Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

Artificial Intelligence in Criminal Justice Administration: Legal Challenges, Ethical Concerns, and the Need for Regulatory Framework in India

Dr. Tarushi Gaur[1], Shivanshu Katare[2]

[1]Assistant Professor, St Wilfred College of Law
[2]Assistant Professor, Faculty of Law, Manipal University Jaipur

Abstract:
The integration of Artificial Intelligence (AI) into criminal justice administration is transforming investigative processes, predictive policing, evidence analysis, sentencing assessment, and prison management across jurisdictions. In India, emerging applications such as facial recognition systems, predictive crime mapping, automated risk assessment tools, and AI-driven forensic analytics present significant opportunities for enhancing efficiency, accuracy, and resource allocation within law enforcement and judicial systems. However, the adoption of AI technologies also raises profound legal and ethical concerns relating to privacy, due process, transparency, accountability, algorithmic bias, and the presumption of innocence. The absence of a comprehensive statutory framework governing AI deployment in criminal justice intensifies the risk of arbitrary surveillance, discriminatory profiling, and opaque decision-making. Constitutional guarantees under Articles 14, 19, and 21 of the Constitution of India particularly the right to equality, freedom, and privacy require that AI-driven interventions meet standards of fairness, proportionality, and procedural safeguards. Furthermore, concerns regarding data protection, explainability of algorithms, and liability for automated decisions underscore the urgent need for regulatory clarity. This paper critically examines the legal challenges posed by AI integration in India's criminal justice system, analyses ethical implications, and argues for a rights-based regulatory framework grounded in constitutional principles and international human rights norms. It proposes legislative oversight, transparency mandates, independent audits, and accountability mechanisms to ensure that technological innovation does not undermine civil liberties. The development of a robust regulatory regime is essential to balance efficiency with justice and to preserve the integrity of India's democratic legal order.

Keywords: Artificial Intelligence, Criminal Justice, Algorithmic Bias, Due Process, Privacy, Regulatory Framework.

1. INTRODUCTION

The rapid integration of Artificial Intelligence (AI) into governance structures has significantly transformed public administration worldwide, and the criminal justice system is no exception. AI technologies ranging from facial recognition systems and predictive policing algorithms to automated risk assessment tools and digital evidence analytics are increasingly influencing how crimes are detected, investigated, prosecuted, and adjudicated. In India, law enforcement agencies and judicial institutions have

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

begun experimenting with AI-based tools to enhance efficiency, reduce case backlogs, improve investigative accuracy, and strengthen crime prevention strategies. However, the deployment of AI in criminal justice raises profound constitutional, legal, and ethical concerns. The use of algorithmic decision-making in matters affecting personal liberty directly implicates core constitutional guarantees under Articles 14, 19, and 21 of the Constitution of India, particularly the rights to equality, freedom, and life and personal liberty.

Artificial Intelligence in the criminal justice context refers to computational systems capable of performing tasks that traditionally require human judgment, including pattern recognition, predictive analytics, and probabilistic assessments. AI systems process large datasets to identify trends, forecast potential criminal activity, and assist in decision-making processes such as bail, sentencing, and parole determinations. In India, applications such as facial recognition technology (FRT), crime mapping software, and data-driven surveillance mechanisms have gained prominence. For instance, law enforcement agencies have deployed automated facial recognition systems to identify suspects during public gatherings, raising concerns regarding mass surveillance and privacy. Similarly, predictive policing models attempt to anticipate crime hotspots based on historical data. While these technologies promise efficiency and enhanced resource allocation, they also risk reinforcing systemic biases embedded within historical datasets.

The constitutional framework governing criminal justice in India emphasizes procedural fairness, presumption of innocence, and protection against arbitrary state action. The Supreme Court's jurisprudence, particularly in *Maneka Gandhi v. Union of India* (1978), expanded the interpretation of Article 21 to require that any procedure depriving personal liberty must be just, fair, and reasonable. Furthermore, in *Justice K.S. Puttaswamy v. Union of India* (2017), the Court recognized the right to privacy as a fundamental right intrinsic to personal liberty and dignity. The deployment of AI-driven surveillance tools directly engages these principles. When algorithms are used to predict criminal behavior or identify suspects without transparent standards, questions arise regarding arbitrariness, lack of accountability, and the erosion of due process safeguards.

