INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

REGULATING ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE: IDENTIFYING LEGISLATIVE GAPS IN INDIA

AUTHORED BY - HAMSAVENI G

Abstract

From digital forensics, facial recognition, and predictive policing to AI-driven judicial decision-making, artificial intelligence (AI) is rapidly changing criminal justice systems worldwide. India still relies on broad and disjointed provisions under existing statutes like the Information Technology Act, 2000, Code of Criminal Procedure, 1973, Indian Evidence Act, 1872, and the recently enacted Digital Personal Data Protection Act, 2023 — which governs data processing but does not specifically regulate AI deployment in criminal justice. In contrast, jurisdictions such as the European Union, United Kingdom, and United States are developing more structured approaches toward the governance of AI in criminal justice through instruments like the EU Artificial Intelligence Act, constitutional safeguards under the Fourth and Fourteenth Amendments in the US, and judicial scrutiny seen in decisions such as Bridges v. South Wales Police in the UK. This doctrinal and comparative research paper assesses these foreign regulatory frameworks while critically examining the legal and procedural shortcomings in India's current criminal justice system. The study contends that India lacks sufficient legislative clarity and robust protections to address issues such as algorithmic bias, privacy infringement, accountability, due process rights, and the admissibility of AI-generated evidence. In particular, the paper highlights urgent reform needs in criminal procedure, evidentiary standards, and liabilities in AI-assisted criminal processes by contrasting India's approach with that of the EU, UK, and USA. The paper concludes with legislative and policy recommendations for India, drawing on comparative foreign models while remaining sensitive to the country's socio-legal context.

Keywords: Artificial Intelligence, Criminal Justice System, Legislative Gaps, India, Comparative Study, EU AI Act, United Kingdom, United States, Algorithmic Bias, Evidence Law.

ISSN: 2582-6433

1. Introduction

The accelerated development of Artificial Intelligence (AI) has started to radically transform criminal justice systems worldwide. It all started as the mere digitisation of investigative tools, but now it has evolved into advanced technologies like predictive police software, autonomous surveillance technology, digital forensic algorithms, facial recognition software and AI-based judicial decision-making platforms. Such technologies hold the promise of greater efficiency, speed and precision but raise serious questions in their wake about constitutionality, legality, and procedural justice. In the Indian context, AI integration into criminal justice has been undertaken so far without the support of a well-defined statutory framework. Rather, varied and disconnected provisions scattered in the Information Technology Act, 2000; the Code of Criminal Procedure, 1973; the Indian Evidence Act, 1872; and the newly passed Digital Personal Data Protection Act, 2023 seem to indirectly regulate some aspects of AI adoption. These laws were developed during a time when AI technologies were either nonexistent or much less ubiquitous; thus, they were not created to adapt to the new challenges algorithmic decision-making, autonomous tools, and evidentiary systems based on machine learning present. Consequently, there is a huge legal uncertainty in India regarding matters such as admissibility of evidence generated by AI, procedural due process standards, transparency, accountability of algorithms, and the safeguarding of fundamental rights like privacy, equality, and liberty.

In contrast to India's dispersed legal stance, some foreign jurisdictions have embraced or are trending towards more systematic strategies for controlling AI in criminal justice. The European Union has pioneered with its draft Artificial Intelligence Act, which aims to regulate AI systems on a risk-based framework and imposes particular safeguards on "high-risk" uses of AI in law enforcement, such as human oversight, accuracy, traceability, and banning particular practices such as real-time facial analysis in public areas except in narrowly specified situations. In the United Kingdom, even though there isn't a single AI-specific Act, the application of AI technologies to policing and criminal justice has already faced judicial review in leading cases such as Bridges v. South Wales Police, where the Court of Appeal underlined the significance of legality, necessity, proportionality, and strong policy guidance prior to employing AI-facilitated surveillance. At the same time, the United States has also seen widespread use of predictive algorithms and AI-driven risk assessment software (e.g., the COMPAS system) at pre-trial and sentencing phases, resulting in an increasing number of constitutional challenges under the Fourth and Fourteenth Amendments — for unlawful search

ISSN: 2582-6433

and seizure, and equal protection of law. These legal and regulatory advances elsewhere offer important lessons to India, as they identify tangible solutions to the risks of algorithmic bias, explainability gaps, disproportional interference with rights, and the necessity of robust oversight and legal accountability.

This essay contends that India needs a clear and forward-looking legal regime to govern the application of AI in its criminal justice system immediately. Although policy-level discourse on AI ethics and national strategies has commenced, statutory changes in foundational criminal justice legislation are still lacking. The current evidentiary framework under the Indian Evidence Act, 1872 — specifically sections 65A and 65B relating to electronic evidence — has yet to be sufficiently tested by courts on matters relating to admissibility, reliability, and chain of custody of AI-produced or AI-processed evidence. Likewise, the Code of Criminal Procedure, 1973 also gives only general procedural protection during investigation and trial, without considering algorithmic decision-making or machine-augmented policing. The Digital Personal Data Protection Act, 2023 is primarily concerned with the processing of personal data by data fiduciaries but fails to address in terms the criminal justice intersection where the State itself becomes both the processor and user of extremely sensitive biometric and behavioural data. This omission has very serious implications for individual freedom and due process rights under Articles 14, 19, 20, 21, and 22 of the Indian Constitution. Without evident bounds of legality, transparency or accountability for AI technologies, the potential for unbridled State surveillance, robotized injustice and discriminatory decision-making grows ever more real.

