the statutory protection. Through doctrinal analyses, comparative jurisprudence, and policy evaluations, the paper states the dire need for a regulatory framework dealing with the issue of algorithmic transparency, independent audits, and strong human oversight.

In summation, the paper makes a case that the promise AI holds for criminal justice shall only be realised when protected under constitutional guarantees and ethical regulation. In the absence of such, this quest for efficiency through technology will, into fact, undo the very notions of fairness and justice it aims to uphold.

Introduction

The inclusion of Artificial Intelligence (AI) in criminal justice has generated both optimism and apprehension. On the one hand, predictive policing tools and algorithmic decision-making promise efficiency, resource optimization, and the possibility of crime prevention.[1] By analysing large datasets, AI systems can identify "crime hotspots," assess the risk of recidivism, and even support judicial decision-making on bail and sentencing.[2] Governments and law enforcement agencies around the world—particularly in the United States, the European Union, and increasingly India—are exploring the use of such technologies as part of their broader vision of a "data-driven governance" model.

But with the promise of predicting behaviour comes the insidious possibility of bias. Algorithms are not unbiased. Algorithms are biased; they propagate the bias of the data on which they are trained[3]. The U.S. experience with the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) software as an example. The COMPAS software labelled black defendants as "high risk" more than white defendants who committed the same or similar offences.[4] The same pattern has arisen with predictive policing software like PredPol – an algorithm that generates data driven "predictions" based on crime "hot spots" – which has been accused of over-policing in minority neighbourhoods leading to distrust and

[1] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 3–7 (2017).
[2] Id. at 12–15.
[3] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 45–47 (2018).
[4] ProPublica, Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

ISSN: 2582-6433

over-policing of people of colour.[5] The algorithm doesn't produce fair or equitable understanding, but simply reproduces the effects of the already unjust system, presented as scientific objectivity.

The primary tension lies between efficiency and equity—predictive policing may offer administrative ease, but raises fundamental questions around due process, fairness, accountability, and human dignity[6]. If we cede judicial or policing decisions to opaque algorithms, who is held responsible when a wrong arrest is made, when excessive bail is imposed, or for knowing someone is being surveilled because of their race? More importantly, how might the individual challenge the decisions of algorithms if the algorithms' operation is concealed as "trade secrets"? The opacity of AI diminishes the procedural safeguards that are central to the criminal justice system.

Globally, new jurisdictions reacted in different ways. In the U.S., the case of State v. Loomis[7] represents a constitutional challenge to the use of algorithmic risk assessments, with the Wisconsin Supreme Court finding bias was acknowledged in developments around the use of COMPAS, while issuing cautionary warnings. The U.S. approach is unexpected in light of the European Union, whose Artificial Intelligence Act, 2024 regards predictive policing as a "high-risk" AI, with obligations to meet transparency, explainability, and oversight requirements.[8]India is experimenting with AI in the judiciary—with initiatives such as the Supreme Court's SUPACE (Supreme Court Portal for Assistance in Courts' Efficiency)[9],but there is not yet a clear regulatory framework for constitutional implications.

The Indian legal context is especially important. With the Supreme Court's ruling in Justice K.S. Puttaswamy v. Union of India[10], recognising the right to privacy as a fundamental right, it is now possible to scrutinise surveillance, and algorithmic tools (like AI) under constitutional guarantees. However, with no AI-specific legal regime for criminal justice currently, India is vulnerable to adopting AI tools without legal safeguards. The challenge is balancing the ambition of digitalising governance with constitutional duties (of fairness, equality and

[5] Rashida Richardson, Jason Schultz & Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice 94 N.Y.U. L. Rev. 192, 199–201 (2019).
[6] Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* 121–23 (2020).
[7] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[8] Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 231) 1.
[9] Supreme Court of India, Press Release: Launch of SUPACE (Apr. 6, 2021).
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

ISSN: 2582-6433

justice). This paper proposes a critical review of AI in criminal justice, with specific emphasis on predictive policing and algorithmic bias. It argues that AI has the potential for efficiency, but cannot replace human judgement under the classical rule of law. The danger with predictive justice is that, without the implementation of regulation requiring algorithmic transparency, independent audits and human oversight, it will quickly deteriorate into biased policing.