A central concern with AI in criminal justice administration is algorithmic opacity. Many AI systems operate as "black boxes," where the internal logic and decision-making processes are not easily explainable. This lack of transparency challenges the constitutional requirement of reasoned decision-making and undermines the ability of accused persons to contest adverse determinations. The principle of natural justice, particularly audi alteram partem (the right to be heard), becomes difficult to operationalize if individuals cannot understand how algorithmic assessments influence outcomes. Additionally, algorithmic bias arising from skewed training data or flawed modeling can disproportionately impact marginalized communities, thereby violating Article 14's guarantee of equality before the law.

The Indian criminal justice system already grapples with systemic challenges such as case backlogs, overcrowded prisons, and investigative inefficiencies. AI technologies are often presented as solutions capable of enhancing institutional capacity. For example, AI-driven document analysis tools can assist courts in managing voluminous case records, and automated transcription services can streamline trial processes. However, technological efficiency cannot override constitutional safeguards. The integration of AI must therefore be accompanied by a robust regulatory framework that ensures transparency, accountability, data protection, and judicial oversight.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

Internationally, debates concerning AI in criminal justice emphasize the need for rights-based governance models. Jurisdictions such as the European Union have proposed regulatory mechanisms that classify AI systems based on risk levels, imposing stricter requirements for high-risk applications affecting fundamental rights. India currently lacks a comprehensive statutory framework specifically addressing AI deployment in criminal justice. Although policy initiatives such as the National Strategy for Artificial Intelligence highlight innovation and technological advancement, they do not provide enforceable safeguards against misuse. The absence of clear legislative standards creates a regulatory vacuum, leaving critical questions of liability, oversight, and accountability unresolved.

This article examines the legal and constitutional implications of integrating AI into India's criminal justice administration. It argues that while AI offers transformative potential, its deployment must be anchored in constitutional morality and human rights principles. Without a carefully designed regulatory architecture, the use of AI risks undermining due process, reinforcing discrimination, and eroding public trust in the justice system. The introduction establishes the normative foundation for a detailed examination of legal challenges and ethical concerns arising from AI-driven criminal justice mechanisms.

2. LEGAL CHALLENGES IN THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

The integration of AI technologies into criminal justice administration presents multifaceted legal challenges that intersect with constitutional principles, statutory safeguards, and evidentiary standards. The first and most significant challenge relates to the right to privacy. The Supreme Court's landmark decision in *Justice K.S. Puttaswamy v. Union of India* (2017) recognized privacy as a fundamental right under Article 21, encompassing informational privacy and protection against unwarranted state surveillance. AI-powered facial recognition systems, biometric databases, and predictive analytics rely on large-scale data collection and processing. The deployment of such systems without clear statutory backing or proportional safeguards may amount to unconstitutional surveillance. The doctrine of proportionality articulated in *Puttaswamy* requires that any restriction on fundamental rights pursue a legitimate aim, be suitable and necessary, and maintain a balance between state interests and individual liberty. Many AI applications in policing currently operate in a legal grey area, raising concerns regarding compliance with these constitutional standards.

A second major legal issue concerns equality and non-discrimination under Article 14. AI systems trained on historical crime data may inadvertently replicate or amplify existing biases within the criminal justice system. If certain communities have historically been over-policed, predictive policing algorithms may disproportionately target those areas, creating a feedback loop of surveillance and enforcement. This phenomenon risks perpetuating structural discrimination. Unlike human decision-makers, algorithmic systems often lack contextual sensitivity, and their outputs may appear objective despite underlying biases. The constitutional guarantee of equality demands that state action be free from arbitrariness and discriminatory impact. Courts may therefore be required to evaluate whether AI-driven decisions satisfy the test of reasonable classification and non-arbitrariness.

The third legal challenge involves due process and fair trial rights. Criminal adjudication in India is governed by principles embedded in the Code of Criminal Procedure, 1973 and the Indian Evidence Act, 1872. When AI-generated evidence or risk assessments are introduced in judicial proceedings, questions arise regarding admissibility, reliability, and cross-examination. For example, if an AI tool predicts the

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

likelihood of reoffending and influences bail decisions, the accused must have an opportunity to challenge the validity of the algorithm. However, proprietary algorithms developed by private vendors may be protected as trade secrets, limiting disclosure. This tension between intellectual property rights and fair trial guarantees complicates the legal landscape.

