Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 6 Issue 1 (2026)

The Future of Justice: Navigating AI's Ethical and Legal Maze In India's Criminal Justice System

Kritika Goyal[1*]
[1]Research Scholar, School of Law, Sushant University, Gurgaon, Haryana, India
*Corresponding Email Id: Kritikapgoyal@gmail.com

Dr. Shreya[2]

[2]Assistant Professor, School of Law, Sushant University, Gurgaon, Haryana, India

ABSTRACT

With India going digital, there is no aspect left that has not been influenced by digital technology. "artificial intelligence (AI) "has become a major tool to transform the criminal justice system. All these methods, from predictive policing to face recognition to courtroom legal research and AI-facilitated judicial decision-making, are being quickly incorporated into police procedures and court processes. But the use of AI in such a sensitive and vast field is significant from the moral, legal, and constitutional standpoints. This research examines the convoluted interaction of AI with the Indian criminal justice framework, weighing the advantages, the danger, and the gaps in the rules of its usage. The article starts discussing existing and future uses of AI in Indian policing, prosecution, and adjudication. It identifies projects like the "Crime and Criminal Tracking Network & Systems (CCTNS), the Inter-operable Criminal Justice System (ICJS)", and experiments currently underway using AI-based crime mapping. These advances have a potential in terms of improving efficiency, decluttering backlogs, and supporting investigation but also raise serious issues related to privacy, transparency, and fairness. The primal question of this research is the ethical and legal dilemma posed by AI in the framework of justice. Algorithmic bias, data protection failures, transparency of decision-making mechanisms ("black box" issue), and compromising human accountability are the primary concerns. The research enlists both Indian constitutional values and global legal norms and identifies the threats of reproducing and exacerbating already existing systemic inequities through AI mechanisms devoid of adequate monitoring and authentication. Based on a doctrinal and comparative examination, this paper assesses regulatory models and jurisprudence of other jurisdictions like the EU and the United States with a view to drawing lessons for India.

Keywords: *Artificial Intelligence, Criminal Justice System, Ethical Challenges, Algorithmic Bias, Legal Regulation*

INTRODUCTION

The night-time digital revolution of the world's societies has put "artificial intelligence (AI)" at the center of government and institutional change, criminal justice included. India, a country of monolithic demographic diversity and intricacy in the law, is no exception to this.For the purpose of enhancing efficiency, accountability, and accuracy in law enforcement and judicial decision-making processes, AI devices are being implemented in "the Indian criminal justice system" at an ever-increasing pace. From predictive policing and face recognition software to algorithmic risk assessment and AI-based legal research, deployments of machine intelligence are beginning to revolutionize the traditional crime control, investigation, and adjudication paradigm.

Although such technological advances promise repeating historical problems—like tardy justice, mounting case backlogs, and inefficient policing—issues of legality, constitutionality, and ethics are also posed at the same time. A criminal justice system resting on fundamental principles of fairness, due process, and human rights cannot afford blind adoption of tools with potential embedded algorithmic bias, secrecy, and data vulnerability. Artificial intelligence models based on defective data, for example, may transfer previous prejudices and deeply ingrained discrimination, especially against vulnerable groups. Furthermore, the "black-box" nature of the overwhelming majority of AI algorithms undermines the transparency and accountability required of judicial decision-making.

Application of AI in such a sensitive area has to, therefore, be rigorously examined under the optics of constitutional values and legal protections. The Indian Constitution with its promise of equality, liberty, and due process offers the normative template by which any technological incursion into criminal justice needs to be measured. Furthermore, the absence of an effective statutory or regulatory framework governing the use of AI in this area exposes a persuasive legal void that has to be filled.

This doctrinal research paper is a critical examination of the legal and ethical implications of AI in India's criminal justice system. It surveys existing AI deployments in Indian policing and judiciary, analyzes the potential risks of their deployment, and compares India's regulative approach with others like "the European Union and the United States". Through close reading of statutes, constitutional principles, court judgments, and global treaties, the paper attempts to propose a model of regulating AI through rights within the criminal justice system that balances technological progress with the demands of justice, fairness, and human dignity.