The research continues with the following questions:

1. Does predictive policing improve justice or reinforce systemic bias?
2. How have different jurisdictions (in particular, the U.S., EU, and India) engaged the regulation of AI in criminal justice?"
3. What can India learn from comparisons of experience to design a constitutional and ethical framework with respect to AI in policing?

By answering these questions, the paper is situated at the intersection of technology, constitutional rights, and criminal justice. Ultimately, it argues that the potential of AI in criminal justice can be achieved only if it is placed within strong regulatory structures that ensure that technology serves justice and does not become master of the justice process.

Conceptual Framework

A. Meaning of Predictive Policing

Predictive policing is the application of artificial intelligence and statistical models to predict future criminal behaviour in two ways, either through predicting locations that will likely be subject to a crime ("place-based prediction") or predicting the likelihood of an individual engaging in criminal behaviour ("person-based prediction")[11]. Predictive policing typically uses historical crime data, arrest data, socio-demographic data, and behavioural data to infer "risk factors" of individuals and communities. Predictive policing's appeal is its promise of efficiency – allocating police resources to high-risk areas, ceasing crime before it takes place, and alleviating some court burden.

Critics of predictive policing cite the "garbage in, garbage out" issue of machine learning.[12] If historical data is biased due to oppressive policing practices (e.g., if police over-patrol minority community neighbourhoods), that algorithm will learn and

[11] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 24–25 (2017).
[12] Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy 3–6 (2016).

ISSN: 2582-6433

continue that historical discrimination.[13]

B. COMPAS Algorithm (U.S.)

The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool represents a major algorithmic decision-making system that criminal justice agencies employ. The United States relies extensively on this system to determine the likelihood of defendant recidivism.

The ProPublica investigation of COMPAS risk assessments demonstrated that Black defendants received nearly double the number of high-risk misclassifications compared to white defendants when evaluated in Florida during 2016.[14]

The risk assessment tool frequently made errors by assigning white defendants lower risk scores than they should have received.[15]

The Wisconsin Supreme Court reviewed the use of COMPAS in sentencing through State v. Loomis[16] after the defendant questioned its due process treatment because the secret methodology of the algorithm remained inaccessible.

The court permitted COMPAS usage but required judges to combine algorithmic results with other factors and warned against using risk scores to establish sentencing duration.[17] Courts demonstrate hesitation towards algorithms through this case since they acknowledge bias exists but do not eliminate AI because of its administrative value.

C. PredPol (Predictive Policing Software)

The predictive policing software PredPol operates as a prominent tool which was initially developed through federal funding from the United States. Through machine learning algorithms PredPol analyses time and location data and crime types to identify predicted crime hotspots. Police departments from different American cities including Los Angeles and Santa Cruz tested his system.

Research findings showed that PredPol led police patrols to concentrate mainly in Black and Latino neighbourhoods without considering the actual crime statistics.[18] The system

[13] Rashida Richardson, Jason Schultz & Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice 94 N.Y.U. L. Rev. 192, 200–03 (2019).
[14] ProPublica, Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[15] Id
[16] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[17] Id. at 761–64.
[18] Kristian Lum & William Isaac, To Predict and Serve?, *Significance* (Oct. 2016).

ISSN: 2582-6433

operated through a feedback loop which caused increased police presence to generate more arrests in those areas thus producing biased data that re-entered the system. Santa Cruz became the first U.S. city to ban predictive policing in 2020 following public opposition.[19]

The main problem with PredPol shows that social inequality within data causes algorithms to enhance existing biases instead of fixing them.

D. Indian Context: AI in Judiciary (SUPACE)

The Indian judiciary has started testing artificial intelligence applications however these implementations do not match the predictive policing systems operating in the United States. The Supreme Court developed SUPACE (Supreme Court Portal for Assistance in Courts' Efficiency) in 2021 as an AI-powered research platform that helps judges through file summarization and brief generation alongside finding applicable precedents.[20]

The current functions of SUPACE do not determine judicial decisions but its implementation creates doubts regarding the potential dependency of judges on computerized algorithms. The former Chief Justice S.A. Bobde explained that SUPACE operates as a tool which provides assistance to judges rather than functioning as a replacement for judicial decision-making.[21] Scholars maintain that research assistance tools can affect judicial reasoning patterns when they lack transparency and explainability features.[22]

Indian policy makers currently debate about using AI technology in crime analytics and policing systems which belongs to the government's "Digital India" program. The absence of a clear AI accountability framework creates significant risks of hidden algorithms and biased outcomes as well as violations of human rights.