Additionally, accountability and liability represent unresolved legal concerns. When an AI system produces an erroneous identification leading to wrongful arrest, determining responsibility becomes complex. Should liability rest with the software developer, the law enforcement agency deploying the system, or the individual officer relying on the output? The absence of statutory clarity on this issue undermines legal certainty. Traditional principles of administrative law require that state action be reasoned and attributable. Automated decision-making blurs these lines, making it difficult to assign accountability.

Data protection constitutes another critical legal dimension. AI systems rely on large datasets, often including sensitive personal information such as biometric identifiers. Although India has recently enacted digital data protection legislation, its application to law enforcement and national security contexts may include exemptions. Without stringent safeguards, data misuse or unauthorized access could infringe upon informational privacy rights. Moreover, the retention and sharing of biometric data across agencies raise concerns about function creep, where data collected for one purpose is repurposed without adequate oversight.

The evidentiary value of AI-generated outputs also requires scrutiny. Under the Indian Evidence Act, electronic evidence must satisfy authenticity and reliability requirements. AI systems that operate probabilistically may not produce deterministic conclusions, complicating their evidentiary weight. Courts must consider whether reliance on algorithmic outputs satisfies standards of proof beyond reasonable doubt in criminal cases. The risk of overreliance on technological tools may undermine judicial independence and human discretion.

Finally, the absence of a comprehensive regulatory framework governing AI in criminal justice exacerbates these challenges. While policy documents encourage innovation, enforceable guidelines on transparency, auditability, and oversight remain limited. Judicial pronouncements have emphasized that technological advancement cannot override constitutional safeguards. Therefore, integrating AI into criminal justice administration necessitates clear legislative standards that address privacy, equality, accountability, and procedural fairness.

The legal challenges associated with AI in criminal justice are deeply intertwined with constitutional principles and statutory protections. Without robust safeguards, AI-driven tools risk eroding due process, amplifying discrimination, and creating opaque systems of governance. The need for a comprehensive regulatory framework grounded in constitutional values is therefore urgent and indispensable for ensuring that technological innovation strengthens rather than undermines justice.

3. ETHICAL CONCERNS IN THE DEPLOYMENT OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Beyond constitutional and statutory legality, the integration of Artificial Intelligence (AI) into criminal justice administration raises profound ethical concerns that directly affect the legitimacy and moral

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

foundation of the justice system. Criminal justice institutions are built upon principles of fairness, accountability, transparency, and human dignity. The use of AI-driven decision-making mechanisms particularly in policing, bail determination, sentencing recommendations, and surveillance introduces complex ethical dilemmas that cannot be resolved solely through technical efficiency or administrative convenience. Ethical governance requires that technological interventions respect individual autonomy, prevent discrimination, and preserve public trust in the justice system.

One of the foremost ethical concerns is algorithmic bias. AI systems are trained on historical datasets that may reflect systemic inequalities embedded within society. If policing data disproportionately reflects arrests or surveillance in marginalized communities, predictive algorithms may reproduce and amplify those disparities. This phenomenon, often described as "data-driven discrimination," creates a feedback loop in which historically over-policed communities become further targeted (O'Neil, 2016). From an ethical standpoint, the principle of fairness demands that technological systems do not entrench structural injustice. Even if unintentional, discriminatory outputs undermine the moral legitimacy of criminal justice administration and conflict with the egalitarian ethos of constitutional democracy.

Closely linked to bias is the issue of transparency and explainability. Many AI models, particularly those employing deep learning techniques, function as "black boxes," where the internal reasoning process is not easily interpretable. In criminal justice contexts, opaque decision-making is ethically problematic because individuals affected by algorithmic outputs may not understand how conclusions were reached. Ethical governance requires explainability commonly referred to as "algorithmic transparency" so that affected persons can meaningfully contest decisions (Binns, 2018). When AI tools influence bail decisions or suspect identification, lack of transparency compromises not only legal rights but also ethical accountability. Decision-making processes that cannot be explained risk eroding public confidence in the justice system.