Research Questions

1. To what degree is artificial intelligence in policing and judicial decision-making compatible with India's constitutional ideals of due process, equality, and privacy?
2. What are the main ethical and legal concerns of AI technologies—algorithmic bias, opacity, and data protection—that are presented by AI technologies to the Indian criminal justice system?
3. How are current Indian legal structures governing or missing out on regulating the use of AI for criminal investigation, prosecution, and adjudication?
4. What can be learned from international regulatory frameworks “like the EU's AI Act and the U.S. algorithmic accountability efforts” in developing an AI governance regime that is rights-based?
5. How is a balance to be achieved between technological advancement and protection of core rights to make sure the fair and equitable use of AI in criminal justice proceedings in India?

RESEARCH OBJECTIVES

1. To study the existing and future uses of “artificial intelligence in India's criminal justice sector”, including policing, prosecution, and adjudication.
2. To explore and critically examine the ethical and legal issues arising out of the deployment of AI technologies, including algorithmic bias, non-accountability, data privacy, and procedural fairness.
3. To evaluate the sufficiency of current Indian constitutional provisions, legislative statutes, and judicial cases in regulating the application of AI in the criminal justice system.
4. To make a comparative examination of foreign legal regimes (especially in the EU and the US) on AI in criminal justice, and examine their applicability to the Indian context.
5. To put forth policy suggestions and a rights-oriented regulatory framework for the ethical, legal, and responsible application of AI in the criminal justice system in India.

Hypothesis

The implementation of artificial intelligence in India's criminal justice system, though promising improvements in efficiency, management of cases, and investigative precision, introduces serious ethical and legal issues that are presently insufficiently dealt with by governing laws and regulatory frameworks. It is believed that in the absence of a strong rights-based legal system built upon constitutional protections like due process, equality, and privacy, unregulated or ill-managed use of AI technologies can create systemic biases, loss of accountability, and infringement of fundamental rights. Hence, it is necessary to critically evaluate and amend the present legal system to ensure that technological innovation in the justice system doesn't happen at the expense of justice.

LITERATURE REVIEW

Virginia Eubanks, in her seminal book Automating Inequality[1], points to how algorithmic technologies used in criminal justice tend to replicate biases within the system and not erase them. Using examples from the United States, she shows how biased data and opaque decisional processes commonly discriminate against marginalized communities, especially with regard to predictive policing and risk assessment algorithms. According to Eubanks, the myth of algorithmic neutrality conceals structural discrimination and magnifies injustice. Her results are particularly pertinent to the Indian situation, with similar socio-economic inequalities and institutional biases prevalent, which would imply that AI adoption without transparency and accountability may reinforce current disparities.

“Cathy O'Neil's Weapons of Math Destruction”[2] offers a critical analysis of how algorithmic systems, especially those involved in policing, contribute to unaccountable decision-making. O'Neil coins the term "WMDs" (Weapons of Math Destruction) for describing algorithms that are opaque, unregulated, and destructive, especially in high-risk areas such as criminal justice. O'Neil's critique of risk-scoring algorithms applied to sentencing offers a cautionary model for India, where debates regarding AI-based judicial instruments are on the horizon. The book highlights the imperative need for legal infrastructure that guarantees algorithmic accountability, transparency, and the right to explanation.

In their research paper, Arora and Khanna (2022) discuss the continued application of AI in Indian law enforcement with an emphasis on platforms such as CCTNS and ICJS. They contend that although these technologies hold the promise of efficiency, they are being rolled out without sufficient legal protection or citizen engagement. The research concludes that data protection, consent, and oversight concerns are for the most part still unaddressed. Their study is important in identifying the technology-deployment vs. regulatory-readiness gap in India, calling for a rights-oriented approach to frame AI regulation in policing.

Bhandari (2021)[3] examines the constitutional aspects of AI deployment in India's criminal justice apparatus, especially from the perspective of fundamental rights. She examines how AI-driven surveillance and predictive policing intrinsically infringe upon privacy rights (as established in Puttaswamy v. Union of India), equality, and trial by fair procedures. The writer emphasizes the need to synchronize AI adoption with constitutional jurisprudence and proposes the creation of a legal framework that encompasses procedural protections, judicial review, and algorithmic transparency.