E. Conceptual Dilemma: Tool vs. Decision-Maker

The main conceptual discussion revolves around whether artificial intelligence functions as an assisting tool for judges and police or as an independent decision-maker. AI outputs function as advisory tools that safeguard human accountability but giving

[19] Santa Cruz City Council, Ordinance Banning Predictive Policing Technology (June 2020).
[20] Supreme Court of India, Press Release: Launch of SUPACE (Apr. 6, 2021).
[21] Id.
[22] Vidushi Marda & Shivangi Narayan, *Artificial Intelligence in the Indian Justice System: Prospects and Perils* 11 Indian J.L. & Tech. 45, 60–62 (2021).

ISSN: 2582-6433

algorithms decision authority threatens to erode constitutional protections of fairness and due process.[23]

The fundamental analysis structure relies on this distinction which shows AI strengthens criminal justice systems while unregulated dependency leads to predictive systems becoming prejudiced systems.

International Developments

A. The United States: Algorithmic Adoption Amidst Constitutional Scrutiny

The United States has served as the testing ground in America for predictive policing and algorithmic risk assessment. Tools like COMPAS and PredPol have been adopted by law enforcement and courts, fuelled by the desire to maximize both cost-effectiveness and efficiency.[24] However, their usage has ignited an intense constitutional debate within the bounds of due process and equal protection as stated in the Fourteenth Amendment.

In the case of State v. Loomis[25], the Wisconsin Supreme Court addressed the issue of algorithmic opacity. The defendant claimed that the use of COMPAS risk scores infringed upon his due process rights because he was unable to view or challenge the data or method used in the risk assessment. Although the court decided to uphold the use of COMPAS, it mandated instructions that judges provide cautionary measures so that the algorithm is not considered determinative.[26] This example further sheds light on the tightrope that judges walk daily: AI's benefits stand to be turned off by the ever-present danger of the AI black box.

In addition, the issue of racial bias has been clearly demonstrated by research studies. An investigation carried out by ProPublica in 2016 revealed that the use of the COMPAS system led to Black defendants being categorized as high-risk at twice the rate of white defendants.[27]Similarly, programs for predictive policing like PredPol have been heavily criticized for creating a feedback loop: the deployment of police to minority neighbourhoods leads to increased arrests, which strengthens the bias in the

[23] Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* 130–33 (2020).
[24] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 34–38 (2017).
[25] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
[26] Id. at 763–65.
[27] ProPublica, Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

ISSN: 2582-6433

datasets.[28]

Such issues have led to policy actions. Due to civil rights issues, predictive policing contracts were ended in several U.S. cities such as Santa Cruz and Los Angeles.[29] In Congress, the Algorithmic Accountability Act of 2022 was proposed, which requires companies to prepare impact evaluations of automated decision systems.[30]

Even though the bill has not been passed, it is a strong indication of the need for regulations. At the same time, the judicial systems are still dealing with the issue of whether algorithmic risk assessments adhere to the constitutional standards of procedural due process.

B. The European Union: The Risk-Based Regulatory Model

Unlike the U.S., which tends to respond after issues arise, the European Union has chosen to address potential problems before they happen. Their Artificial Intelligence Act, which they adopted in 2024, is the world's first attempt at crafting a legal framework for AI as a whole.[31] This framework differentiates AI systems with four levels of risk: (1) unacceptable risk (systems that are banned), (2) high risk (systems under strict regulation), (3) limited risk (systems that must comply with transparency rules), and (4) minimal risk (systems that are largely unregulated).

Critically, AI in criminal justice, including predictive policing and biometric identification, is classified as "high-risk."[32]This classification means such AI systems must meet:

1. Conformity assessments before deployment;
2. Human oversight requirements;
3. Transparency requirements, including documentation of training data; and
4. Accountability procedures such as post-market monitoring

The Act, as an example, prohibits the use of real-time facial recognition in public areas, allowing it only in very limited circumstances (for example, the search for a missing child or the prevention of a terrorist attack).[33] The EU's policy is based on the broad fundamental rights framework that the EU has, relying on the Charter of Fundamental

[28] Kristian Lum & William Isaac, To Predict and Serve? Significance (Oct. 2016).
[29] Santa Cruz City Council, Ordinance Banning Predictive Policing Technology (June 2020).
[30] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022).
[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 231)
[32] Id. arts. 6–8.
[33] Id. art. 5.