Another major ethical issue concerns autonomy and human agency. Criminal justice decisions traditionally involve human judgment, discretion, and contextual evaluation. The increasing reliance on AI systems risks creating "automation bias," where human actors defer excessively to algorithmic recommendations (Crawford, 2021). Ethical decision-making requires maintaining meaningful human oversight, particularly in determinations affecting liberty. The delegation of critical decisions to automated systems may dilute individual accountability and create a perception that responsibility lies with technology rather than human actors. Such diffusion of responsibility undermines ethical principles of answerability and moral agency.
Privacy and surveillance represent additional ethical concerns. AI-powered facial recognition systems and predictive surveillance tools enable large-scale monitoring of public spaces. While such systems may enhance crime detection, they simultaneously threaten individual autonomy and chill democratic freedoms such as assembly and expression. Ethical frameworks emphasize proportionality and necessity in surveillance practices (United Nations High Commissioner for Human Rights [UNHCHR], 2021). Indiscriminate or continuous monitoring risks normalizing a surveillance society where individuals alter behavior due to fear of constant observation. The ethical tension lies in balancing collective security with respect for personal space and dignity.

Furthermore, there are ethical concerns regarding the presumption of innocence and predictive justice. AI-based predictive policing tools forecast potential criminal activity based on statistical correlations rather than individual culpability. This predictive approach may inadvertently shift the focus from proven

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

conduct to anticipated behavior. Ethical principles within criminal jurisprudence emphasize that individuals should be judged on actions, not probabilities. Overreliance on risk assessment tools may erode the foundational presumption of innocence by treating individuals as potential threats rather than rights-bearing citizens.

Equally significant is the issue of consent and data governance. AI systems require extensive data collection, often including biometric information, geolocation data, and personal identifiers. Ethical governance demands informed consent, purpose limitation, and data minimization. In criminal justice contexts, however, individuals may have little opportunity to consent or object to data processing. The ethical obligation to protect vulnerable populations becomes especially pressing when state power intersects with technological surveillance.

Finally, the broader ethical question concerns legitimacy and trust. Criminal justice institutions derive authority not only from law but also from societal confidence in their fairness. If AI systems are perceived as opaque, biased, or unaccountable, public trust may erode. Ethical AI governance therefore requires participatory oversight, public consultation, and inclusive policymaking to ensure that technological adoption aligns with democratic values.

The ethical concerns associated with AI in criminal justice extend beyond legality to fundamental questions of fairness, autonomy, transparency, and dignity. Addressing these concerns requires embedding ethical principles within regulatory frameworks and institutional practices. Without deliberate safeguards, AI-driven criminal justice risks compromising the very values it seeks to uphold.

4. THE NEED FOR A COMPREHENSIVE REGULATORY FRAMEWORK IN INDIA

The convergence of legal and ethical challenges underscores the urgent need for a comprehensive regulatory framework governing the use of AI in India's criminal justice administration. While technological innovation holds the potential to improve efficiency and resource allocation, its deployment must be anchored in constitutional principles, human rights standards, and ethical safeguards. Currently, India lacks a dedicated statutory regime that specifically addresses AI use in policing, judicial decision-making, or correctional administration. Policy initiatives encouraging digital governance do not substitute for enforceable legal standards ensuring accountability and rights protection.

A foundational element of regulatory reform must be the adoption of a risk-based classification model. High-risk AI systems such as facial recognition tools, predictive policing algorithms, and automated risk assessment instruments should be subject to stringent oversight. Comparative regulatory approaches, such as the European Union's AI regulatory proposals, classify systems based on their impact on fundamental rights, imposing stricter compliance requirements on high-risk applications (European Commission, 2021). India could adopt a similar model, requiring mandatory human oversight, periodic audits, and transparency disclosures for AI systems deployed in criminal justice contexts.

Transparency and explainability must form core pillars of the regulatory framework. Developers and deploying agencies should be required to disclose the logic, data sources, and performance metrics of AI systems. Independent algorithmic audits could assess bias, accuracy, and reliability before and during deployment. Transparency enhances accountability and facilitates judicial scrutiny where necessary.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

Courts must have access to sufficient information to evaluate whether algorithmic tools comply with constitutional standards of fairness and non-arbitrariness.

Data protection and privacy safeguards constitute another essential regulatory dimension. AI systems operating within criminal justice rely heavily on biometric and personal data. Regulatory frameworks should incorporate strict purpose limitation, data minimization, retention limits, and secure storage requirements. Oversight bodies must monitor compliance to prevent misuse or unauthorized data sharing. Aligning AI governance with constitutional privacy jurisprudence ensures that surveillance tools do not exceed legitimate objectives.

Accountability mechanisms are equally critical. Clear allocation of liability must be established in cases of wrongful arrest or erroneous identification resulting from AI outputs. Administrative law principles require that state action be attributable and reviewable. A statutory regime should clarify the responsibility of law enforcement agencies, supervisory authorities, and technology providers. Without defined accountability structures, victims of algorithmic errors may struggle to obtain remedies.