Browne and Millar (2020)[4] present a “comparative analysis of AI regulatory responses in the European Union, the United States, and Australia” in their policy brief. The brief describes how the EU's draft Artificial Intelligence Act seeks to categorize AI risks and impose obligations in the form of transparency, human intervention, and legal redress. The authors contend that India does not have such systematic regulation and warn against the adoption of technology in the absence of analogous legal protection. Their comparative perspectives are worthwhile in suggesting a model of regulation specifically crafted for India that promotes democratic values and basic rights.

RESEARCH METHODOLOGY

The ethical and legal ramifications of “artificial intelligence (AI) “in India's criminal justice system are critically examined in this study using a doctrinal legal methodology, which mostly relies on the examination of primary and secondary legal sources. It entails a thorough examination of the laws, court rulings, policy documents, and constitutional clauses that are pertinent to the application of AI in law enforcement, prosecution, and adjudication. Additionally, the study uses comparative legal analysis, using knowledge from global frameworks like the Artificial Intelligence Act of the European Union and US AI governance models.Academic literature, law review articles, government reports, and expert commentaries are analyzed to identify legal gaps, emerging concerns, and potential safeguards. The aim is to assess the compatibility of AI technologies with India’s constitutional values and propose a rights-based legal framework for their ethical and accountable use within the criminal justice system.

Scope and Limitation

Scope

This research focuses on examining the legal, ethical, and constitutional dimensions of “artificial intelligence (AI)” integration within the Indian criminal justice system. It studies the current and emerging uses of AI in policing, investigation, judicial decision-making, and case management, with particular emphasis on systems like the “Crime and Criminal Tracking Network & Systems (CCTNS) and the Inter-operable Criminal Justice System (ICJS)”. The research explores the implications of AI in light of Indian constitutional guarantees such as the right to equality, privacy, and due process. Additionally, the study includes a comparative analysis of regulatory frameworks and jurisprudence from the “European Union and the United States” to suggest appropriate regulatory and policy responses for India.

Limitation

This study is doctrinal in nature and therefore limited to the analysis of legal texts, judicial decisions, policy documents, and secondary literature. It does not involve empirical fieldwork, such as interviews with law enforcement officers or technologists, nor does it include technical assessments of specific AI algorithms or software. Further, while comparative perspectives are included, the research does not cover all jurisdictions globally, focusing instead on selected models with high relevance to the Indian context. Given the evolving nature of AI and its legal regulation, some findings may require reassessment as newer laws, technologies, or court decisions emerge.

AI In the Indian Criminal Justice System – Current Applications and Legal Framework

“artificial intelligence (AI) “is being increasingly embraced in the Indian criminal justice system to overcome systemic inefficiencies, deal with massive amounts of criminal data, and enhance investigation capabilities. In light of the government's thrust toward Digital India, several AI-based initiatives have been launched across law enforcement, prosecution, and judicial spheres. While these technologies promise more efficiency and greater surveillance power, the use of these also raises important legal and ethical considerations, especially in terms of the rights of the individual under the Indian Constitution. This chapter discusses the pragmatic applications of AI in India's criminal justice system and analyzes the legal and constitutional issues surrounding their use.

CCTNS and ICJS: Digitizing Crime Data for Smart Governance

The "Crime and Criminal Tracking Network and Systems (CCTNS)" is one of the flagship projects of the National e-Governance Plan (NeGP) initiated by the Ministry of Home Affairs to develop a national integrated system for efficient policing by computerized crime and criminal information. CCTNS enables online registration of FIR, tracing of offenders, and inter-state data sharing.It lays the groundwork for AI-based data analysis to identify patterns and make predictions for crime prevention (Mehta & Sharma, 2021).