ISSN: 2582-6433

Rights of the European Union, especially Articles 7 (respect for private life) and 8 (data protection).[34] The EU's framework for the model prioritises the protection of rights instead of efficiency and builds legal frameworks in advance of adoption on a larger scale. Autor's defend this as an example of the EU's precautionary tradition in regulating emerging technologies, which was also seen in data protection with the General Data Protection Regulation (GDPR)[35]. For other regions such as India, the EU's framework works as an example for incorporating constitutional protections within AI regulation.

C. China: Expansive Surveillance with Limited Safeguards

The case of China stands out in this regard. The rest of the world is moving away from it, but China is racing to implement the "Sharp Eyes" and "Safe Cities" programs, which incorporate vast amounts of data to AI-fuelled predictive surveillance and policing. These systems combine facial recognition, large-scale data analysis, and immediate tracking to swiftly check and tag-and-track suspects and keep tabs on "high-risk" clients, as well as to forecast and suppress public disturbances.

An illustrative example is the "Integrated Joint Operations Platform" used by Chinese law enforcement in Xinjiang. This platform compiles data from surveillance cameras, smartphones, and biometric databases to produce "suspicion scores."[36]It has been reported that algorithm-driven detentions are common, which is a flagrant instance of pre-crime justice.[37]

From a legal standpoint, China's Personal Information Protection Law (PIPL) of 2021 is in some aspects reminiscent of GDPR.[38]Nevertheless, public order and state security exemptions under the Chinese framework are far more sweeping than those in the EU, granting practically unrestricted powers to the police.[39]The focus is on state security and social stability, not individual rights.

[34] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1
[35] Paul Craig, EU Administrative Law 258–62 (3d ed. 2018).
[36] Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (May 1, 2019).
[37] Id.
[38] Personal Information Protection Law of the People's Republic of China (adopted Aug. 20, 2021, effective Nov. 1, 2021).
[39] Id. art. 13.

ISSN: 2582-6433

D. Comparative Lessons

The U.S., the EU, and China each reflect different approaches:

- The U.S. seems to have the most cutting-edge AI adoption but addresses its issues last minute through litigation and local legislation, with serious issues about constitutional fitness.
- The EU adopts a rights-based risk tiered model while the AI regulation is embedded beforehand.
- China emphasizes efficiency and security and uses AI on a large scale with little judicial oversight, disregarding rights.

The lesson for India is evident in that the adoption prior to necessary controls is fraught with the danger of embodying the bias of the U.S. or the autocratic tilt of China. India can follow the EU model for protection of rights and modify it to its constitutional structure of Articles 14, 19, and 21.

Issues and Concerns with AI in Criminal Justice

Artificial Intelligence provides efficiency and predictive accuracy, but application in criminal justice can raise many serious questions around fairness, accountability, and human rights. If unchecked, these issues pose a threat to the legitimacy of justice systems.

1. Algorithmic Bias and Discrimination.

AI systems may represent social inequities explicitly because they are developed using historical crime data that were influenced by biased policing practices. For example, the U.S. tool COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), provided, as described by ProPublica, trumpeted a high rate of false positives when labelling African-American defendants high-risk compared to white defendants with similar criminal histories.[40] This supports systemic racism instead of remedying it.

2. Lack of Transparency (The "Black Box" Problem)

Most AI algorithms involved in sentencing or predictive policing are proprietary and therefore opaque, meaning that neither the defendant nor the courts have access to the

[40] Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (May 23, 2016).

ISSN: 2582-6433

decision-making process. This raises due process implications under Article 21 of the Indian Constitution (the Right to Fair Trial), as well as Article 6 of the European Convention on Human Rights (ECHR). In State v. Loomis, the Wisconsin Supreme Court allowed the use of COMPAS but acknowledged the transparency issue creates "serious constitutional issues". [41]

3. **Threat to Due Process and Presumption of Innocence**

Predictive policing shifts the criminal justice system from penalizing past conduct to proactively anticipating future conduct, which creates a "pre-crime" environment much like that of the futuristic movie Minority Report. Predictive policing uses probabilities and statistical likelihood models to punish individuals not for what they may do, but for the potential probabilities of their undertaking a probabilistic future act. Predictive judgments clearly conflict with the presumption of innocence, one of the foundations of criminal law.