Additionally, meaningful human oversight must be mandated. AI systems should function as decision-support tools rather than decision-makers. Final determinations affecting liberty such as bail, sentencing, or preventive detention must remain within human judicial discretion. Regulatory standards should prohibit fully automated decisions in criminal justice without human review. This safeguard preserves moral agency and reinforces the constitutional commitment to due process.

Capacity building and judicial training are also indispensable components of reform. Judges, prosecutors, and law enforcement officials require technical literacy to understand algorithmic processes and limitations. Without adequate knowledge, oversight mechanisms may prove ineffective. Educational initiatives can strengthen institutional competence and prevent blind reliance on technological outputs.
Finally, public participation and democratic oversight should guide AI governance. The development of regulatory standards must involve consultation with civil society, legal scholars, technologists, and affected communities. Transparent policymaking enhances legitimacy and fosters trust in technological innovation.

The regulation of AI in India's criminal justice system must balance innovation with constitutional fidelity. A comprehensive framework grounded in transparency, accountability, proportionality, and human oversight is essential to prevent erosion of civil liberties. By embedding ethical and constitutional safeguards into the architecture of AI governance, India can harness technological advancements while preserving the integrity of its democratic legal order.

5. COMPARATIVE REGULATORY APPROACHES AND GLOBAL BEST PRACTICES

The development of an effective regulatory framework for Artificial Intelligence (AI) in India's criminal justice system can benefit significantly from comparative legal experiences and evolving global standards. Across jurisdictions, governments and international organizations have recognized that AI systems deployed in high-stakes environments such as policing, sentencing, and surveillance require enhanced oversight to safeguard fundamental rights. Comparative analysis reveals a growing consensus that risk-based regulation, transparency, accountability, and human oversight are indispensable elements of responsible AI governance.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

The European Union (EU) has adopted one of the most comprehensive regulatory approaches through the proposed Artificial Intelligence Act. The EU model classifies AI systems according to risk levels, with "high-risk" systems such as those used in law enforcement, biometric identification, and judicial decision-making subject to strict compliance requirements, including mandatory conformity assessments, data governance standards, transparency obligations, and human oversight mechanisms (European Commission, 2021). Biometric surveillance systems, particularly real-time facial recognition in public spaces, are treated with heightened scrutiny due to their potential impact on privacy and freedom of expression. This risk-based model reflects a recognition that criminal justice applications directly implicate fundamental rights and therefore demand more rigorous safeguards than low-risk commercial AI tools.

In the United States, regulatory responses have been more fragmented but have increasingly emphasized due process and algorithmic accountability. Judicial scrutiny of risk assessment tools used in sentencing, such as in *State v. Loomis* (2016), highlighted concerns regarding proprietary algorithms and transparency. Although the Wisconsin Supreme Court permitted the use of risk assessment software, it cautioned against overreliance and mandated judicial awareness of limitations. Moreover, several U.S. municipalities have restricted or banned facial recognition technology in policing due to concerns over racial bias and privacy violations (Garvie et al., 2016). These developments underscore the importance of public accountability and local oversight in regulating high-risk technologies.

International human rights bodies have also articulated normative principles for AI governance. The United Nations High Commissioner for Human Rights (2021) has called for a moratorium on AI systems that pose serious risks to human rights, particularly biometric surveillance technologies lacking adequate safeguards. The Organisation for Economic Co-operation and Development (OECD) Principles on AI emphasize transparency, robustness, accountability, and respect for human rights (OECD, 2019). These principles reflect an emerging global consensus that technological innovation must align with democratic values and rule-of-law principles.

Comparative experiences further demonstrate the importance of independent auditing and impact assessments. Algorithmic impact assessments (AIAs), which evaluate potential risks before deployment, are increasingly recommended as a best practice. Such assessments examine data quality, bias, proportionality, and anticipated societal impact. Incorporating mandatory AIAs within India's regulatory framework would enhance accountability and prevent unintended harm. Regular third-party audits could ensure ongoing compliance and detect discriminatory outcomes.

Another significant aspect of global best practice involves participatory governance. Transparent public consultations, civil society engagement, and parliamentary oversight contribute to legitimacy and public trust. Democratic oversight mechanisms prevent AI deployment from becoming an exclusively technocratic endeavor detached from societal values. For India, where public confidence in criminal justice institutions is essential for effective governance, embedding participatory safeguards within AI regulation would strengthen institutional credibility.