By a doctrinal and comparative analysis, this paper critically assesses the current statutory framework in India and determines the most important areas where reform is called for in a bid to safely host and regulate AI technologies in criminal justice. In comparison with the more advanced and progressive regimes of the European Union, United Kingdom, and United States, the Indian system has no specific legal approach to addressing AI-specific issues like algorithmic obscurity, automatic decision-making, proportionality of State intervention, and accountability in events of harm or false convictions. Therefore, it becomes necessary to examine whether and how the regulatory precedents of these other jurisdictions can be used to inform India's statutory reform process. The article proposes that India has to use the layered approach — that involves internal amendments in present criminal procedure and evidence legislation to sort out matters of admissibility, fairness, accountability and responsibility, while, at the same time, beginning processes towards enacting a full-fledged AI legislating law

ISSN: 2582-6433

specific to criminal justice. Such a law has to have fundamental principles of transparency, explainability, accuracy, accountability, human-in-the-loop oversight, and care for constitutional protections. Through timely and strong legal reform alone can India make use of the advantages of AI in criminal justice without threatening fair trial rights and public confidence in the rule of law.

2. Understanding Artificial Intelligence in Criminal Justice

2.1 What is Artificial Intelligence?

Artificial Intelligence (AI) describes the ability of computer systems to conduct tasks that would normally need human intelligence, like reasoning, learning, decision-making and perception. AI systems vary from rule-based programmes, that adhere to pre-stipulated instructions (symbolic AI), to sophisticated machine-learning and deep-learning models that learn patterns from data and modify their behaviour over time. With regards to criminal justice, AI technologies can process enormous amounts of structured and unstructured data, discovering patterns that human eyes might miss. Examples of such technologies are supervised learning algorithms, unsupervised algorithms, natural language processing systems, autonomous visual monitoring and predictive analytics engines. With increasingly autonomous and black-boxed AI systems, they basically disrupt classic assumptions around human control, judgment, and legal responsibility in law-enforcement procedures.

2.2 Applications of AI in Criminal Justice

AI is now embedded throughout the criminal justice process. In the investigation phase, predictive policing platforms—PredPol, HunchLab, and others—sift historical crime statistics to project where criminal activity is expected, directing patrol resources accordingly. Facial recognition technologies compare live CCTV feeds and biometric databases to spotlight possible suspects. Meanwhile, digital forensics solutions deploy machine learning to recover apparently deleted files, mine encrypted drives, and accelerate cybercrime examinations. AI-enhanced surveillance systems choreograph several video streams, flagging movement patterns deemed anomalous. During prosecution and trial, correctional risk models—most notably the COMPAS tool in the United States—estimate offenders' likelihood of recidivism, influencing bail, sentencing, and parole deliberations. Other courts are piloting applications that summarise lengthy case files, transcribe witness accounts, or assist magistrates in drafting judicial opinions. In India adoption is still in the early stage, yet pilots are visible—from the Delhi Police leveraging facial recognition for crowds, to predictive crime analysis in Maharashtra, to

ISSN: 2582-6433

digital forensics laboratories that employ machine learning for cyber-evidence processing.

2.3 Benefits and Challenges

By improving policing and adjudication's effectiveness, speed, and accuracy, artificial intelligence (AI) holds the potential to completely transform criminal justice. It enables law enforcement organizations to process complex information that might be impractical for manual review, save resources, and make data-informed decisions. While AI-assisted risk tools may help make decisions more objectively, predictive systems have the potential to prevent crime by facilitating proactive policing. But these advantages come with a number of significant procedural, ethical, and legal issues. Algorithm opacity, sometimes referred to as the "black box" problem, undermines accountability and transparency by making it challenging to determine how decisions are made. Concerns regarding the constitutional guarantees of equality and non-arbitrariness are raised by the way that the use of biased historical data can reinforce and embed discrimination against marginalized communities.

Furthermore, the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India may be violated by AI-enabled surveillance and facial recognition systems that restrict free movement and behavior. Regarding the admissibility, dependability, and probative value of AI-generated evidence under the Indian Evidence Act, 1872, courts may encounter difficulties from an evidentiary standpoint. Additionally, it is still unclear who is responsible when an AI tool results in an erroneous arrest or conviction. These issues highlight the need for a strong regulatory framework to be established before AI becomes ingrained in India's criminal justice system, a task that this paper contends demands immediate legislative attention.

3. Indian Legal Framework Governing AI in Criminal Justice

3.1 Statutory Framework in India

As of right now, India has no specific legislation governing the creation or application of AI in the criminal justice system. Rather, different facets of AI use are indirectly governed by a disjointed set of general-purpose laws. The foundation of India's digital legal system is the Information Technology Act, 2000, which was first passed to promote electronic commerce and punish cybercrimes. The Act does not outline standards for AI-enabled investigative tools or envision algorithmic surveillance, even though provisions like Sections 43 and 66 deal with unauthorized access to computer systems and data theft, and Section 72 penalizes unauthorized disclosure of personal information.