4. **Questions Regarding Privacy and Surveillance**

AI surveillance technologies like (China's facial recognition systems), allow governments to monitor millions of their citizens in a "panopticon-like" real-time. These systems may be effective in detecting certain crimes, but create intense violations of an individual's right to privacy under Article 17 of the ICCPR.

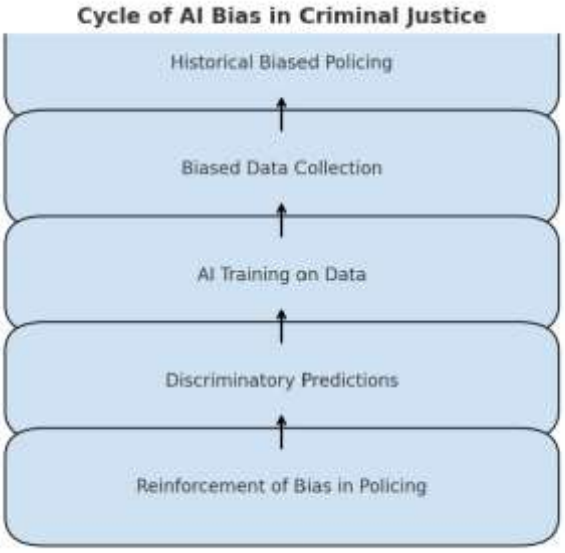
One recent study found that authorities in China used AI surveillance to help monitor the Uyghur minorities, signifying a global concern for digital authoritarianism.[42]

5. **Accountability and Liability Gaps**

When an AI system creates a wrongful outcome (e.g., wrongful arrest or wrongful denial of parole), it is unclear who bears liability: the software company, the state, or the judge relying on the system. This "accountability gap" creates a dangerous legal void. Although the EU's proposed AI Liability Directive tries to fill this gap with strict liability for high-risk AI developers, there are no such frameworks in place in India.

[41] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[42] Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering*

ISSN: 2582-6433



Issues and Concerns with AI in Criminal Justice

Even though the use of Artificial Intelligence (AI) in criminal justice offers a pathway for efficiency, and predictive validity there are serious legal, ethical, and constitutional issues that need to be addressed. These problems are centred on bias, discrimination, transparency, accountability, and rights violations.

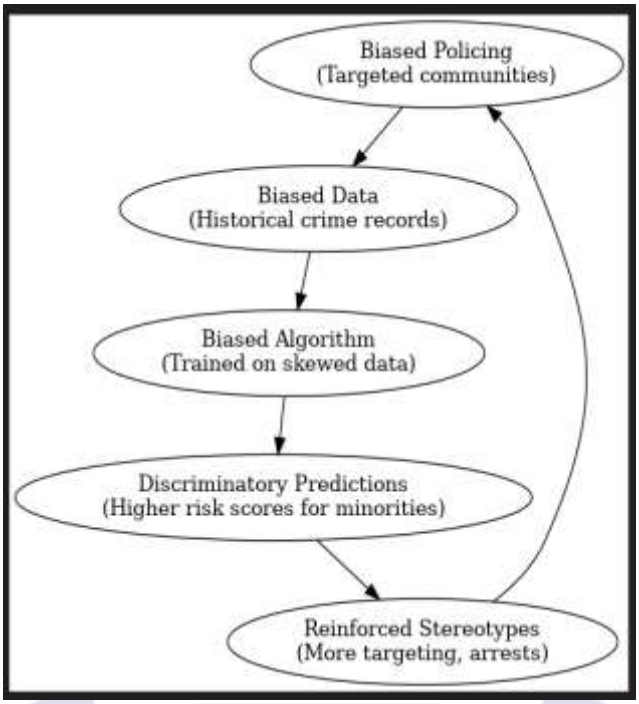
A. Algorithmic Bias and Discrimination

AI systems that rely on historical police data are reflective of structural inequalities that existed within the underlying data. For example, COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), which is utilized in U.S. courts to determine recidivism risk, was able to denote Black defendants as "high risk" nearly two times more than white defendants, while they had similar re-offending rates. [43]This illustrates the loop of bias that AI perpetuates when the foundation is already biased.

[43] Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016).

