VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# ARTIFICIAL INTELLIGENCE AND THE CRIMINAL JUSTICE SYSTEM IN INDIA: OPPORTUNITIES, CHALLENGES AND LEGAL IMPLICATIONS

- Anushka[1]

## ABSTRACT

With rapid advancements in Artificial Intelligence (AI) technologies being made across various fields, there has emerged a scenario wherein such advanced technologies have permeated the field of criminal justice.In light of the above, therefore, it becomes necessary to deliberate on some important questions in respect of justice, fairness, due process, and human rights. India, a nation that has long grappled with issues such as a congested judiciary, a high number of undertrial cases, dysfunctional police departments, and ingrained biases, finds itself at a crossroads where the emergence of such technologies holds both great promise as well as great danger. In this research paper, an attempt will be made to examine the emergence of AI technologies within the Indian criminal justice system in respect of how the same are being employed in predictive policing, facial recognition technology, forensic sciences, judicial processes, and prisons. On the basis of the Constitutional philosophy, legislation, judicial rulings, and international experience, it can be concluded that the employment of AI technologies offers tremendous possibilities; however, if not controlled, it might exacerbate pre-existing biases and infringe upon fundamental human rights.

The paper reviews the current lack of laws regarding AI in India and suggests an effective regulatory mechanism which can strike a balance between technological development and protection of civil liberties. The findings of the research show that the proper use of AI in the criminal justice system needs to be achieved through joint efforts of different parties.

[1] Student at Atal bihari Vajpayee School of Legal Studies, Chattrapati Shahu Ji Maharaj University, Kanpur

**Key Words :** Artificial intelligence, Criminal Justice, Predictive Policing, Facial Recognition, Due Process, Algorithmic Bias, Legal Implications, Fundamental Right, Surveillance.

## CHAPTER 1- INTRODUCTION

### INTRODUCTION

In general, the confluence between technology and law has always posed certain difficult questions for jurisprudence. However, the current age of artificial intelligence[2] poses an even greater dilemma since this new technology promises to change the way governments operate. Generally referred to as the simulation of human intelligence processes by machines specifically computer systems, artificial intelligence comprises machine learning[3], natural language[4] processing, deep learning, computer vision among other computational methods through which machines can do jobs that used to be carried out by humans. In criminal justice[5], artificial intelligence can be found in face recognition, policing algorithms, decisions on bail and sentencing, forensic examination, prisons, and crime prediction among others.

In its operations, India's criminal justice system exhibits certain structural deficiencies. According to reports, there are about five crores pending cases[6] in the Indian judiciary with the Supreme Court of India dealing with over eighty thousand cases. From National Crime Records Bureau[7] (NCRB), it is clear that crime underreporting, poor investigation structure, and lengthy trial periods plague the system in India. Furthermore, prisons have exceeded capacity for years now with most of the inmates being those held for trial purposes.

However, the use of artificial intelligence in the criminal justice process involves more than technological issues; it is inherently legal and political in nature. The implementation of such technologies has serious implications for Articles 14[8] (equal treatment before the law), 19

[2]Cathy O'Neil, Weapons of Math Destruction (Crown Publishers, 2016)
[3]Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (3rd edn., Pearson, 2010)
[4]Daniel Jurafsky & James H. Martin, Speech and Language Processing (Pearson, 2009)
[5]Andrew Ashworth, The Criminal Process (Oxford University Press, 2010)
[6]National Judicial Data Grid (NJDG), Pending Cases Report (2023)
[7]National Crime Records Bureau, Crime in India 2022 (2023)
[8] The Constitution of India, 1950

(freedom of speech and movement), 21[9] (right to life and personal liberty), and 22 (protection from arbitrary arrest and detention) of the Constitution of India. It also gives rise to concerns regarding the applicability of the ICCPR in relation to the right to a fair trial[10], presumption of innocence, and prohibition against arbitrary detention.

The rest of this paper is organized as follows. After this introduction, Section III highlights the main problem statement. Section IV provides a review of previous literature on artificial intelligence in the criminal justice system with specific regard to the Indian context. Section V states the study objectives. Section VI discusses the research questions. Section VII elaborates the research methodology. Section VIII provides a detailed analysis and discussion of the application of artificial intelligence in each aspect of the criminal justice system. Section IX presents the findings and observations of this paper.

## STATEMENT OF PROBLEM

The criminal justice system in India[11] currently finds itself at a crossroads. In one sense, the pressing need for reforms within the existing framework owing to the backlog of cases, poor forensic science facilities, and inefficiencies in the system makes a strong case for the incorporation of AI-powered technology. However, at the same time, the accelerated use of AI in policing, prosecution, and decision-making poses grave threats to constitutional rights[12] and due process[13].

The primary concern that will be examined in this research is the widening regulatory gap created by the use of AI in India's criminal justice system without adequate regulations to govern its use. There are a number of interconnected reasons why this gap poses a threat.

First, AI algorithms[14] trained using data from past judicial processes can exacerbate pre-existing social biases[15] against marginalised groups[16], such as religious minorities, Scheduled Castes and

[9]The Constitution of India, 1950
[10]International Covenant on Civil and Political Rights (ICCPR), 1966
[11]Upendra Baxi, The Crisis of the Indian Legal System (Vikas Publishing, 1982)
[12]The Constitution of India, 1950
[13]Maneka Gandhi v. Union of India, (1978) 1 SCC 248
[14]Cathy O'Neil, Weapons of Math Destruction (Crown Publishers, 2016)
[15]Julia Angwin et al., "Machine Bias", ProPublica (2016)

Scheduled Tribes, as well as economically weaker groups. Police algorithms that depend on historical crime data can lead to the practice of over-policing marginalised communities who have been victims of discriminatory policing practices in the past, which would result in a self-fulfilling prophecy of high levels of crime in such communities.

Second, the use of facial recognition technology[17] for surveillance[18] by various police forces operating in the states of Delhi, Telangana and Tamil Nadu in India is a serious violation of civil liberties and the right to privacy[19] enshrined as a fundamental right in Article 21[20] of the Indian Constitution after the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) Moreover, the facial recognition technology exhibits greater inaccuracies for dark-skinned people.