Apart from CCTNS, there is the Inter-operable Criminal Justice System (ICJS) to connect the databases of five significant criminal justice institutions: police, courts, prisons, forensics, and prosecution. ICJS facilitates real-time data exchange among such stakeholders and facilitates AI-enabled automation in bail determination, forensic report generation, and case tracking (Ministry of Home Affairs, 2022). Such platformed systems serve as the basis for AI implementation in criminal justice processes, yet their use creates necessary privacy, consent, and security issues regarding data.

Predictive Policing and Facial Recognition Technology

One of the more controversial applications of AI in India is "predictive policing", where machine learning algorithms analyze historical crime data to forecast potential criminal activity or locations of concern. States like Telangana and Uttar Pradesh have experimented with predictive models and heat maps to optimize police patrolling. However, such systems often rely on biased or incomplete data, risking the reinforcement of structural inequalities in policing (Jain, 2021)[5].

Similarly, Facial Recognition Technology (FRT) is being deployed by police departments in Delhi, Hyderabad, and Chennai for surveillance, crowd control, and identification of suspects. While AI-based FRT can accelerate identification processes, its use in public spaces without clear legal authorization has drawn criticism from civil rights groups. The Internet Freedom Foundation (2020)[6] noted that FRT lacks a statutory basis in India, and its operation may violate the right to privacy upheld in "Justice K.S. Puttaswamy v. Union of India (2017)"[7]. The absence of transparency, consent, and oversight mechanisms further complicates its legality.

Legal and Constitutional Framework: A Vacuum in Regulation

Despite the increasing adoption of AI in criminal justice, India currently lacks a dedicated legal framework to regulate its use. The deployment of AI in sensitive areas such as surveillance, risk assessment, and judicial decision-making occurs in a largely regulatory vacuum, raising concerns about violations of "Articles 14 (Right to Equality), 19 (Freedom of Expression), and 21 (Right to Life and Personal Liberty) of the Constitution of India".

The Supreme Court's landmark judgment in Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right, imposing a proportionality requirement on any state action involving data collection and surveillance. However, most AI tools used in policing and adjudication operate without meeting this threshold of legality, necessity, and proportionality. Further, there is no AI-specific data protection law in place, as the Digital Personal Data Protection Act, 2023[8] has only recently been enacted and does not comprehensively address algorithmic accountability or bias in automated decision-making.

In this legal vacuum, the use of AI technologies in criminal justice processes risks undermining procedural fairness, reinforcing existing biases, and compromising the foundational principles of due process and human dignity enshrined in the Constitution.

Ethical And Legal Challenges – Algorithmic Bias, Accountability, And Transparency

As AI technologies gain deeper penetrations within the Indian criminal justice system, apprehensions regarding their legal and ethical consequences have risen to the forefront. On one hand, AI has the potential to provide efficiency and objectivity. On the other hand, it also poses serious risks which could jeopardize the rule of law and basic rights. Among these challenges are algorithmic bias, lack of transparency in automated decision-making (commonly referred to as the "black box" problem), and the erosion of accountability in legal processes. These issues pose a direct threat to constitutional protections such as equality before the law, procedural fairness, and the right to privacy. This chapter delves into these challenges in great detail, focusing on how their unaddressed existence can aggravate systemic imbalances and erode trust in institutions of justice.

Algorithmic Bias and Discriminatory Outcomes

The most long-standing issue plaguing AI is algorithmic bias, where AI systems decide things in disproportionate ways against certain groups on the basis of their race, gender, caste, religion, or socio-economic status. These biases, in turn, largely originate in the training data against which AI models have been trained. If there is evidence that historical crime data represents policing prejudice or biased policing, AI technologies developed using such data are likely to replicate and even enhance these discriminations (Eubanks, 2018)[9].

In the Indian context, where caste and communal profiling have traditionally shaped policing, algorithmic decision-making could end up perpetuating such biases inadvertently. For instance, predictive policing techniques could end up targeting marginalized areas disproportionately because of a greater recorded rate of crimes—not necessarily the higher actual rate—resulting in over-policing of vulnerable communities (Bhandari, 2021)[10]. In the absence of mechanisms for detecting bias and correction, AI tools could end up contravening Article 14 of the Constitution, which ensures equality before the law.

