ARTIFICIAL INTELLIGENCE IN THE CRIMINAL JUSTICE SYSTEM: LEGAL AND ETHICAL CHALLENGES

Adv. Basil P Thankaraj, LL.M. (Commercial Law), CSI College for Legal Studies, Kottayam, MG University, Kottayam

ABSTRACT

Artificial Intelligence (AI) has emerged as a transformative force across various sectors, including healthcare, finance, and governance. In recent years, its integration into the criminal justice system has significantly altered traditional methods of policing, investigation, and adjudication. Technologies such as predictive policing, facial recognition, risk assessment algorithms, and automated evidence analysis promise increased efficiency and accuracy in crime prevention and administration of justice. However, these developments also raise profound legal and ethical concerns regarding privacy, fairness, accountability, and human rights.

This article examines the role of Artificial Intelligence in the criminal justice system and analyzes the constitutional, legal, and ethical challenges arising from its application. It explores how AI driven decision-making may threaten fundamental principles such as equality before law, due process, and the right to a fair trial. The study further evaluates the adequacy of existing legal frameworks in regulating AI based technologies and highlights the risk of algorithmic bias and lack of transparency in automated systems.

The article argues that while AI can assist human decision makers, it must not replace judicial discretion or undermine procedural safeguards. The conclusion emphasizes the need for a comprehensive regulatory framework, ethical standards, and judicial oversight to ensure that the use of AI strengthens the rule of law rather than weakening it.

Keywords: Artificial Intelligence, Criminal Justice System, Algorithmic Bias, Privacy, Due Process, Human Rights, Technology Law.

TABLE OF ABBREVIATIONS

AI – Artificial Intelligence

CCTV – Closed-Circuit Television

SCC – Supreme Court Cases

EWCA – England and Wales Court of Appeal

Art – Article

IPC – Indian Penal Code

CrPC – Code of Criminal Procedure

IT Act – Information Technology Act

PIL – Public Interest Litigation

DNA – Deoxyribonucleic Acid

ESG – Environmental, Social and Governance

GDPR – General Data Protection Regulation

TABLE OF CASES

Indian Case Laws:

1. Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
2. Maneka Gandhi v. Union of India (1978) 1 SCC 248
3. Selvi v. State of Karnataka (2010) 7 SCC 263
4. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473

International Case Laws:

5. State v. Loomis , 881 N.W.2d 749 (Wis. 2016)
6. R (Bridges) v. South Wales Police, [2020] EWCA Civ 1058
7. Carpenter v. United States, 585 U.S.(2018) | 138 S. Ct. 2206

1. INTRODUCTION

The criminal justice system is founded on the principles of justice, fairness, accountability, and protection of fundamental rights. Traditionally, the system has relied on human discretion and judicial reasoning in matters of investigation, prosecution, and punishment. However, the rapid development of Artificial Intelligence has introduced a new paradigm in the administration of criminal justice. Law enforcement agencies across the world now rely on AI-driven tools for

predictive policing, biometric identification, and surveillance. Courts increasingly encounter cases where digital evidence is processed and analyzed through algorithmic systems.

Artificial Intelligence refers to the ability of machines to perform tasks that normally require human intelligence, such as learning, reasoning, and decision-making. In the criminal justice context, AI systems analyze large volumes of data to detect patterns and predict outcomes. While this technological shift promises efficiency and accuracy, it also raises profound legal and ethical questions. Can machines replace human judgment in matters affecting life and liberty? Can algorithmic decisions satisfy constitutional standards of fairness and reasonableness? Does technological efficiency justify intrusion into privacy and personal autonomy?[1]

The growing dependence on AI has transformed criminal justice from a human-centered system into a data-driven mechanism. This transformation requires a careful legal evaluation to ensure that technological innovation does not come at the cost of justice, equality, and human rights. The present article seeks to explore the role of Artificial Intelligence in criminal justice and analyze its constitutional, legal, and ethical challenges.

2. CONCEPT OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Artificial Intelligence in criminal justice involves the use of algorithmic systems to assist or influence decisions at different stages of the justice process. Predictive policing uses historical crime data to forecast where crimes are likely to occur and who is likely to commit them. Facial recognition technology identifies individuals by comparing biometric data with digital databases. Risk assessment algorithms evaluate the probability of reoffending and are used in bail and sentencing decisions. AI is also widely used in digital forensics to analyze CCTV footage, call records, emails, and social media activity.