ISSN: 2582-6433

Although investigation, arrest, evidence gathering, trial, and sentencing are all governed by the 1973 Code of Criminal Procedure (CrPC), its procedural safeguards were designed with human actors and traditional investigative techniques in mind. The chain of custody for automatically generated digital evidence and machine decision-making are not taken into consideration in the sections pertaining to search, seizure, and confession. Similarly, Sections 65A and 65B of the Indian Evidence Act, 1872, which were added in 2000 to allow for electronic evidence, only address the admissibility and authenticity of digital content; they do not specifically regulate evidence produced or processed by self-learning AI systems, nor do they address algorithmic explainability or bias.

India's first comprehensive privacy law, the Digital Personal Data Protection Act, 2023 (DPDP Act), governs how "data fiduciaries" process personal data. Section 17(2) of the DPDP Act exempts state processing in matters of national security, law enforcement, and offense prevention, even though it is pertinent to AI-driven criminal justice tools that gather and process biometric, behavioral, or location data. As a result, it has little effect on police departments using AI surveillance tools to prevent the invasive gathering of personal information.

3.2 Judicial Interpretation & Case Law

Notwithstanding the lack of criminal laws specifically addressing AI, Indian courts have produced significant constitutional jurisprudence that is pertinent to the use of AI. The Supreme Court ruled in People's Union for Civil Liberties (PUCL) v. Union of India (1997) that telephone tapping is against Article 21's right to privacy unless it is accompanied by procedural protections like prior authorization and periodic review. A nine-judge bench more recently upheld the fundamental right to privacy in Justice K.S. Puttaswamy v. Union of India (2017), emphasizing that any state intrusion must pass the triple test of legality, necessity, and proportionality. These rulings set the stage for further judicial examination of AI-based monitoring technologies employed by Indian law enforcement, such as facial recognition and predictive policing.

The admissibility, bias, and fairness of AI-generated insights in criminal trials have not yet been directly addressed by Indian courts, though. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Supreme Court issued guidelines regarding the admissibility of electronic records; however, these guidelines primarily apply to digital documents rather

ISSN: 2582-6433

than autonomous algorithmic outputs. Digital forensic reports generated by AI-powered tools are sometimes admitted by trial courts, but there is no thorough judicial investigation into their explainability or dependability. Instead of particular statutory or evidentiary standards controlling the use of AI in criminal proceedings, the judiciary has up to this point relied on general constitutional principles.

3.3 Identified Gaps and Challenges

The existing Indian legal system has a number of serious flaws. First, it is impossible to impose risk-based obligations or restrictions akin to the EU model because there is no statutory definition or classification of AI systems in criminal justice. Second, there is legal ambiguity regarding liability, oversight, and accountability in cases of wrongful arrest, conviction, or discriminatory outcomes made possible by AI because the current procedural laws do not recognize algorithmic decision-making. Third, the DPDP Act severely restricts law enforcement's privacy protections, allowing them to use intrusive AI-powered surveillance with little to no external scrutiny or transparency requirements. Fourth, there is still debate regarding the admissibility and probative value of AI-generated evidence under the Evidence Act, particularly when the training data or underlying algorithm are opaque or proprietary. This puts the accused's right to a fair trial and their capacity to successfully refute the evidence against them in jeopardy.

Although policy documents recognize these difficulties, they have not resulted in legally enforceable protections. While acknowledging smart policing and public safety as key application areas under its "AI for Public Safety" pillar, the NITI Aayog's 2018 "National Strategy for Artificial Intelligence" specifically cautioned that ethical frameworks and legal oversight would be necessary to prevent abuse. The dangers of widespread surveillance, profiling, and opaque algorithmic decision-making in state operations were also emphasized in the B.N. Srikrishna Committee Report on Data Protection (2018), which served as the basis for the DPDP Act. It suggested that transparency, proportionality, and purpose limitation be followed, especially when law enforcement uses AI tools. However, these recommendations have mostly remained aspirational rather than legally binding, which has led to a growing discrepancy between the criminal justice system in India and the actual application of the law.

India runs the danger of integrating AI-based systems into its judicial and law enforcement systems in a way that compromises procedural justice and constitutional rights in the absence

ISSN: 2582-6433

of focused legislative reform. To map out India's future, a comparative analysis of the more structured regulatory approaches used in the US, UK, and EU becomes crucial.

4. Comparative Foreign Approaches

4.1 European Union

With a strong and progressive legal framework, the European Union has become a global leader in the effort to regulate artificial intelligence. The draft Artificial Intelligence Act (AIA), the first comprehensive attempt by any jurisdiction to directly legislate the development, deployment, and oversight of AI systems, is at the heart of this endeavor. Using a risk-based approach, the AIA divides AI applications into four categories: low, high, limited, and unacceptable risk. Social scoring systems and some types of real-time biometric surveillance in public areas are examples of AI applications that are strictly forbidden if they are judged to present an intolerable risk. The designation of AI systems used in the judiciary and law enforcement as "high-risk," which necessitates that they adhere to strict legal requirements prior to deployment, is particularly pertinent to criminal justice.

The AIA mandates that "high-risk" AI systems used for biometric identification, facial recognition, predictive policing, crime analytics, and judicial decision-support meet enforceable standards for cybersecurity, accuracy, robustness, and human oversight. In order to maintain accountability, providers must maintain thorough technical documentation, carry out conformance assessments, and guarantee that human operators continue to be "meaningfully in control." A new European Artificial Intelligence Board will coordinate cross-border regulatory coherence, and national supervisory authorities have been given the authority to keep an eye on compliance. Through the principles of lawfulness, purpose limitation, data minimization, and transparency, the Act also incorporates protections from other legal instruments, such as the General Data Protection Regulation (GDPR), thereby safeguarding individuals' privacy and data rights.