Third, the use of AI in judicial decision-making[21] raises serious concerns in relation to the rights to a fair trial[22], the right to an explanation in judicial decisions, and the requirement that justice should not only be done but seen to be done. The lack of transparency[23] in algorithms, which has become popularly known as the "black box[24]" problem, renders it impossible for the litigating parties to question the basis of the judicial decision made through the use of the AI tool.

Fourth, there is no law regulating the use of AI [25]technology in the criminal justice process in India. While certain provisions of the IT Act, 2000[26], draft Digital Personal Data Protection Act, 2023[27], and National AI Strategy do offer some peripheral regulation of the use of AI technology, there is no specific law regulating the use of AI technology in this important area.

## CHAPTER 2 – REVIEW OF LITERATURE

[16]Marc Galanter, Competing Equalities (Oxford University Press, 1984)
[17]Joy Buolamwini & Timnit Gebru, "Gender Shades" (2018)
[18] David Lyon, Surveillance Society (Open University Press, 2001
[19]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[20]The Constitution of India, 1950
[21]D.Y. Chandrachud, "Artificial Intelligence in Indian Courts" (2020)
[22]International Covenant on Civil and Political Rights (ICCPR), 1966
[23]European Commission, Ethics Guidelines for Trustworthy AI (2019)
[24]Frank Pasquale, The Black Box Society (Harvard University Press, 2015)
[25]NITI Aayog, National Strategy for Artificial Intelligence (2018)
[26]Information Technology Act, 2000
[27]Digital Personal Data Protection Act, 2023

## REVIEW OF LITERATURE

There have been notable advancements in AI[28] and its application in the judicial process[29] in the last decade, mainly due to activities carried out in the US, EU countries, and lately in the global south[30]. Literature reviews show the following main trends in the field.

### Foundational Texts on Algorithmic Justice

As described by Angwin et al(2016) in their groundbreaking ProPublicaresearch piece "Machine Bias[31]," the racially discriminating[32] effects of the COMPAS algorithm[33], an instrument used in the US courts to determine the risk of recidivism[34] of an individual, were brought to light. Specifically, African Americans were found to be almost twice as likely to be marked by the algorithm as criminals than Caucasians.

O'Neil's critique of algorithms in 'Weapons of Math Destruction'[35] (2016) was more comprehensive in nature and discussed how such tools entrenched discrimination[36], avoided responsibility, and worked on an extremely large scale[37]. The author's approach toward analyzing AI on the basis of its opacity[38], scale, and damage is a helpful framework for understanding the impact of AI on the Indian criminal justice system.

Brayne (2020)'s ethnographic study of the LAPD[39] and their adoption of predictive policing[40] tools has emphasized that these algorithms not only predicted crimes but created them in some ways.

In her analysis of the sociological dimension[41] of adopting AI, she has shown the importance of considering sociological perspectives when discussing the impact of AI from a legal standpoint.

[28]Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (3rd edn., Pearson, 2010)
[29]Richard Susskind, Tomorrow's Lawyers (Oxford University Press, 2013)
[30]UNDP, Artificial Intelligence for Development (2021)
[31]Julia Angwin,Jeff Larson, Surya Mattu and Lauren Kirchner, "Machine Bias", ProPublica (23 May 2016)
[32]United States v. Loomis, 881 N.W.2d 749 (Wisconsin Supreme Court, 2016)
[33]Julia Angwin et al., "Machine Bias", ProPublica (2016)
[34]John Monahan & Jennifer Skeem, "Risk Assessment in Criminal Justice" (2016)
[35]Cathy O'Neil, Weapons of Math Destruction (Crown Publishers, 2016)
[36]Solon Barocas & Andrew Selbst, "Big Data's Disparate Impact" (2016)
[37]Nick Bostrom, Superintelligence (Oxford University Press, 2014)
[38]Frank Pasquale, The Black Box Society (Harvard University Press, 2015)
[39]Los Angeles Police Department Reports (2018)
[40]Sarah Brayne, Predict and Surveil (Oxford University Press, 2020)

### Facial Recognition and Surveillance

According to Garvie et al's "The Perpetual Line-Up" (2016), a pioneering work examining the use of facial recognition technology[42] in policing in America, reported extensive applications of this technology in American police departments[43], with accuracy disparities for non-whites. The study's conclusions can be readily applied to the Indian context, where facial recognition technologies are extensively used by the police without adequate legal protections.

In her research "Gender Shades[44]" (2018), Buolamwini and Gebru found that facial recognition technologies offered by the world's most successful technology corporations perform less accurately on darker skin and women. With India's diverse demographics, including a sizable number of people with dark skin[45], the accuracy disparities[46] raise crucial legal issues.

### AI in the Indian Context

The issue of AI and criminal justice has witnessed substantial growth, yet the amount of research generated is still fairly young as compared to the literature produced by Western jurisdictions. For instance, Narayan and Roy (2021) conducted an early attempt at evaluating various AI-driven predictive policing[47] technologies employed by state-level police forces in India. Their findings revealed that these systems were introduced with little regard for proper impact assessments[48], adequate privacy measures[49], and any sort of accountability[50].

In another study, Singh (2022) analyzed India's AFRS[51] developed by the National Crime Records Bureau (NCRB) and pointed out how it contradicted the constitutionally guaranteed right to privacy in India due to the lack of a proper data protection[52] regime. Lastly, the Internet

[41]David Garland, The Culture of Control (2001)
[42]Clare Garvie et al., "The Perpetual Line-Up" (2016)
[43]Georgetown Law Center on Privacy & Technology Report (2016)
[44]Joy Buolamwini & Timnit Gebru (2018)
[45]NIST Report (2019)
[46]NIST, Face Recognition Vendor Test (2019)
[47]Narayan & Roy, "Predictive Policing in India" (2021)
[48]NITI Aayog, Responsible AI for All (2021)
[49]Justice K.S. Puttaswamy v. Union of India (2017)
[50]Internet Freedom Foundation Report (2021)
[51]NCRB Tender Document (2019)
[52]Digital Personal Data Protection Act, 2023

Freedom Foundation is known for consistently providing information on the legal problems associated with India's surveillance[53] apparatus.