These technologies operate through complex mathematical models that process vast amounts of data beyond human capacity. Supporters of AI argue that such systems increase efficiency, reduce human error, and improve objectivity. However, critics contend that these systems often lack transparency and are prone to bias. Algorithms are designed and trained by humans and therefore reflect human prejudices and assumptions. The danger lies in treating algorithmic

[1] See Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–5 (3d ed. 2010).

outputs as neutral and infallible while ignoring their underlying flaws.[2]

Moreover, AI systems tend to function as "black boxes," where the logic behind decisions is not easily accessible or understandable. This creates serious difficulties in legal proceedings where transparency and accountability are essential. When a person is denied bail or subjected to police scrutiny based on an algorithmic assessment, it becomes necessary to know how and why such a decision was reached. Without such knowledge, the accused is deprived of the opportunity to challenge the decision, thereby weakening procedural justice.

3. CONSTITUTIONAL FRAMEWORK AND FUNDAMENTAL RIGHTS

The use of AI in criminal justice directly impacts several constitutional guarantees, particularly the right to privacy, the right to fair trial, and the principle of equality before law. The right to privacy has assumed central importance in the digital age, where personal data is constantly collected and processed. In Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court of India recognized privacy as a fundamental right under Article 21 and held that any infringement must satisfy the tests of legality, necessity, and proportionality. AI-based surveillance systems, facial recognition cameras, and biometric databases involve continuous monitoring and data collection, which may violate these standards if implemented without clear legal authority and safeguards.[3]

Mass surveillance through AI tools poses the danger of creating a surveillance state where individuals are constantly observed and evaluated. Such a system undermines autonomy and dignity, which are integral to the right to life and personal liberty. The absence of comprehensive data protection laws further aggravates this problem, as personal information can be misused or exploited without accountability.

The right to fair trial and due process of law is another cornerstone of criminal justice. In Maneka Gandhi v. Union of India (1978), the Supreme Court held that any procedure affecting personal liberty must be just, fair, and reasonable. This principle requires transparency, opportunity to be heard, and reasoned decision-making. AI systems, however, often operate through undisclosed algorithms, making it impossible to scrutinize their reasoning. When courts or law enforcement agencies rely on such systems, they risk violating the accused's right

[2] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[3] INDIA CONST. arts. 21–22.

to a fair trial.[4]

The principle of equality before law under Article 14 is also threatened by algorithmic bias. AI systems rely on historical data that may reflect social inequalities related to caste, class, or economic status. When such data is used to train algorithms, the resulting predictions may disproportionately target marginalized communities. This creates a cycle of discrimination where certain groups are repeatedly subjected to police scrutiny and harsher treatment. Such outcomes violate the constitutional guarantee of equal protection of laws and undermine public confidence in the justice system.[5]

4. ETHICAL AND LEGAL CHALLENGES

One of the most significant challenges posed by AI in criminal justice is algorithmic bias. AI systems learn from past data, and if that data reflects biased policing or discriminatory practices, the algorithm will reproduce and amplify those patterns. This means that AI does not eliminate human prejudice but rather embeds it into technological systems. The danger of such bias is that it is often hidden and difficult to detect, making discrimination appear objective and scientific.

Another major challenge is the lack of transparency in algorithmic decision-making. Many AI tools used in criminal justice are developed by private companies and protected as proprietary technologies. This prevents public scrutiny and judicial examination of their functioning. Transparency is a fundamental requirement of justice, and secret algorithms undermine the legitimacy of legal decisions. When an accused person cannot understand or challenge the basis of a decision affecting liberty, the principle of natural justice is violated.

Accountability is also a critical concern. In traditional legal systems, responsibility for decisions lies with identifiable human actors such as police officers and judges. With AI systems, responsibility becomes diffused among programmers, users, and institutions. This makes it difficult to determine who should be held accountable for errors or injustices caused by algorithmic decisions. Such diffusion of responsibility weakens the deterrent effect of law and erodes trust in legal institutions.[6]

[4] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248, 283–84 (India).
[5] INDIA CONST. art. 14.
[6] Council of Eur., *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule*

Furthermore, excessive reliance on machines risks dehumanizing justice. Criminal law involves moral evaluation, empathy, and contextual understanding, which cannot be reduced to numerical probabilities. AI systems lack the capacity for compassion and ethical reasoning, making them unsuitable as independent decision-makers in matters involving life and liberty.