Alongside this, police authorities processing personal data in criminal investigations are subject to obligations under the Law Enforcement Directive (EU) 2016/680, which stipulates that intrusive technologies, like biometric-based AI, must be strictly necessary and proportionate to their goals, with improved safeguards for sensitive data. Furthermore, AI governance is governed by the EU Charter of Fundamental Rights, which mandates that any interference with privacy, liberty, or equality must be justified through a rigorous proportionality review. The

ISSN: 2582-6433

EU has specifically considered moratoriums or stringent restrictions on police use of real-time facial recognition, recognizing its high potential for rights violations, in contrast to India, where the use of facial recognition tools has continued without legislative scrutiny.

Legality, transparency, explainability, human oversight, and accountability are therefore ingrained as non-negotiable requirements for AI in criminal justice, making the EU's AI governance regime preventive and principle-driven. Even though the AIA has not yet been fully operationalized, it already stands in stark contrast to India's approach, which does not yet have a statutory definition of AI, a risk classification system, or required safeguards for use by law enforcement. The EU model serves as a workable model for making sure that procedural guarantees and fundamental rights are not sacrificed in order to achieve AI's efficiency gains. This structured framework—in particular, the concepts of "high-risk" classification, prior conformance assessments, mandatory documentation, and a dedicated supervisory authority to oversee AI applications in criminal justice—could greatly influence India's future regulatory efforts.

4.2 United Kingdom

In order to regulate the use of AI in criminal justice, the UK currently lacks a single comprehensive statute on the subject and instead depends on sectoral regulation, judicial review, and executive policy guidance. Automated facial recognition (AFR), predictive analytics, and risk assessment tools are just a few of the AI-driven technologies that UK law enforcement agencies use, especially when conducting surveillance and policing operations. Important common-law principles on proportionality, necessity, and accountability have developed as a result of court tests of the legitimacy and application of these tools. The landmark case is Bridges v. South Wales Police, [2020] EWCA Civ 1058, in which the Court of Appeal determined that the appellant's Article 8 right to privacy under the European Convention on Human Rights was violated by the police's use of live automated facial recognition and that there was insufficient legal framework, clear policies, and safeguards to be deemed "in accordance with the law." The Court emphasized that in order to prevent arbitrary use, police deployment of AI surveillance tools necessitates prior authorization, clear usage guidelines, and publicly available policies. Similar to this, the High Court recognized the invasive nature of AFR in R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police, [2019] EWHC 2341 (Admin), emphasizing that its legality depends on its deployment being carefully considered and its interference with fundamental rights being

ISSN: 2582-6433

proportionate.

The need for responsible innovation is emphasized in the UK Government's "National AI Strategy," and the Department for Science, Innovation, and Technology's White Paper: A Pro-Innovation Approach to AI Regulation (2023) outlines five overarching principles for AI governance: contestability, safety, transparency, fairness, and accountability. Instead of establishing a new AI regulator, these principles are enforced by already-existing ones. As a result, organizations such as the Information Commissioner's Office (ICO) are in charge of monitoring AI use related to processing personal data under the UK General Data Protection Regulation (UK-GDPR). AI surveillance systems must be proven to be required, proportionate to policing objectives, subject to impact assessments, and supported by robust data governance procedures, according to the ICO's guidance, "The Use of Live Facial Recognition Technology by Law Enforcement" (2021).

In contrast to the EU's legislative model, the UK uses a "soft law" regulatory approach, which depends less on primary legislation and more on judicial oversight and data protection regulators. Before AI tools can be used in policing, this strategy still imposes strict requirements for legality (a clearly defined legal basis), proportionality, and transparency. A de facto regulatory barrier over AI in criminal justice is created by the emphasis on public consultation, documented operational policies, and oversight, as well as the courts' readiness to declare "illegal" deployments. For India, the UK model shows how, even in the absence of specific AI legislation, a common-law system akin to its own can use administrative policy, judicial review, and pre-existing data protection frameworks to impose significant procedural discipline on AI use. It emphasizes the need for impact analyses, open operating procedures, and the potential for individual legal challenges to AI-assisted criminal justice actions—elements that are absent from the current Indian strategy.

4.3 United States

Artificial intelligence has quickly spread throughout policing, prosecution, and sentencing in the US criminal justice system. Nevertheless, the US lacks a comprehensive federal law governing AI, in contrast to the EU. Rather, a mix of case law, non-binding agency guidelines, and constitutional protections, along with a small amount of state-level legislation, regulate the use of AI in criminal justice. As a result, the regulatory environment in the United States provides an illustration of a bottom-up, jurisprudence-driven strategy, in which statutory

ISSN: 2582-6433

oversight is largely superseded by judicial oversight.