In their study, Chandrachud (2020), examining the potential use of AI in Indian courts[54], acknowledged that while AI tools could assist in legal research and case management, their use in adjudication proper raised profound constitutional concerns, particularly regarding due process[55] and judicial accountability[56]. The Supreme Court's e-Courts Mission Mode Project and SUPACE[57] (Supreme Court Portal for Assistance in Court's Efficiency) represent institutional acknowledgements of AI's potential, albeit cautiously framed as research assistance rather than adjudication tools.

## OBJECTIVES OF THE STUDY

These are the objectives that will guide the research carried out in the current study:

- To carry out a critical analysis of the existing and potential uses of AI in the various aspects of the Indian criminal justice system, such as policing, prosecution, adjudication, and corrections.
- To highlight and analyze the benefits of AI technology in improving the efficiency, efficacy, and uniformity in criminal justice processes in India.
- To highlight the risks and problems posed by the use of AI in criminal justice systems in India, particularly those related to algorithmic discrimination, violations of privacy, violation of due process, and threats to the enjoyment of constitutional rights in India.
- To evaluate the sufficiency of India's current legal and regulatory regime in regulating the uses of AI in criminal justice processes and identify the gaps in the current regime.
- To derive from international regulatory experiences on the uses of AI in criminal justice processes, particularly that of the EU AI Act.

[53]IFF, Project Panoptic (2021)
[54]D.Y. Chandrachud, "AI in Indian Judiciary" (2020)
[55]Maneka Gandhi v. Union of India (1978)
[56]Upendra Baxi, Judicial Accountability in India
[57]Supreme Court of India, e-Committee Report

- To recommend a suitable regulatory regime for governing the uses of AI in criminal justice processes in India.

## RESEARCH QUESTION

The current study is guided by the following research questions:

- What is the current scenario in relation to the application of artificial intelligence in India's criminal justice process, and what are the major domains of its application?
- To what extent do the applications of artificial intelligence in the criminal justice process in India comply with the basic rights guaranteed in Part III of the Constitution of India, including Articles 14, 19, 21, and 22?
- Do the applications of technologies of predictive policing and facial recognition entail any violation of the right to privacy as enshrined in Justice K.S. Puttaswamy (Retd.) v. Union of India[58], and if yes, on what grounds?
- What are the ethical and legal considerations involved in the application of AI for decision support in judicial processes, especially in light of considerations of natural justice and the right to fair trial?
- Is the current legal framework of the IT Act 2000[59], the Criminal Procedure Code (revised as Bharatiya Nagarik Suraksha Sanhita 2023), and the DPDP Act[60] adequate to regulate the use of artificial intelligence in criminal justice processes?
- What can India learn from other nations' experiences, and what is the most suitable model for AI governance in India?

# CHAPTER 3 – METHODOLOGY

## RESEARCH METHODOLOGY

[58]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[59]Information Technology Act, 2000
[60]Digital Personal Data Protection Act, 2023

.The study is mainly doctrinal[61] in nature, utilizing the black letter law[62] approach supplemented by socio-legal and comparative analysis[63]. In the doctrinal aspect, it includes a systematic scrutiny of constitutional provisions, legislative statutes, rulings of Supreme Court and the High Courts in India, reports of standing committees of parliament, and policy pronouncements from government ministries.

Primary sources considered for the study include the Indian Constitution, Bharatiya Nyaya Sanhita 2023[64] (BNS), Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS), Bharatiya Sakshya Adhiniyam 2023 (BSA), Information Technology Act, 2000[65] and its 2008 amendment, Digital Personal Data Protection Act 2023, NCRB's Automated Facial Recognition System (AFRS) tender notice, Responsible AI framework from Ministry of Electronics and Information Technology, and Supreme Court rulings like Puttaswamy[66] (2017) and Selvi v. State of Karnataka (2010).

Secondary literature consists of peer-reviewed[67] scholarly journals, legal books, and think tanks like the Internet Freedom Foundation[68], the Centre for Internet and Society, the National Law School of India Review, and international agencies like the UN Special Rapporteur[69] on the right to privacy and the European Union Agency for Fundamental Rights.

Comparative analysis entails an evaluation of the regulatory frameworks in place in the European Union[70], the United States[71], the United Kingdom[72], China, and Singapore. The comparative approach[73] adopted herein is not for the purpose of transplanting the laws of other jurisdictions wholesale into the Indian context but rather to examine best practices that can be adopted by the Indian constitution, institutions, and socio-cultural context.

[61]S.N. Jain, Legal Research Methodology (LexisNexis, 2016)
[62]Salmond, Jurisprudence (Sweet & Maxwell, 12th edn
[63]Zweigert & Kötz, Introduction to Comparative Law (Oxford University Press, 1998)
[64]The Bharatiya Nyaya Sanhita, 2023
[65]Information Technology Act, 2000
[66]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[67]Oxford University Press, Legal Research Guidelines
[68]Internet Freedom Foundation, Project Panoptic (2021)
[69]UN Report on Right to Privacy (2019)
[70]European Union, Artificial Intelligence Act (2024)
[71]State v. Loomis (2016)
[72]UK Government, Algorithmic Transparency Standard (2021)
[73]Zweigert& Kötz, Comparative Law (1998)

## CHAPTER 4 - ANALYSIS AND DISCUSSION

ANALYSIS AND DISCUSSION

### AI in Policing: Predictive Algorithms and Surveillance Technologies

Predicative policing[74] can be described as an approach where mathematically driven tools[75] are used for predicting crimes, predicting criminals, and deploying police resources. In India, a number of states are using or have tried predictive policing systems. In Uttar Pradesh, the police force uses a predictive analytic system which assigns risk scores based on one's criminal record, sociometric analysis, among other criteria. Similarly, the Himachal Pradesh Police has used the system called 'Himachal Predictive'. Moreover, predictive policing has been tried in other states like Andhra Pradesh and Telangana.