5. AI AND CRIMINAL INVESTIGATION

The use of AI in criminal investigation has expanded through surveillance technologies, data analytics, and forensic tools. Law enforcement agencies increasingly rely on facial recognition systems and predictive analytics to identify suspects and prevent crime. While these tools enhance efficiency, they also intrude deeply into personal liberty. The Supreme Court has previously scrutinized the use of scientific techniques in criminal investigation. In Selvi v. State of Karnataka (2010), the Court held that involuntary administration of narco-analysis, polygraph tests, and brain mapping violated the right against self-incrimination and personal liberty under Articles 20(3) and 21. The Court emphasized that technological methods cannot override constitutional protections.

The reasoning in Selvi is highly relevant to AI-based investigative tools. Just as involuntary scientific tests were found unconstitutional, unregulated use of AI surveillance and data mining may similarly infringe upon mental privacy and bodily autonomy. The principle that technology must operate within constitutional limits applies equally to modern AI systems.[7]

The admissibility of AI-generated evidence also raises complex issues. Digital evidence processed through AI must satisfy legal standards of authenticity and reliability. In Anvar P.V. v. P.K. Basheer (2014), the Supreme Court laid down strict conditions for the admissibility of electronic evidence under Section 65B of the Evidence Act. As AI increasingly plays a role in analyzing digital material, courts must ensure that such evidence meets statutory requirements and that its methodology can be scrutinized by the defense. Without such safeguards, AI-generated evidence may compromise the fairness of trials.[8]

6. COMPARATIVE JUDICIAL PERSPECTIVE

International jurisprudence provides valuable guidance on the regulation of AI in criminal

of Law, CETS No. 225 (2024).
[7] *Selvi v. State of Karnataka*, (2010) 7 S.C.C. 263, 302–03 (India).
[8] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, India Code (2023).

justice. In State v. Loomis (2016), the United States Supreme Court considered the use of a risk assessment algorithm in sentencing. While the Court permitted its use, it acknowledged serious concerns regarding transparency and potential bias. The case sparked global debate on whether algorithmic tools can be reconciled with due process and fairness.

In the United Kingdom, the Court of Appeal in R (Bridges) v. South Wales Police (2020) held that the use of live facial recognition technology violated privacy rights due to the absence of a proper legal framework and safeguards. The Court emphasized that technological innovation must be accompanied by clear legal standards to prevent misuse. Similarly, in Carpenter v. United States (2018), the US Supreme Court recognized that digital surveillance technologies require heightened constitutional scrutiny due to their intrusive nature.

These decisions reflect a growing global consensus that AI must be regulated within the framework of human rights and constitutional law. Efficiency and innovation cannot justify erosion of fundamental freedoms.

7. FUTURE PROSPECTS AND SAFEGUARDS

The future of AI in criminal justice must be guided by strong legal and ethical safeguards. Comprehensive legislation is required to define the permissible scope of AI use in policing and courts. Such laws should ensure transparency, accountability, and protection of fundamental rights. Algorithmic decision-making must be open to judicial review, and individuals should have the right to know and challenge how decisions affecting their liberty are made.

Human oversight must remain central to the justice process. AI should function only as a decision-support tool rather than an independent authority. Judges and law enforcement officers must exercise independent judgment and not blindly rely on algorithmic outputs. Strong data protection mechanisms are essential to prevent misuse of personal and biometric information. Ethical principles such as fairness, non-discrimination, and proportionality should guide the development and deployment of AI systems.[9]

Judicial activism may also play a crucial role in shaping AI jurisprudence. Courts must interpret constitutional guarantees in light of technological realities and ensure that innovation does not undermine human dignity. The evolution of AI law must therefore be rooted in constitutional

[9] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

morality and respect for individual rights.

8. CONCLUSION

Artificial Intelligence has the potential to revolutionize the criminal justice system by improving efficiency, accuracy, and resource allocation. However, its unchecked use poses serious risks to constitutional values such as privacy, equality, due process, and human dignity. Justice cannot be reduced to algorithmic outputs devoid of human reasoning and moral judgment. The growing dependence on machines risks transforming criminal justice into a mechanized process detached from ethical considerations.

The law must evolve alongside technology to ensure that innovation strengthens rather than weakens the rule of law. AI should be treated as an auxiliary tool that assists human decision-makers, not as an authority that replaces them. Judicial oversight, legislative regulation, and ethical governance are indispensable to preserving justice in the digital age. Ultimately, true progress lies not merely in technological advancement but in the ability of the legal system to uphold fairness, accountability, and human dignity in an increasingly automated world.