The Fourth Amendment, which forbids unjustified searches and seizures, and the Fourteenth Amendment, which ensures due process and equal protection, provide the main legal restrictions on the application of AI in criminal justice. Because they allow for invasive, warrantless tracking, artificial intelligence (AI) systems used in surveillance (such as facial recognition and Stingray cell-site simulators) and evidence collection are frequently contested on Fourth Amendment grounds. Meanwhile, concerns regarding algorithmic bias and opaque decision-making have been brought up by AI-inspired sentencing and bail decisions, which violate the Fourteenth Amendment. The Wisconsin Supreme Court affirmed the use of the COMPAS risk-assessment algorithm in sentencing decisions in the landmark case of State v. Loomis, 881 N.W.2d 749 (Wis. 2016), but cautioned that courts must notify defendants of the algorithm's use and refrain from treating its results as determinative because the algorithm was proprietary and its methodology was opaque. This ruling has drawn a lot of criticism for failing to require transparency in the underlying algorithm, despite reflecting an effort to strike a balance between efficiency and individual rights.

The use of AI responsibly is now being encouraged by federal guidance. Policies were released by the U.S. Department of Justice mandating that prosecutors' use of risk-assessment tools undergo periodic validation for socioeconomic and racial bias. In its AI Risk Management Framework (2023), the National Institute of Standards and Technology (NIST) called for openness and human supervision of critical AI systems. The Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (2023) issued by President Biden also requires federal agencies to create safeguards for the use of AI in criminal justice tasks, specifically in the areas of explainability, accountability, and non-discrimination.

Ad hoc legislative initiatives at the state level show a growing awareness of the negative effects of AI. One of the strongest privacy laws in the US is the Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/1 (2008), which governs the gathering and use of biometric data, including facial geometry scans, and allows private individuals to file lawsuits for misuse. Comparably, the California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 et seq. (2018), requires private companies that gather personal data to be transparent, though it has little bearing on public law enforcement. Collectively, these advancements show a patchwork strategy in which AI systems are widely employed in law enforcement and

ISSN: 2582-6433

sentencing, but the boundaries are primarily derived from state laws and constitutional interpretation rather than a single federal system.

The U.S. experience serves as an example for India of the dangers of algorithmic governance in the absence of comprehensive legislation, as well as the potential for abuse to be curbed by agency-led policies, judicial oversight, and constitutional protections. It emphasizes in particular the necessity of taking into account algorithmic discrimination, defendants' access to explicable evidence, and independent verification of AI tools—protective measures that are currently absent from India's legal system. India runs the risk of following the American path of corrective rather than preventive control, where courts are compelled to retroactively balance individual rights against operational expediency, if it keeps using AI in criminal justice without passing clear regulations.

5. Comparative Analysis: India vs EU, UK & USA

5.1 India vs European Union

In terms of both legal philosophy and regulatory architecture, India's approach to regulating AI in criminal justice differs significantly from that of the European Union. India currently relies on a number of general statutes, including the Digital Personal Data Protection Act of 2023, the Code of Criminal Procedure of 1973, the Indian Evidence Act of 1872, and the Information Technology Act of 2000, none of which were specifically written with artificial intelligence in mind. As a result, there is no legal definition of "AI," no risk level classification, and no official process for prior evaluation or approval before law enforcement agencies use AI-powered tools. In reality, Indian police forces have implemented tools like facial recognition software and predictive policing software through executive orders and pilot projects with little documentation, little transparency, and almost no external oversight from independent or judicial authorities.

Under the EU Artificial Intelligence Act (AIA), on the other hand, the European Union is developing a custom legislative framework that presents a methodical, risk-based approach to regulating AI systems. Criminal justice and law enforcement AI applications are specifically categorized as "high-risk" by the AIA, which means they must meet strict standards for accuracy, robustness, transparency, documentation, human oversight, and conformance assessment prior to deployment. Real-time facial recognition in public places is one example of a use that is either strictly forbidden or permitted under very limited circumstances.

ISSN: 2582-6433

Additionally, in order to enforce sanctions and monitor compliance, the EU system sets up a regulatory infrastructure that includes a European Artificial Intelligence Board and national supervisory authorities. Strong data protection measures and accountability for processing personal data in criminal investigations are enforced by the General Data Protection Regulation (GDPR) and Law Enforcement Directive 2016/680, which supplement this.

Therefore, the EU's strategy is proactive, rights-centric, and legislative in nature, whereas India's current regime is reactive, fragmented, and executive-led. The EU emphasizes human-in-the-loop oversight, proportionality and necessity assessments, and transparency (also known as "explainable AI") as prerequisites for the use of AI in criminal justice. These principles are deeply ingrained in the EU Charter of Fundamental Rights. In contrast, India does not incorporate proportionality and legality concerns into ex-ante regulatory obligations; instead, it leaves them to post-hoc constitutional review by courts under Puttaswamy. India's enforcement of safeguards is primarily dependent on individual lawsuits contesting police behavior rather than systemic monitoring because the country lacks a formal conformity assessment process, audit trail requirement, or specialized regulator.

In conclusion, India can benefit from the EU model since it shows how important it is to define AI legally, categorize risk levels, mandate transparency and accountability procedures, and clearly delineate regulatory responsibility for adherence. The current legislative gap could be filled and fundamental rights could be protected from the erosion of AI-powered criminal justice tools by implementing a similar framework that is adapted to India's institutional and constitutional context.

5.2 India vs United Kingdom

Despite having similar adversarial criminal justice systems and a common-law heritage, India and the UK have very different regulatory approaches to AI in law enforcement. India has little legal oversight of AI, which permits the introduction of technologies like facial recognition and predictive policing through administrative experimentation with few procedural restrictions. On the other hand, the UK has a "soft law" framework in which the use of AI is governed by a combination of sector-specific guidelines, judicial review, and data protection laws under the UK General Data Protection Regulation (UK-GDPR).