From a constitutional point of view, there are a number of rights affected when it comes to predictive policing. Firstly, since predictive policing assigns risk scores to people based on their predicted future actions, it goes against the principle of presumption of innocence[76], which is the very foundation of Article 21[77]. The Supreme Court of India has ruled that liberty 'can be curtailed only according to procedures established by law', and that those laws should be 'fair, just and reasonable[78]', as per the case of Maneka Gandhi vs Union of India, 1978. It would be difficult to reconcile this approach with predictive policing.

The Automated Facial Recognition System (AFRS)[79], which was introduced by the NCRB in 2019, can be termed as one of the largest projects involving the use of artificial intelligence for surveillance[80] in India. Its main idea is the creation of an interconnected database of facial recognition images obtained through CCTV cameras, crime reports, passport details, Aadhaar

[74]Sarah Brayne, Predict and Surveil (Oxford University Press, 2020)
[75]Andrew Ferguson, The Rise of Big Data Policing (NYU Press, 2017
[76] Maneka Gandhi v. Union of India,(1978) 1 SCC 248
[77]The Constitution of India, 1950
[78]Maneka Gandhi v. Union of India, (1978)
[79] Internet Freedom Recognition, Project Panoptic (2021)
[80]David Lyon, Surveillance Society (2001)

records[81], and prison records, among others, to be used by all police departments in India. There are several aspects of this project that can be considered as being unconstitutional.

Under the decision of the nine-judge bench in Puttaswamy v Union of India, it has been clearly stated that privacy[82] is a part of the Right to Life and Personal Liberty guaranteed under Article 21 of the Indian Constitution. The decision laid down a three-tier test to determine whether a privacy violation was justified. This included legality (whether the interference is legal), legitimacy (whether the interference is for a legitimate public purpose), and proportionality[83] (whether the method of interference is proportional to the objective). All these requirements have not been fulfilled in the case of the AFRS as of now.

In addition to this, studies have revealed that FRT has higher failure rates when used on people with darker skin colors and women. According to research conducted by the National Institute of Standards and Technology (NIST) of the United States, some of the commercial FRT algorithms used in the country have failed to correctly identify the faces of Asians and African-Americans by ten to a hundred times more than Caucasian men. In an Indian setting, the implications of these errors become far worse since they could lead to imprisonment.

**AI in Prosecution and Investigation**

The use of AI is becoming more common in the investigative and prosecution phases through forensic analysis[84], digital evidence processing, cybercrime investigations, and case management systems. AI tools are increasingly used at CFSL and state forensic science laboratories in evidence analysis by applying technologies of pattern recognition in fingerprints matching and DNA profiling, as well as digital forensics[85]. Such an application, if properly validated, has the potential to enhance the integrity of forensic evidence, reduce mistakes in the analysis process and avoid false convictions caused by forensic errors.

[81]NCRB, AFRS Tender Document (2019)
[82] Justice K.S Puttaswamy Case (2017)
[83]Puttaswamy v. Union of India, (2017)
[84]NCRB, Crime in India 2022 (2023)
[85]Interpol, Digital Forensics Report (2020)

The new Indian legal document called Bharatiya Sakshya Adhiniyam 2023 (BSA), which replaces the Evidence Act 1872, contains sections regulating the use of electronic evidence[86], including evidence created through computers. In particular, Sections 63 of BSA regulating secondary evidence and Section 65B governing the use of electronic evidence provide a statutory basis for the introduction of AI-produced evidence in criminal investigations. Nonetheless, both sections were developed before the wide implementation of AI-based technologies and do not answer a number of issues relating to the use of AI evidence, such as the auditing of algorithms, the necessity of presenting expert opinions on AI methods and validation criteria for AI software.

In the case of Selvi v. State of Karnataka[87], 2010, the Supreme Court of India categorically held that the practice of employing narcoanalysis[88], brain-mapping, and polygraph tests is violative of the rights guaranteed under Articles 20(3)[89] and 21 of the Indian Constitution. Though the case pertains to techniques of investigation other than those based on artificial intelligence, but the logic behind it could possibly be applied to certain behavioral analysis tools based on AI technology, including deception detecting AI and micro-expression analysis software.

**AI in Judicial Decision-Making**

AI's involvement in judicial decision-making[90], even when it acts only as a decision support system and not as a decision maker itself, poses the most constitutionally and juridically complex issues. In India, the SUPACE (Supreme Court Portal for Assistance in Court's Efficiency) system of the Supreme Court, which uses artificial intelligence, provides assistance to judges in finding relevant judgments, extracts facts from pleadings, and finds precedents. It should be noted that the Supreme Court always insists on presenting SUPACE as an 'artificial intelligence tool that does not take decisions' and only 'assists in information gathering.'

Nevertheless, there is a thin line between these two functions of an AI system, as it becomes more complicated. This issue can hardly be regarded as purely speculative. When a judge uses suggestions made by an AI system or the summary provided by it, this choice automatically

[86] Bharatiya Sakshya Adhiniyam,2023
[87] Selvi v. State of Karnataka, (2010) 7 SCC 263
[88]Selvi v. State of Karnataka, (2010) 7 SCC 263
[89]The Constitution of India, 1950
[90]Frank Pasquale, The Black Box Society (2015)

becomes a factor that influences the judicial outcome. In case such an AI system shows signs of bias in its algorithms either because of the biased data used or simply because of how it was designed, the judicial process will be affected accordingly.Right to a reasoned decision is an essential part of the guarantee of a fair procedure under Article 21, according to the decision of the case of Mohd. Arif alias Ashfaq v. Registrar, Supreme Court of India (2014), where the court ruled that absence of reasoned decisions is unconstitutional. In cases where an AI system influences the outcome of litigation, litigants have the right to know about such influence and understand the process behind the inputs given by the AI system, along with their right to challenge any mistakes or prejudices that the AI system might have shown. Algorithmic transparency becomes a must for this and none of the presently available AI systems in judiciary possess it.

The American example of the application of COMPAS provides insight into the issue. The Wisconsin Supreme Court in State v. Loomis (2016) allowed for the use of COMPAS scores at sentencing but under stringent terms, one of them being that the score cannot be the determining factor and that the method behind calculating it should be made known to the parties concerned. However, due to the commercial ownership of the COMPAS algorithm, the defendant was unable to challenge the methodology.