ISSN: 2582-6433

Flowchart: The Cycle of AI Bias in Criminal Justice



B. Transparency and the "Black Box" Problem

AI models, particularly in the deep learning space, tend to be opaque: The model's reasoning cannot be articulated and explained to judges, or lawyers, or defendants. This is a breach of the due process rights granted by the U.S. Constitution[44] and by Articles 14 and 21 of the Indian Constitution, which require fairness, equality, and so non-arbitrariness in criminal proceedings.

C. Accountability and Liability

Another significant challenge is accountability when things go wrong with the use of AI tools. If an algorithm unjustifiably predicts high-risk behaviour and a resulting judge relies upon that algorithm's recommendation, who is the accountable party — the software company, the state, or the judge? Without an established framework for accountability, we risk establishing a liability vacuum, which discredits the rule of law.

D. Criminal Human Rights Violations

From a global perspective, predictive policing will be violating the right to privacy under Article 17 of the ICCPR[45] and the right against arbitrary detention under Article

[44] U.S. Const. amend. XIV, 1 (Due Process Clause).
[45]International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

ISSN: 2582-6433

9. In India, in the Puttaswamy case [46], OUR Supreme Court ruled that privacy is a fundamental right, and the unchecked use of unharnessed effects of AI surveillance has the possibility to violate people's right to privacy.

E. Indian Concerns

India has begun to implement AI mid-level surveillance, such as the facial recognition system that the Delhi Police deployed during public protests.[47] Reports on the Delhi Police surveillance have indicated an error rate above 30 percent, with the greatest number of wrongful accusations directed towards marginalized and minority groups. This highlights the concern of integrating AI when insufficient regulatory mechanisms are put in place to restrain its use.

Comparative Legal Analysis

The international path of Artificial Intelligence (AI) in criminal justice is varied in legal and ethical strategy. Whereas the United States, European Union, and China have followed proactive models—ranging from predictive policing to legislative controls—India lags behind at a nascent level. A comparative perspective presents not merely the contrast of regulatory development but also common conundrums of balancing innovation, security, and rights.

1. India vs. United States

The American experience highlights the dangers of embracing AI without robust protections. Softwares like COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) have been under severe criticism on racial bias, where Black defendants were almost twice as likely to be incorrectly classified as high-risk as White defendants with comparable backgrounds.[48] Wisconsin v. Loomis courts held that the use of COMPAS was legitimate but raised a red flag concerning due process concerns.[49]

India's adoption of AI, on the other hand, remains experimental. Pilot programs for predictive policing (such as Delhi Police's Crime Mapping Analytics and Predictive System – CMAPS) have not been followed up with legislation checks or judicial

[46] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[47] Shweta Ghosh, *Delhi Police's Use of Facial Recognition During Protests*, The Wire (Feb. 2020).
[48] Julia Angwin et al., Machine Bias, *ProPublica* (May 23, 2016).
[49] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

ISSN: 2582-6433

oversight.[50]Therefore, while the U.S. offers lessons on bias and transparency, India has the chance to formulate safeguards prior to broad deployment.

2. India vs. European Union

The EU is the most rights-based approach. Its draft Artificial Intelligence Act (2021) categorically treats AI in criminal justice as "high-risk," with strict guarantees such as human monitoring, risk evaluation, and transparency requirements.[51] For instance, biometric monitoring of public areas is highly regulated, with the exception of narrowly prescribed objectives such as counter-terrorism.

India does not have a comparable legal framework. The Digital Personal Data Protection Act, 2023 talks about privacy in general but does not cover AI-driven decision-making in criminal law. Therefore, although India and the EU have democratic values in common, regulatory maturity differs drastically between them—EU tending to go for anticipatory legislation, India still relying on piecemeal guidelines.

3. India vs. China

China represents the security-oriented model to the extreme. AI-based surveillance systems, facial recognition technology, and predictive policing (as in Xinjiang) are being deployed aggressively for crime prevention and social control.[52] They work within a legal framework in which state security takes precedence over individual rights.

In India, constitutional protections such as Article 21 (Right to Life and Personal Liberty) and judicial activism (e.g., Puttaswamy v. Union of India, validating privacy as a fundamental right[53] limit the scope of China-style authoritarian deployment. India's limited institutional capacity nevertheless creates apprehensions of "function creep" unless early safeguards are implemented.