The function of judicial oversight both before and during deployment is a crucial distinction.

ISSN: 2582-6433

The UK Court of Appeal invalidated the indiscriminate use of automated facial recognition tools in Bridges v. South Wales Police, [2020] EWCA Civ 1058, highlighting the importance of legality, proportionality, and clear policy documentation. The Court mandated that law enforcement conduct equality impact assessments, have clear operational boundaries, and make usage policies publicly available. In contrast, India has approved technologies like the Automated Facial Recognition System (AFRS) through executive orders without first conducting an ethical analysis or publishing standard operating procedures. As a result, legal concerns can only be brought up through post-facto constitutional challenges.

Additionally, the UK Government's approach, which is outlined in the White Paper – A Pro-Innovation Approach to AI Regulation (2023) and the National AI Strategy, adopts five guiding principles: contestability, safety, accountability, transparency, and fairness. Current regulators like the Information Commissioner's Office (ICO), which publishes particular guidelines on AI surveillance technologies, enforce these principles even though they are not legally binding. Similar concerns are expressed in policy documents such as the NITI Aayog National Strategy for AI (2018) in India, but they are still aspirational, and no enforcement body has been established to guarantee adherence to moral AI principles.

Therefore, the UK's regulatory ecosystem (courts + ICO + policy guidance) provides procedural discipline and accountability in the use of AI within criminal justice, something that is conspicuously lacking in India, even though the UK does not yet have a single AI Act like the EU. The UK model shows how robust oversight procedures, published policies, and a court's willingness to block illegal uses can provide a significant check on police powers even in the absence of codified AI legislation. Emulating the UK's emphasis on proportionality assessments, publicly accessible operating policies, and regulatory oversight by an independent data authority could strengthen legitimacy and protect fundamental rights without stifling technological innovation for India, which operates under a similar constitutional and common-law framework.

5.3 India vs United States

While neither country has a comprehensive, AI-specific federal statute, both the US and India use AI technologies in criminal adjudication and policing. The regulatory ramifications of this differ depending on the jurisdiction. Law enforcement in India uses AI in a low-regulation setting, primarily due to agency-level decisions and constrained only by broad constitutional

ISSN: 2582-6433

principles like those outlined in Justice K.S. Puttaswamy v. Union of India (2017). The United States, on the other hand, mainly depends on constitutional litigation, agency guidance, and targeted state legislation to impose affirmative limits on the use of AI in criminal justice, even though it does not have a criminal justice statute specifically regarding AI.

At the federal level, invasive use of AI-enabled surveillance systems like mobile phone tracking and facial recognition has been contested by citing Fourth Amendment protections against unreasonable search and seizure. Concerns about the fairness of the Fourteenth Amendment have also led judges to exercise caution when it comes to AI-assisted risk assessment and sentencing. The Wisconsin Supreme Court permitted the use of the proprietary COMPAS risk algorithm in State v. Loomis, 881 N.W.2d 749 (Wis. 2016), but it required notice and limitations to prevent the defendant's due process rights—a type of conditional legitimacy created by the court—from being violated. Similar case law evaluating algorithmic tools used by judges or prosecutors has not yet been seen in India.

Additionally, U.S. federal agencies have released normative guidance. For example, the NIST AI Risk Management Framework (2023) suggests transparency, human oversight, and verifiable documentation, while the Department of Justice's AI policy memorandum mandates frequent validation and bias testing for risk-assessment tools. Most notably, federal law enforcement agencies are specifically instructed to reduce bias and guarantee explainability prior to implementing AI in President Biden's Executive Order on Safe, Secure, and Trustworthy AI (2023). There are no comparable executive-level normative guidelines in India.

In contrast to the current regulatory environment in India, where the DPDP Act, 2023, does not allow individuals to sue the State for biometric misuse, state-level legislation such as the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/1 (2008), which grant individuals a private right of action against misuse of biometric data by both private and public actors, demonstrate a more proactive regulatory mindset. India's centralized yet loose approach to law-enforcement exemption under the DPDP Act lacks the pockets of strong accountability that these restricted but enforceable laws provide in the United States.

As a result, even though neither nation has unified AI laws at this time, the US makes up for this by establishing strong checks and balances on AI-assisted criminal justice procedures

ISSN: 2582-6433

through state-level regulatory experiments, federal policy guidance, and a strong constitutional litigation culture. In contrast, India's lack of agency-level accountability mechanisms, weak ex-ante controls, and limited judicial intervention opportunities make it more susceptible to unchecked State practice, indicating the urgent need for legislative and policy reform.

6. Need for Legislative Reform in India

India's current criminal justice laws are essentially insufficient to control machine-driven policing, surveillance, and adjudication since they were never intended to handle the complexity of artificial intelligence. The 1973 Code of Criminal Procedure allows for human investigators, prosecutors, and judges to make decisions, but it offers no authorization process, chain-of-custody protections, or procedural rights in cases where AI systems influence or produce those decisions. Similarly, even with the addition of Sections 65A and 65B, the Indian Evidence Act of 1872 does not take into account algorithmic outputs or machine-learned inferences, nor does it provide any means of evaluating their scientific methodology, bias propensity, or reliability. While outlining digital offenses and responsibilities, the Information Technology Act of 2000 makes no mention of "artificial intelligence," establishes no risk-based classification, or lays out legal requirements unique to AI implementations. Therefore, without a legal framework to guarantee accountability, transparency, or constitutional compliance, law enforcement agencies are now implementing technologies like facial recognition and predictive policing through administrative decisions.