**AI in Bail and Sentencing Decisions**

India's bail jurisprudence, which has undergone a significant overhaul in light of the introduction of specific bail-related provisions in the Bharatiya Nagarik Suraksha Sanhita 2023, is still highly discretionary and open to bias. Algorithms that assess flight risk, danger to community, and propensity to commit an offence have been proposed as a tool to curtail discretion[91] in the bail process and to generate more predictable results.

Nevertheless, this use of algorithms should be considered in light of the Supreme Court decision in Arnesh Kumar v. State of Bihar (2014), where strict guidelines were laid down for the arrest and detention process to protect Article 21 right and the overarching constitutional requirement

[91] Arnesh kumar v. state of bihar, (2014) 8 SCC 273

of individualisation[92] of the deprivation of liberty. The problem with an algorithmic approach is that an algorithm will make predictions based on group characteristics, such as high probability of flight from particular social backgrounds and regions, and thus impact differentially on marginalised communities even in the absence of overt discriminatory intent.

Moreover, any AI tool used in bail or sentencing decisions must comply with the principle of individualisation established in Bachan Singh v. State of Punjab (1980) and Mithu v. State of Punjab (1983), which require that punishment be calibrated to the specific facts and circumstances of the individual offender. An algorithmic system that reduces the individual to a data point and assigns risk scores based on statistical correlations is fundamentally at odds with this constitutional mandate.

**AI in Prison Management and Rehabilitation**

AI uses in prison administration include behavioral monitoring programs, systems to match prisoners with rehabilitation programs, risk assessment for making early release determinations, and predictions of prisoners likely to attempt suicide or indulge in violence. All of these use cases have their unique problems connected to dignity, custodial privacy, and release procedures.

According to various Supreme Court rulings in the cases like Sunil Batra v. Delhi Administration (1978) and Francis Coralie Mullin v. Administrator, Union Territory of Delhi (1981), the fact remains that prisoners are still entitled to fundamental rights even when they are incarcerated, with all the right to human dignity[93] and good health. Behavioral monitoring using AI continuously can reduce inmates to mere targets of algorithmic management without respecting their rights as humans requiring humane treatment.

**Algorithmic Bias and Structural Inequality**

Undoubtedly, one of the most basic issues raised by the use of artificial intelligence within the Indian context of criminal justice is that of algorithmic bias[94], which refers to the existence of systematic and unreasonable differences in the outcome of operations conducted through an AI-

[92]Bachan Singh v. State of Punjab, (1980) 2 SCC 684
[93] Sunil Batra v. Delhi Administration (1978) 4 SCC 494
[94] Cathy O'Neil (2016)

based process to the detriment of certain groups of people. As far as the Indian criminal justice system is concerned, there is evidence of the over-policing of Dalits, Muslims, Adivasis, and poor people in terms of the available historical data.

From the constitutional perspective, one can argue that the use of an AI-based system for producing outcomes of an arbitrary and discriminatory nature would be unconstitutional based on Article 14[95], since such action would constitute a violation of the principle of reasonable classification stipulated in Article 14 of the Constitution through the 'intelligible differentia' requirement. Thus, any classification, including algorithmic classification, must have a rational nexus to a legitimate governmental purpose**.**

**The Legal Vacuum: Regulatory Gaps in India**

At present, India has no legislation that regulates AI within the criminal justice system. The legislation currently available, although extensive in many ways, is far from sufficient for effective regulation of AI. In particular, the Information Technology Act 2000, designed to regulate e-commerce and cybercrime, does not offer any provisions regarding governance of artificial intelligence technologies. The more recent legislation – Digital Personal Data Protection Act 2023 – represents considerable progress in data protection; however, it only addresses issues of consent-based processing of personal data and cannot tackle the dangers associated with AI processing in law enforcement context where processing is always done against individual will.

Finally, three new criminal procedure codes, Bharatiya Nyaya Sanhita 2023, Bharatiya Nagarik Suraksha Sanhita 2023, and Bharatiya Sakshya Adhiniyam 2023, represent the first comprehensive modernization of India's criminal procedure system since independence; however, although these laws regulate electronic evidence, digital investigations, and proceedings in online space, they include no provisions regulating application of AI in any criminal procedure processes.

[95] The Constitution of India, 1950

The Government of India through its Ministry of Electronics & Information Technology (MeitY) has put out an initiative called the "Responsible AI Framework" and has also been involved in AI governance internationally by endorsing the G20 AI Principles. The problem with all these documents is that they are aspirational in nature and lack legal backing. The emphasis in the National AI Strategy released by NITI Aayog is more towards the economic opportunities offered by AI rather than addressing any risks related to AI usage in areas like criminal justice.

## CHAPTER 5 – COMPARATIVE ANALYSIS ON NATIONAL AND INTERNATIONAL PERSPECTIVES

Comparative Perspectives

The Artificial Intelligence Act of the European Union (EU), coming into effect from 2024 onwards, is the most stringent and comprehensive legislation regulating the use of AI across the globe and serves as a useful template for Indian lawmakers to learn from. The EU AI Act[96] is based on a risk assessment[97] mechanism, according to which AI systems are categorized in terms of unacceptable risk (and therefore prohibited), high risk (requiring stringent regulation), limited risk (requiring transparency measures) and minimal risk (no restrictions at all). Law enforcement, criminal justice and immigration management operations fall within the category of high-risk AI activities and are subjected to such conditions as conformity assessment, technical documentation, human supervision, accuracy testing and post-market monitoring.

Moreover, the EU AI Act explicitly prohibits the use of certain AI practices altogether, like using real-time biometric identification[98] systems in public areas by law enforcement[99] services (except in the case of certain serious offences). This shows that the approach adopted by the EU in its legislative document is far more rigorous and precautionary in nature compared to what is currently taking place in India through unregulated use of facial recognition in public spaces[100].