Transparency and the 'Black Box' Issue

Most AI systems, particularly those that are based on sophisticated machine learning algorithms, are "black boxes"—their inner workings are either incomprehensible to humans or concealed for proprietary reasons. The absence of explainability renders it challenging for persons impacted by AI choices to comprehend, query, or dispute them (Wachter et al., 2017)[11].

In the criminal justice process, this obscurity can result in a serious breach of due process. For example, if an AI application plays a role in bail, sentencing, or profiling judgments without adequate explanation, it could violate Article 21, which assures the right to life and personal liberty, including fair trial and procedural safeguards. The lack of "right to explanation" provisions or legally required transparency standards in Indian legislation enhances this problem.

The issue is further exacerbated by judicial or legislative oversight being absent regarding algorithmic decision-making. In contrast to conventional judicial rationale, which has to be documented and is subject to appeal, AI-driven choices are difficult to audit. This adversely affects transparency as well as the public's confidence in the justice system.

Accountability, Human Control, and Ethical Issues

Another core issue is accountability dilution when AI is utilized in the delivery of justice. Decisions made by AI tend to be experienced as objective or impartial, which can give rise to blind faith in algorithmic recommendations by police officers or judges. Upon mistake occurrence—e.g., incorrect matches in face recognition or biased risk scores—no one tends to attribute responsibility clearly, complicating redress and remedy through the law (Rahwan et al., 2019)[12].

The human oversight principle is critical in criminal justice, where a decision can determine the liberty or dignity of an individual. Transferring such important decisions to opaque, non-human agents with inadequate checks and balances may result in breaches of natural justice and constitutional protections. Furthermore, moral principles such as consent, proportionality, and necessity are often disregarded when applying AI technologies at scale within public systems.

Legally speaking, the lack of statutory protection or binding ethical standards creates a broad regulatory vacuum. Although some countries have implemented AI charters or ethics commissions, India does not yet have a full-fledged framework that requires human-in-the-loop decision-making or pre-deployment impact assessments for AI systems used in the criminal justice system.

Legal And Ethical Challenges of Ai in Criminal Justice - An Indian Perspective

As India grapples with the legal and ethical challenges of deploying “artificial intelligence (AI) “in its criminal justice system, comparative insights from jurisdictions that have taken proactive steps in AI governance can offer valuable lessons. The European Union (EU) has pioneered a risk-based regulatory framework through its proposed Artificial Intelligence Act, aiming to balance innovation with fundamental rights protection. In the United States, a patchwork of federal guidelines and state-level algorithmic accountability laws underscores a more decentralized approach emphasizing transparency and civil rights. Other nations—such as the United Kingdom, Canada, and Australia—have developed ethics boards, impact assessment protocols, and sectorspecific regulations for AI applications. This chapter critically examines these models, evaluating their relevance and adaptability to India's constitutional and institutional context.

Algorithmic Bias and Discriminatory Outcomes

One of the most worrying issues with the use of AI in India's criminal justice system is algorithmic bias. AI systems usually learn from past data which itself might be reflective of deeply ingrained societal biases—especially on the lines of caste, religion, and economic status. This could result in discriminatory policing or judicial decisions that adversely impact marginalized populations. For example, predictive policing software, when trained on discriminatory arrest records, can disproportionately target Dalit or Muslim areas, resulting in over-policing and wrongful profiling (Kumar & Singh, 2022). This goes against Article 14 of the Indian Constitution, which promises equality before law. Comparable experiences in the US, where risk-assessment technology such as COMPAS was found to have racial biases, should be a cautionary note (Angwin et al., 2016)[13]. In India, the lack of anti-bias procedures or routine audits for AI-powered legal tools underscores the issue even further.