In light of India's social circumstances, these regulatory gaps are especially concerning. The risk of an arbitrary and uneven deployment of AI systems is increased by significant infrastructure differences between urban and rural police units. The constitutional framework, particularly Articles 14, 19, 20, 21, and 22, mandates that any interference by the State with life, liberty, or privacy must pass the legality, necessity, and proportionality tests. However, even the people targeted by these technologies are unaware of how AI is currently being used. Furthermore, marginalized groups are disproportionately susceptible to algorithm-based profiling and surveillance due to India's stark digital divide. AI systems run the risk of escalating rather than reducing current injustices in the criminal justice system if proper safeguards ensuring transparency and redressal are not in place.

Therefore, there is an urgent need for legislative action in three key areas: institutional oversight, procedural safeguards, and statutory authorization. First, a technical impact

ISSN: 2582-6433

assessment outlining the AI system's design, purpose, accuracy limitations, bias propensity, and human-oversight plan should be included in the Criminal Procedure Code amendment that would make the use of AI at any point during an investigation or prosecution subject to prior judicial authorization. In order to maintain judicial accountability and discretion, statutory provisions must explicitly acknowledge algorithmic outputs as non-determinative advisory tools that are always subject to independent human judgment. A meaningful opportunity for the accused to challenge the validity, relevance, and probative value of such evidence at trial should also be provided by amending the Evidence Act to specifically regulate AI-generated or AI-assisted evidence. This would allow courts to require the disclosure of algorithmic models, training datasets, and error rates. Crucially, when liberty is at risk, judicial scrutiny must always take precedence over assertions of proprietary confidentiality.

Lastly, in addition to reforming the rules of evidence and procedure, a specific oversight mechanism needs to be put in place. All AI systems used by law enforcement and courts should be registered by a statutory AI Oversight Authority made up of multidisciplinary experts. This authority should also be responsible for reviewing conformance assessment reports, conducting regular audits, and receiving individual complaints. By guaranteeing ongoing monitoring as opposed to sporadic, litigation-driven review, such an authority would fill the current void. The National Human Rights Commission and data protection regulator should be specifically mandated to publish yearly transparency reports on AI used in criminal justice and to enforce adherence to the legality, fairness, and proportionality principles until such legislation is passed. Without these changes, India's criminal justice system's unbridled adoption of AI-based technologies poses a threat to the country's long-standing constitutional guarantees of due process and the rule of law.

7. Recommendations (Law & Policy)

India must take a purposeful and moral approach to regulating AI in the criminal justice system in light of the comparative analysis that has been done. Enacting a specific legislative framework that defines artificial intelligence systems and categorizes them based on the level of threat they pose to constitutional values must be the top priority. India should identify high-risk AI applications in criminal justice, such as facial recognition, predictive policing, biometric surveillance, and algorithmic risk assessment, and require them to undergo ex ante authorization, conformity assessment, and continuous audit requirements, taking inspiration from the European Union's strategy. By doing this, it would be impossible to implement such

ISSN: 2582-6433

technologies without a clear record of their goals, specifications, accuracy standards, plans for human oversight, and possible rights implications.

A judicial magistrate must authorize any investigative technique that uses artificial intelligence (AI) and provide a reasoned application outlining its design, scope, and safeguards. This requirement is similar to the one currently in place for search, seizure, and interception authorization. These obligations must be operationalized through amendments to the Code of Criminal Procedure, 1973. In addition, the Indian Evidence Act of 1872 needs to be changed to specifically address evidence that has been produced or processed by AI. Any AI system used by the police or prosecution should be subject to disclosure by courts, which should include the underlying algorithm, training dataset, error rates, and validation records. This would protect the accused's ability to successfully contest the validity and scientific foundation of any incriminating evidence that currently enters the courtroom through ambiguous forensic reports.

The current exemption for law enforcement under Section 17(2) should be significantly narrowed by amending the Digital Personal Data Protection Act, 2023, given that AI systems handle vast amounts of personal data, including sensitive biometric information. This would ensure that police use of AI is still subject to purpose limitation, data minimization, and time-bound retention. The creation of an independent AI oversight body, similar to the European Artificial Intelligence Board, would provide the institutional capacity needed to oversee the use of AI by law enforcement, enforce legal requirements, publish codes of practice, and carry out compliance audits across agencies. In addition, the National Human Rights Commission and State Human Rights Commissions may be legally empowered to investigate and receive complaints regarding the improper or overuse of AI-powered policing tools.

Mandatory algorithmic impact assessments must be adopted at the policy level in India before any government purchases or uses AI for criminal justice. The results of these evaluations, which should include projected effects on civil liberties, equality, proportionality, privacy, and harm to vulnerable groups, should be made public. This would bring India's practices into line with the US and UK's stakeholder consultation and transparency policies. In order to minimize discriminatory or disproportionate outcomes, a national framework for bias testing, fairness auditing, and periodic validation of AI systems must be implemented. This is in line with the US's evolving jurisprudence under the Fourteenth Amendment and the EU's anti-discrimination

ISSN: 2582-6433

obligations. The government must maintain the contractual right to examine proprietary software and reject deployment if transparency is not provided when AI systems are purchased from private vendors.