4. Key Comparative Insights

Three comparative insights across jurisdictions emerge:

[50] Press Trust of India, Delhi Police Uses AI-Based Crime Mapping System, *The Hindu* (Jan. 2020).
[51] European Commission, Proposal for a Regulation on Artificial Intelligence, COM/2021/206 final.
[52] Human Rights Watch, China's Algorithms of Repression (2019).
[53] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

ISSN: 2582-6433

1. Regulatory Maturity – EU has the most formalised regulation, U.S. is based on judicial oversight, China follows state-driven authoritarian models, and India is in the process of evolving.
2. Rights Protection – EU emphasizes privacy and due process, U.S. struggles with equal protection, China is focused on state security, while India balances rights in the books but has weak enforcement.
3. Ethical Concerns – Bias (U.S.), over-surveillance (China), over-regulation vs. innovation trade-off (EU), and regulatory vacuum (India).

Conclusion

Artificial intelligence in criminal justice is both remarkable promise and deep risk. As witnessed through the examination of predictive policing, risk-assessment software, and judicial use of data-analytics tools, AI is more than a technical achievement but rather a structural change in the manner in which societies construct, identify, and punish crime. At its best, AI increases efficiency, lessens human bias, and enhances law enforcement's preventive reach. At its worse, it reinforces bigotry, subverts due process, and substitutes human judgment with inscrutable, unaccountable decision-making.

The comparative law review conducted here highlights a global fault line. The United States, for all its pioneering uses of AI in policing, continues to be haunted by racial profiling, algorithmic transparency, and inadequate federal regulation, as seen in State v. Loomis and COMPAS controversy. The European Union, in contrast, has embraced a more precautionary approach through the draft AI Act, explicitly categorizing AI in criminal justice as “high-risk” and embedding transparency and accountability requirements. China, meanwhile, exemplifies the perils of unrestrained AI deployment, where predictive policing feeds into a system of social credit and mass surveillance, prioritizing state control over individual liberty. India is in a middle position—trying AI in policing and judiciary, but with no effective regulatory mechanism in place to protect constitutional rights, triggering warnings for unregulated implementation.

An ongoing theme across jurisdictions is the cycle of bias reproduction. Data captured in a discriminatory system produces biased algorithms, which then perpetuate systemic prejudice. This cycle, as shown in Figure 1, shows that the issue is not merely technological but structural and cultural. Regulation therefore needs to address not only the tool but also the policing,

ISSN: 2582-6433

governance, and accountability ecosystem in which AI is situated.

The test for legislators is thus not to ban AI in its entirety, but to embrace its promise while reigning in its dangers. For that, they need a multipronged regulatory approach grounded in the values of transparency, equity, responsibility, and proportionality. Mechanisms like algorithmic audits, explainability standards, human-in-the-loop processes, and public reporting on AI application in criminal justice must be integral components of that framework. No less important is judicial involvement: courts need to develop doctrines safeguarding basic rights against algorithmic arbitrariness, just as they previously safeguarded persons against administrative despotism.

At a normative plane, the issue is whether criminal justice ought to be predictive in the first place. Should law be interested in pre-empting crime on the basis of statistical likelihoods, or in judging real behavior? This philosophical conflict—between prediction and punishment—has not been resolved, and AI raises the stakes for resolving it. A purely predictive model threatens to collapse individuals into data points, stripping them of moral agency and treating them as chronic suspects instead of rights-bearing citizens. Law, though, needs to continue being founded on human dignity, due process, and equality before the law.

This essay therefore advocates for a principled regulation of AI based on international best practices while sensitive to local contexts. The United States emphasizes the risk of proprietary system over-dependence; the EU illustrates rights-based regulation's worth; China cautions against authoritarian abuse; and India, with its constitutional culture of freedom and equality, can create a framework that weighs innovation and protects rights. If carefully designed, such regulation can safeguard against the downward slide "from prediction to prejudice" and guarantee that AI supports justice instead of undermining it.

In the end, A.I. should be a tool — not a judge. The measure of a fair and functioning criminal justice system is not how quickly or efficiently it operates, but how fair, open, and accountable it is. No regulatory model can be allowed to leave out human judgment, constitutional principles, and democratic oversight. Only then can societies also make sure that artificial intelligence serves, rather than sabotages, the goals of justice.