[96] European Union, AI Act 2024
[97] State v. Loomis (2016)
[98] European Union, AI Act (2024)
[99] EU Fundamental Rights Agency, Facial Recognition Report (2020)
[100] European Parliament Reports on AI Regulation (2023)

Whereas the British example with the implementation of the Algorithmic Transparency Recording Standard (ATRS)[101], which demands that public bodies[102] publish data regarding algorithm usage in decision making transparency[103], provides a stepwise strategy that could be more realistic for India, several cities in the US, such as San Francisco, Oakland, and Boston, have introduced a ban on facial recognition technology in government operations. This highlights the increasing understanding that there are instances when it is better to regulate than to innovate too soon.

**National Perspective**

The use of Artificial Intelligence technologies in the process of work of the criminal justice system in India is at an initial stage. The government authorities use different types of technologies, such as facial recognition and the use of predicting policing, for increasing the efficiency of investigation and preventing crimes. It should be noted that technological innovations, including facial recognition and crime maps, show the tendency to apply technological means. However, these innovations remain more administrative than legislative ones.

Thus, it can be concluded that the problem of the use of artificial intelligence in India includes the absence of uniform mechanisms for regulating their use. There is no special legislation regulating the activities related to the implementation of artificial intelligence technologies in practice. Thus, the issue of the lack of sufficient attention to the problem of algorithm transparency, accountability, and data protection has emerged because there is no legislative regulation.

From the perspective of constitutional law, the utilization of Artificial Intelligence can be reviewed under the case of Justice K.S. Puttaswamy v. Union of India. In this regard, it becomes clear how crucial privacy and security become for citizens. Meanwhile, it should be mentioned that at the moment there is almost no case concerning the usage of artificial intelligence during criminal proceedings.

[101]UK Government, Algorithmic Transparency Standard (2021)
[102]UK Cabinet Office Report (2021)
[103]OECD, AI Principles (2019)

As a result, another barrier that can take place during implementing the use of artificial intelligence in the criminal process is poor institutional readiness[104]. To achieve success while using artificial intelligence, it is important to have qualified workers and solid databases. Moreover, some guidelines should be formed as well. At the same time, it is evident that poor institutional readiness poses a threat to improper technology usage.

**International Perspective**

In contrast to the Indian scenario, there have been successful efforts to implement artificial intelligence in the criminal justice system of many developed nations alongside solving some of the problems associated with the same.

Some of the applications of artificial intelligence in the criminal justice system of America relate to predictive policing and risk assessments. In essence, algorithms are applied to determine whether a particular person poses a risk to commit any crime in the future and help decide whether the accused would be placed under probation or subjected to certain punishment. The application of such algorithms, however, has been criticized for its inherent bias as per past data. One such case involves the use of risk score algorithms as was highlighted by State v. Loomis (2016), where the defendant was unable to argue against his risk score owing to opaque algorithms.

Similarly, in the United Kingdom, the use of artificial intelligence in the form of facial recognition technology has been quite successful in making predictions. However, the problem of inaccuracy persists owing to false identification[105] of criminals resulting in arbitrary detention[106] of suspects.

[104]World Bank, AI Readiness Index (2020)
[105]NIST Report (2019)
[106]ICCPR, 1966

The European Union adopted a safer and more human-oriented approach in its regulatory practices by concentrating on rights-based regulation[107] of AI technologies. This approach entails the formulation of an all-encompassing model of regulation based on classification of the different categories of AI technologies depending on the risk level, and imposing binding obligations for high-risk applications, including those involving use of AI technologies in criminal law enforcement processes.

Furthermore, the Indian nation must also take into consideration yet another important aspect, and this is related to legal liability of AI technology application. International examples clearly illustrate the fact that in order to control the situation effectively, there should be some form of liability for wrong decision-making.

Algorithmic Governance vs Rule of Law

One other issue in comparative analysis would be the change from the rule of law[108] to something like 'algorithmic governance[109]'. The processes of decision making are increasingly becoming less dependent on human reason and increasingly dependent upon computer algorithms in international jurisdictions. There arises a need for determining if the governance structure in this case is driven by law or technology. Given the fact that rule of law forms an essential part of the Indian constitution, the issue should definitely be examined critically.

Threat of "Technological Determinism"

Another significant factor that needs mention here is the growing belief that technology surpasses the importance of human decision-making. Technological determinism[110] holds that technology is always more accurate and objective than humans. Yet, based on global experiences, it has been observed that artificial intelligence algorithms can replicate and even perpetuate biases. Human discretion will still be essential for India's criminal justice system.

Necessity of Independent Regulatory Mechanism

[107]European Union, AI Act (2024)
[108]A.V. Dicey, Introduction to the Study of the Law of the Constitution
[109]Frank Pasquale, Black Box Society (2015)
[110]Langdon Winner, Autonomous Technology (1977)

Looking at the experiences of many countries internationally, it is quite evident that it is necessary to have an institution that will oversee and regulate the use of Artificial Intelligence. In many nations, bodies have been set up to monitor AI use, manage ethical issues[111], and address complaints against AI use. At the moment, India's criminal justice system does not have an institution like this one.

Certification of AI Applications in Criminal Justice System

There is another issue related to non-standardized applications of AI that arises through the comparison of national laws. It has been observed through different conversations that the testing of AI applications should be done before applying them into practical life. This ensures that no ethical norms are violated by using any system.

Effect on Democratic Accountability

The usage of AI could even affect democratic accountability as well. Under traditional scenarios, there is always an opportunity to challenge the decision made by the relevant government authority. However, it becomes difficult to challenge those decisions if it is made on the basis of algorithmic calculations. Many issues related to the subject matter have been debated within the international literature. It becomes imperative for the Indian government to keep up with this factor even after adopting AI.

Need for AI Legislation in the Future

One of the significant aspects taking into consideration the current international scenario is that there should be legislation for AI in the future. The existing laws do not cater to the special issues that arise due to AI. Many countries are considering legislation as one of the methods to deal with these issues. In addition, India should concentrate on legislations in relation to criminal law.

**Determination of Comparative Analysis**

[111]EU Ethics Guidelines (2019)

From the comparison analysis, it is clear that while the use of Artificial Intelligence may transform the entire criminal justice system, the misuse of Artificial Intelligence[112] might create serious constitutional concerns. Therefore, there needs to be adoption of technology within India but with proper consideration of law. From lessons from other countries and by ensuring that the policies comply with the Constitution, India would definitely benefit from the use of Artificial Intelligence in the criminal justice process.