Finally, comparative jurisprudence reinforces the necessity of maintaining meaningful human control. Both European and American legal developments stress that automated systems should assist not replace

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

human judgment in decisions affecting liberty. Ensuring that judges and law enforcement officials retain ultimate decision-making authority preserves accountability and aligns with due process guarantees.
In sum, comparative regulatory approaches offer valuable lessons for India. Risk-based classification, transparency mandates, algorithmic audits, participatory governance, and strict oversight of biometric surveillance represent key components of emerging global standards. Adapting these principles within the Indian constitutional context can ensure that AI deployment in criminal justice enhances efficiency without compromising civil liberties.

6. CONCLUSION AND RECOMMENDATIONS FOR A RIGHTS-BASED REGULATORY FRAMEWORK

The integration of Artificial Intelligence into India's criminal justice administration represents a transformative development with far-reaching implications for constitutional governance. While AI technologies promise efficiency, predictive capacity, and improved administrative coordination, their deployment within a system that directly impacts personal liberty necessitates careful constitutional scrutiny. The principles of equality, due process, privacy, and dignity enshrined under Articles 14, 19, and 21 of the Constitution of India serve as normative anchors that must guide technological adoption. Without robust safeguards, AI-driven systems risk entrenching bias, undermining procedural fairness, and eroding public trust in the justice system.

A rights-based regulatory framework should begin with comprehensive legislation specifically addressing AI in criminal justice contexts. Such legislation must clearly define permissible uses, establish risk classifications, and mandate compliance standards for high-risk applications such as facial recognition and predictive policing. Incorporating proportionality analysis consistent with constitutional jurisprudence in *Maneka Gandhi v. Union of India* (1978) and *Justice K.S. Puttaswamy v. Union of India* (2017) would ensure that AI deployment is necessary, suitable, and balanced against individual rights.

Transparency and explainability should form central pillars of reform. Mandatory disclosure of data sources, algorithmic logic, and accuracy metrics would enable meaningful judicial and public scrutiny. Individuals adversely affected by algorithmic decisions must have access to remedies, including the right to challenge AI-generated outcomes. Establishing statutory obligations for independent audits and impact assessments would further enhance accountability.

Data protection safeguards must be rigorously enforced. AI systems in criminal justice often rely on sensitive biometric and personal data. Clear limitations on data collection, retention, and sharing are essential to prevent misuse. Oversight by an independent regulatory authority potentially in coordination with data protection bodies would provide institutional checks against abuse.

Human oversight must remain non-negotiable. Automated systems should function strictly as decision-support tools. Final determinations affecting liberty such as bail, sentencing, or preventive detention must rest with accountable human authorities. Prohibiting fully automated decision-making in criminal justice contexts preserves moral agency and aligns with principles of natural justice.

Capacity building within the judiciary and law enforcement agencies is equally crucial. Technical literacy and ethical awareness training can empower officials to critically evaluate algorithmic outputs rather than

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 1, January-February 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i01.1207

relying on them unquestioningly. Education initiatives should emphasize the limitations and risks of AI technologies.

Finally, democratic oversight and public participation must inform regulatory development. Engaging civil society, legal experts, technologists, and marginalized communities ensures that AI governance reflects diverse perspectives and protects vulnerable groups from disproportionate harm. Transparent policy formulation enhances legitimacy and fosters trust.

In conclusion, Artificial Intelligence presents both opportunity and risk for India's criminal justice system. Harnessing its benefits requires a calibrated regulatory approach rooted in constitutional morality and human rights principles. By embedding transparency, accountability, proportionality, and human oversight into the architecture of AI governance, India can ensure that technological innovation strengthens rather than undermines justice. A robust, rights-oriented regulatory framework will not only safeguard civil liberties but also reinforce the integrity and credibility of India's democratic legal order.

REFERENCES:

1. Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 81, 149–159.
2. Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
3. European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*.
4. Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
5. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
6. O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing.
7. United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age*.
8. European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*.
9. Garvie, C., Bedoya, A. M., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law Center on Privacy & Technology.
10. Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
11. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
12. OECD. (2019). *OECD principles on artificial intelligence*. Organisation for Economic Co-operation and Development.
13. State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
14. United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age*.