Increasing capacity is also crucial. Specialized training on the operational boundaries, evidentiary value, and rights implications of AI tools is required for judges, prosecutors, and police in order to encourage responsible and informed use of these technologies. It should be mandatory to institutionalize human-in-the-loop mechanisms, which guarantee that responsible human actors, not automated systems, make the final decisions regarding arrest, charge, bail, and sentencing. The fundamental components of criminal justice—human agency and moral responsibility—are upheld by this strategy.

India should eventually work toward a comprehensive Artificial Intelligence (Criminal Justice) Regulation Act that takes into account its particular constitutional framework, sociological realities, and law enforcement requirements. Legal definitions, authorization processes, evidentiary rules, oversight mechanisms, privacy protections, audit mandates, and accountability provisions must all be consolidated into a unified regulatory framework by this statute. An interim Model Standard Operating Procedure issued by the Ministry of Home Affairs in consultation with the Ministry of Law and Justice should immediately restrict executive use of AI in criminal justice until such legislation is enacted. This procedure should require the publication of use-case documents, operational guidelines, and access to grievance mechanisms.

Artificial intelligence has the potential to significantly improve the criminal justice system in India, but only if it is governed proactively, openly, and in accordance with the constitution rather than retroactively through infrequent court rulings. India can take advantage of AI without compromising its long-standing commitment to due process, justice, and the rule of law by incorporating legislative clarity, procedural safeguards, independent oversight, transparency, and capacity building.

8. Conclusion

With its promise of previously unheard-of efficiencies in policing, evidence analysis, and adjudication, artificial intelligence is set to revolutionize criminal justice systems around the globe. However, as this study shows, the use of AI in criminal justice administration presents

ISSN: 2582-6433

significant ethical, doctrinal, and constitutional issues that cannot be resolved solely by the executive branch. India is at a regulatory crossroads right now. The State's legal system is still based on laws written for analogue times, even as it increasingly experiments with AI-driven technologies, such as forensic analysis, facial recognition, and predictive policing. Executive-led adoption of robust surveillance and decision-support systems without explicit procedural safeguards, transparency obligations, or accountability mechanisms has resulted from the lack of statutory recognition of AI and fragmented procedural and evidentiary rules.

Alternative regulatory trajectories that provide both normative guidance and cautionary lessons are revealed through comparative analysis with the US, UK, and EU. The proactive, legislative approach that defines AI, categorizes risks, and incorporates structured safeguards prior to deployment is what distinguishes the EU model. The UK serves as an example of how judicial vigilance and principled soft-regulation can impose meaningful discipline through proportionality, transparency, and oversight—even in the absence of a codified AI law. The U.S. experience shows how algorithmic entrenchment in sentencing, policing, and evidence presentation can be dangerous in the absence of ex ante regulation. It also shows how constitutional litigation and state-level legislation can be used to gradually correct abuses.

India now needs to start implementing significant legal reform and go beyond policy declarations. According to this paper's doctrinal contributions, meaningful regulation necessitates: (i) statutory authorization and risk-based categorization of AI technologies used in criminal justice; (ii) changes to the Indian Evidence Act and Code of Criminal Procedure that incorporate requirements for explainability, transparency, human oversight, and judicial scrutiny; and (iii) the establishment of independent institutional oversight that can effectively monitor compliance, enforce safeguards, and provide redress. The due process, privacy, nondiscrimination, and fairness requirements of the Constitution require that technological advancements in criminal justice only take place within a well-defined legal framework that respects individual rights.

Therefore, regulating artificial intelligence in India's criminal justice system is a constitutional requirement rather than just a technical or administrative problem. AI can be used as a tool to uphold the rule of law rather than weaken it if lawmakers take a proactive, moral, and all-encompassing approach to legislation. Before technological adoption surpasses legal protection, India must take advantage of the chance to create a distinctively indigenous yet

ISSN: 2582-6433

globally informed regulatory framework.

References

Cases

1. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
2. *Bridges v. Chief Constable of S. Wales Police*, [2020] EWCA (Civ) 1058 (UK).
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
4. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).
5. *R. (Bridges) v. Chief Constable of S. Wales Police*, [2019] EWHC (Admin) 2341 (UK).
6. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016) (U.S.).

Statutes & Regulations

1. Cal. Civ. Code §§ 1798.100–.199 (West 2018).
2. Code of Criminal Procedure, No. 2 of 1974, India Code (1974).
3. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
4. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
5. Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).
6. 740 Ill. Comp. Stat. 14/1 (2008).
7. Indian Evidence Act, No. 1 of 1872, India Code (1872).
8. Information Technology Act, No. 21 of 2000, India Code (2000).
9. Directive (EU) 2016/680, 2016 O.J. (L 119) 89.

Policy Documents & Reports

1. Dep't for Sci., Innovation & Tech., *A Pro-Innovation Approach to AI Regulation* (U.K., Mar. 2023).
2. Ministry of Electronics & Info. Tech., *National Strategy for Artificial Intelligence* (India, 2018).
3. Nat'l Inst. of Standards & Tech., *Artificial Intelligence Risk Management Framework* (U.S., 2023).
4. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (India, 2018).