## CHAPTER 6- FINDING,CHALLENGES AND OBSERVATIONS

### FINDINGS, CHALLENGES AND OBSERVATIONS

**From the analyses performed in the above sections, it becomes clear that:**

There is increasing use of AI[113] in the criminal justice system in India without any regulation thereof. There is deployment of facial recognition technology[114] by multiple state police agencies without compliance with mandatory transparency requirements, risk assessments, or any accountability mechanisms. The deployment shows a desire by the institution to rely on technology to solve structural issues without regard to the constitutional and human rights concerns raised by such deployment.

The Automated Facial Recognition System (AFR System) being introduced by the National Crime Records Bureau is unconstitutional. First, there is no specific law authorizing its use,

[112]NITI Aayog (2018)
[113]NITI Aayog, National Strategy for Artificial Intelligence (2018)
[114]Internet Freedom Foundation, Project Panoptic (2021)

secondly, it does not pass the test of proportionality[115] set out in Puttaswamy v Union of India and finally, it will be a case of mass surveillance violating the right to privacy[116] guaranteed by Article 21 of the Constitution.

Algorithmic discrimination[117] is a systemic problem that could undermine efforts towards equality in the criminal justice system. AI models trained using the criminal justice data generated over many years in India may end up being discriminatory against minority groups such as Dalits, Muslims, and Adivasis. It would amount to a possible violation of Article 14[118] which the government cannot justify without proving the effectiveness of debiasing techniques on the AI model.

There is no discussion about AI in the three criminal codes[119]passed by the Parliament in 2023. Though the new codes cover all aspects of substantive and procedural criminal law in great detail, the omission of any mention of AI from them means that there is an area of criminal justice norms that needs judicial interpretation.

SUPACE[120] is a project initiated by the Supreme Court of India using which the judges and lawyers can benefit from the use of AI while conducting legal research or managing cases. Nevertheless, as AI-based judicial tools become more advanced in the future, clear guidelines are going to be essential.

India has an opportunity to learn from these experiences and adopt a proactive rather than reactive regulatory posture.It goes without saying that the current legal and regulatory system in India is totally unsuited to the task of regulating the use of AI in the field of criminal justice. Neither the Information Technology Act 2000[121], nor the DPDP Act 2023[122], and even the new criminal laws can be considered suitable and proportionate regulatory systems necessary for the safe implementation of the use of AI technology in criminal justice processes.

[115]Puttaswamy v. Union of India, (2017)
[116]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[117]Julia Angwin et al., “Machine Bias”, ProPublica (2016)
[118]The Constitution of India, 1950
[119]Bharatiya Nyaya Sanhita, 2023
[120] Supreme Court e-Committee Report
[121]European Union, AI Act (2024)
[122]Digital Personal Data Protection Act, 2023

There are positive instances of AI being used in the criminal justice process in India. For example, AI can be quite effective for forensic analysis, helping manage criminal cases, conducting research to facilitate a lawyer's job, optimizing schedules of trials, and also making documents in the courts available in different languages, which would help victims of crime more efficiently.

It is clear from international experience that preemptive regulation[123] is much more effective than the regulation of artificial intelligence technologies in the field of criminal justice after their harmful effects become apparent. This conclusion follows from such examples as the EU AI Act, American bans on facial recognition implemented at the municipal level, and algorithmic transparency regulations implemented in the UK.

## CHAPTER 7- CONCLUSION, SUGGESTIONS AND RECOMMENDATIONS

### Suggestions and Recommendations

Based on the foregoing analysis, the following suggestions are proposed:

**Implementation of an Artificial Intelligence (Regulation) Act**: The parliament ought to enact a detailed law regarding the management of AI technology following the risk-based framework used in the EU AI Act. The AI technology used in criminal justice must fall under high-risk systems[124] and be subjected to pre-implementation conformity assessment, algorithmic impact assessment that includes bias analysis, documentation, human supervision, and effective post-deployment monitoring methods. Some AI technologies, such as live biometric mass surveillance of general publics, must not be used at all.

[123]European Union, AI Act (2024)
[124]EU AI Act (2024)

**Algorithmic Transparency**: Any AI technology implemented within the criminal justice sector must be made transparent by ensuring the objectives and functions of the technology are revealed, the data used in training the AI technology is revealed, the accuracy of the technology for different demographic groups is made available, any validation measures taken are revealed, and the limitations of the technology are known. Contractual terms between the vendors and the government when purchasing AI technologies must include the requirement of explainability and auditability while preventing proprietary opacity.

**Statutory Regulation of Use of FRT**: The use of facial recognition technology[125] in law enforcement would require statutory authorization and must fulfill the requirement of the Puttaswamy proportionality test[126]. Statutory regulation needs to state the purpose for the use of FRT, the need for judicial authorization for its use, standards that need to be fulfilled prior to the deployment of such technology with special emphasis on different demographic groups, and also remedies for any wrongful identification done using this technology.

**Amendment of Criminal Procedure Codes with regard to AI**: Amendments are needed in Bharatiya Nagarik Suraksha Sanhita[127] and Bharatiya Sakshya Adhiniyam[128] regarding the utilization of artificial intelligence in investigative, prosecutorial, and adjudicative process. These amendments must include the rules regarding admissibility of AI evidence, expert testimony concerning AI methodologies, right to information about AI system used in case of the accused, and the duty of judges to conduct careful review of all AI-related cases.

**Independent Regulatory Body for AI Deployment**: India needs to set up an independent regulatory body[129] that will have the responsibility to regulate the application of AI in the areas where it carries high risks, such as criminal justice. The body should have the power to conduct audits, investigate complaints, give guidelines, impose sanctions for non-compliance, and conduct consultations with the stakeholders before implementing AI applications.