Lack of Transparency and Accountability

A second essential issue is the nontransparent nature of AI decision-making, colloquially known as the "black box" issue. Sophisticated machine learning algorithms—deep learning models, in particular—make decisions that are difficult to interpret, even for their creators. This poses a direct threat to procedural due process and the right to a fair trial under Article 21 of the Constitution. Defendants should be capable of comprehending and contesting judgments made against them, but AI tools are typically explainable to a limited extent. In K.S. Puttaswamy v. Union of India (2017), the Supreme Court specified that in any system impacting fundamental rights, transparency is an absolute requirement. Without explain ability, AI use in criminal justice can result in outcomes that neither the judiciary nor the accused can comprehend the rationale behind, destroying judicial institutions' trust with the public (Chander, 2020)[14].

In addition, accountability issues arise whenever there are mistakes caused by AI-made decisions. If an individual is unjustly denied bail or found guilty due to defective AI suggestions, it is not obvious who should be held accountable—the coder, the agency deploying it, or the government? The legal maxim ubi jus ibi remedium (where there is a right, there must be a remedy) is undermined when no one can be held accountable. This dilution of responsibility and agency in human beings is not consistent with established jurisprudence on state responsibility (Law Commission of India, 2018)[15].

Privacy Issues and Misuse of Data

Operation of AI in criminal justice is largely dependent on the processing of huge volumes of personal data, biometric data, and behavioral data. In India, where police forces are increasingly using surveillance technologies such as facial recognition and predictive policing, data privacy and consent issues are of utmost concern. While the Digital Personal Data Protection Act, 2023 is trying to establish a legal framework, its enforcement structures are weak and disjointed. Unregulated access to personal information by AI systems not only infringes on informational privacy but also creates avenues for illegal surveillance and profiling (Sharma & Bansal, 2023)[16].

In addition, the AI tools deployed in India usually function with no guidelines on user consent, data retention, or minimization. This contravenes the guidelines established by the Puttaswamy judgment, which considered privacy a basic right and set out the "necessity-proportionality-legality" triad for any state incursion (Puttaswamy, 2017)[17]. The lack of independent enforcement bodies or efficacious data protection authorities has left the right to privacy highly vulnerable.

Legislative and Institutional Safeguards

Even with the swift incorporation of AI tools in Indian judicial and law enforcement agencies, there is a disturbing lack of legislations governing their usage. Efforts by institutions such as NITI Aayog and the Bureau of Police Research and Development (BPR&D) have brought forth the potential of AI to be used in governance but without legal instruments that can be enforced (NITI Aayog, 2020)[18]. This regulatory lacuna results in the arbitrary or experimental application of AI systems without ethical assessment, legal oversight, or public accountability.

India needs immediate statutory backing for requiring ethics auditing, algorithmic testing, human-in-the-loop systems, and rights-based protections for AI application in criminal justice. The judiciary needs to adapt as well to critically examine

AI-based evidence and decisions, drawing clear precedents on admissibility, transparency, and due process. Without this, the potential of AI as a revolutionary legal instrument may become counterproductive, leading to institutionalized injustice and a degradation of constitutional principles.

CONCLUSION AND SUGGESTIONS

CONCLUSION

“artificial intelligence (AI) “integration into India's criminal justice system is a double-edged sword—while it has the ability to ease investigations, facilitate judicial efficiency, and declog courts, it also threatens to exacerbate current biases and overstep into fundamental rights. From facial recognition software to predictive policing algorithms, AI in India remains unregulated, with fundamental ethical and legal concerns still unanswered. There is no uniform and enforceable structure in the existing law and policy scenario that can guarantee that AI deployment follows constitutional principles of equality before law, due process, and privacy.

The study emphasizes the fact that the lack of transparency of algorithms, inadequate data protection mechanisms, and absence of public scrutiny procedures may cause irreparable erosion of faith in law enforcement and the judiciary among the public. Comparative lessons from the UK and US show that nations are shifting towards a more prudent, principle-driven adoption of AI, with right guidelines and regulation measures. India has to go beyond pilot projects and scattered digital initiatives to an overarching, ethical, and rights-oriented governance model for AI.

Recommendations

Pass a Comprehensive AI Governance Law for Criminal Justice:

There is a pressing need for targeted legislation that regulates the application of AI in criminal inquiries, surveillance, predictive policing, and judicial proceedings. This legislation should set the standards of fairness, non-discrimination, human oversight, and accountability.