[125]Internet Freedom Foundation, Project Panoptic (2021)
[126]Puttaswamy v. Union of India, (2017)
[127]BNSS, 2023
[128]BSA, 2023
[129]OECD AI Governance Framework (2019)

**Human Oversight in AI-Assisted Criminal Justice Decision-Making Processes**: Any final decision regarding a person's life in criminal justice processes that has serious consequences cannot be made purely based on AI recommendations without human oversight. This human oversight must not be superficial but should entail substantial human intervention[130] in the process of decision-making. The individuals involved in decision-making must be equipped with the ability to analyze AI recommendations, receive adequate information to enable them to independently make their judgments, and exercise their right to overrule AI outcomes.

**Requirement for Regular Bias Auditing and Bias Remediation**: If any AI system is put into use within the criminal justice context, such systems need to be audited for biases, which can lead to disparate impacts on any protected group according to the constitution. In case of detection of bias in the AI tool, its usage needs to be stopped until the bias issue is resolved or if not possible to be resolved, then it needs to be stopped altogether. Audit outcomes need to be disclosed publicly. The state needs to invest in technical capabilities of oversight authorities to conduct audits.

**Development of Rights-Friendly AI**: India must direct public funds for research and development of AI solutions that are developed for the Indian constitution, demographics, including debiasing methods in the process of AI development, making AI systems explainable, and development using diverse datasets. Law schools need to collaborate with computer science departments, civil society organisations, and the government for continuous rights impact assessment while designing AI systems for criminal justice.

**Judicial Education and Awareness**: The Supreme Court and High Courts need to create educational programs regarding AI technology and its abilities, the dangers associated with AI, the potential risks of algorithmic bias, and the constitutional requirements that govern decisions assisted by AI. Any judge who employs the help of AI in his/her judicial proceedings needs to undergo such education and should also be advised not to rely blindly on the assistance of AI. Judicial independence of the judiciary from the influence of both the executive and vendors is crucial.

[130]UNESCO, AI Ethics Recommendation (2021)

## Conclusion

AI as a technological innovation in India's criminal justice system[131] creates an apparent paradox which, however, can serve both as a defining opportunity as well as a massive challenge for India. AI could prove to be extremely useful in overcoming inefficiencies, delays[132], lack of forensic science infrastructure, and discrimination in the justice system, and yet its unregulated deployment could result in reinforcing biases, undermine individual rights and freedoms, and subvert human dignity to the principle of efficiency.

As has been discussed above, the resolution to this apparent paradox should not consist in a choice between embracing technological development or respecting civil liberties, but rather in ensuring that AI technologies are regulated in accordance with legal frameworks embodying the principles of India's constitution. In this context, the Constitution of India has proven to provide a wealth of guidance for regulating the use of AI, as it guarantees the protection of citizens' rights to equality, liberty, privacy, and dignity in Articles 14, 19, 21, and 22.

The analysis demonstrates that India currently lacks the regulatory infrastructure[133] necessary to govern AI in criminal justice responsibly. The three new criminal codes of 2023[134], while representing significant substantive reform, fail to address AI. The DPDP Act 2023[135], while improving data protection standards, does not adequately address law enforcement data processing. This regulatory vacuum must be urgently addressed.

At no point in time have there been higher stakes. With AI becoming increasingly advanced and more commonplace in criminal justice processes, the time is fast running out for implementing governance frameworks that will safeguard the rights of individuals. Indeed, the experiences of both the US[136] and China[137], with the former having seen AI contribute to racism in risk assessment tools and the latter being an example of the use of AI surveillance by a repressive

[131]Upendra Baxi, The Crisis of the Indian Legal System (1982)
[132]NCRB, Crime in India 2022 (2023)
[133]NITI Aayog, National AI Strategy (2018)
[134] Bharatiya Nyaya Sanhita, 2023
[135]Digital Personal Data Protection Act, 2023
[136]State v. Loomis (2016)
[137]Human Rights Watch, AI Surveillance Report (2019)

state, highlightthe pressing need for the Indian government to establish a regulatory structure for AI in criminal justice prior to the process becoming irreversible.

## REFERENCES

### Cases


- Puttaswamy vs Union of India, (2017) 10 SCC 1.
- Maneka Gandhi vs Union of India, (1978) 1 SCC 248.
- Selvi vs State of Karnataka, (2010) 7 SCC 263.
- Bachan Singh vs State of Punjab, (1980) 2 SCC 684.

- Arnesh Kumar vs State of Bihar, (2014) 8 SCC 273.
- Francis Coralie Mullin vs Administrator, Union Territory of Delhi, (1981) 1 SCC 608.
- Sunil Batra vs Delhi Administration, (1978) 4 SCC 494.
- Mohd. Arif alias Ashfaq vs Registrar, Supreme Court of India, (2014) 9 SCC


**B. Legislation**


The Constitution of India, 1950.

The Bharatiya Nyaya Sanhita, 2023.

The Bharatiya Nagarik Suraksha Sanhita, 2023.

The Bharatiya Sakshya Adhiniyam, 2023.

The Information Technology Act, 2000 (as amended in 2008).

The Digital Personal Data Protection Act, 2023.


**C. Books and Articles**


- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). 'Machine Bias.' ProPublica.
- O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishers.
- Brayne, S. (2020). Predict and Surveil: Data, Discretion, and the Future of Policing. Oxford University Press.
- Buolamwini, J. & Gebru, T. (2018). 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.' Proceedings of Machine Learning Research.
- Garvie, C., Bedoya, A., & Frankle, J. (2016). 'The Perpetual Line-Up: Unregulated Police Face Recognition in America.' Georgetown Law Center on Privacy and Technology.
- Narayan, S., & Roy, A. (2021). 'Predictive Policing in India: An Empirical Assessment.' Journal of National Law University, Delhi.
- Singh, P. (2022). 'Facial Recognition Technology and the Right to Privacy in India.' NUJS Law Review, 15(3).

- Chandrachud, D.Y. (2020). 'Artificial Intelligence in the Indian Courts.' Supreme Court Journal.
- Internet Freedom Foundation. (2021). Project Panoptic: Mapping Facial Recognition Projects in India. IFF Publications.
- European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- NITI Aayog. (2021). Responsible AI for All: Adopting the Framework. Government of India.
- National Crime Records Bureau. (2023). Crime in India 2022.