Institutionalize Algorithmic Accountability Mechanisms:

All AI deployed in the criminal justice system needs to be subjected to independent audits, ethical impact assessments, and bias detection reviews. Oversight must be institutionalized through the establishment of regulatory bodies or ombudsman offices with powers of law enforcement to ensure ethical deployment of AI.

Enhance Human Oversight in All AI-Directed Systems

AI must never be used independently in decision-making positions. Human players—judges, police officers, or investigators—must be enabled and equipped to critically assess AI reports. Public servants within the justice system need mandatory AI ethics training to be implemented.

Fill Data Protection Gaps through Enhanced Enforcement

Despite the enactment of a national data protection law, there is still no effective enforcement, grievance redressal mechanism, and real-time regulatory oversight. Particularly for predictive policing and facial recognition, rigorous data minimization and proportionality principles need to be maintained.

Establish Judicial Benchmarks for AI Evidence and Fair Trials:

Courts will need to develop guidelines for admitting AI-provided evidence while protecting the rights of the accused. This involves ensuring defense attorneys receive access to underlying algorithms, providing expert testimony to contest defective models, and requiring court orders referring to AI tools to be open.

Engage Marginalized Communities in Policy-Making:

Policy design must be inclusive, with the voices of the communities disproportionately impacted by AI surveillance—minors, women, and economically disadvantaged groups—heard through legislative and administrative consultations.

Work Internationally to Establish Standards and Best Practices:

India must actively engage in global platforms such as the OECD, UNESCO, and the Global Partnership on AI to influence and absorb international norms on ethical AI. This cooperation can assist India in ensuring its domestic framework aligns with changing international standards.

REFRENCES

1. Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
2. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Publishing Group.
3. Arora, S., & Khanna, R. (2022). AI and law enforcement in India: Opportunities and regulatory challenges. Indian Journal of Law and Technology, 18(1), 45–68.
4. Bhandari, V. (2021). Artificial intelligence and criminal justice in India: Constitutional dilemmas and democratic deficits. NUJS Law Review, 14(2), 129–155.
5. Browne, R., & Millar, J. (2020). Regulating AI in criminal justice: Comparative models and lessons for India. Centre for Internet and Society Policy Brief, 12(3), 1–15.
6. Mehta, A., & Sharma, D. (2021). AI and digital transformation in Indian law enforcement: Challenges and future directions. Journal of Indian Law and Technology, 17(1), 45–62.
7. Ministry of Home Affairs. (2022). Annual Report 2021–22. Government of India. Retrieved from https://www.mha.gov.in
8. Jain, S. (2021). Predictive policing in India: Legal lacunae and social consequences. National Law School of India Review, 33(2), 120–138.
9. Internet Freedom Foundation. (2020). Project Panoptic: Facial Recognition Technology in India. Retrieved from https://internetfreedom.in
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
12. Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
13. Bhandari, V. (2021). Artificial intelligence and criminal justice in India: Constitutional dilemmas and democratic deficits. NUJS Law Review, 14(2), 129–155.
14. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005.
    The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
15. Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.
16. Bhandari, V. (2021). Artificial intelligence and criminal justice in India: Constitutional dilemmas and democratic deficits. NUJS Law Review, 14(2), 129–155.
17. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
18. Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J. F., Breazeal, C., ... & Lazer, D. (2019). Machine behaviour. Nature, 568(7753), 477–486. https://doi.org/10.1038/s41586-019-1138-y
19. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
20. Chander, A. (2020). The racist algorithm? Michigan Law Review, 119(4), 1023–1048.
21. Law Commission of India. (2018). Report No. 277: Wrongful Prosecution (Miscarriage of Justice): Legal Remedies. Government of India.
    Sharma, D., & Bansal, M. (2023). Privacy and AI: Evaluating India's data protection framework. Indian Journal of Law and Technology, 19(1), 77–94.
22. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
23. NITI Aayog. (2020). Responsible AI for All: National Strategy for Artificial Intelligence. https://niti.gov.in