ARTIFICIAL INTELLIGENCE IN FORENSIC IDENTIFICATION: MANEUVERING THE CHALLENGES AND TRAVERSING THE OPPORTUNITIES WITHIN THE FRAMEWORK OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

Hasrat Boparai, Research Scholar, Department of Laws, Panjab University, Chandigarh.

Satwinder Singh, Master of Laws, University Institute of Legal Studies, Panjab University, Chandigarh

ABSTRACT

The application of Artificial Intelligence (AI) into forensic identification processes heralds a transformative shift in the landscape of administration of the criminal justice system, primarily under the Criminal Procedure (Identification) Act, 2022, with far-reaching implications in conjunction with its conspicuous opportunities. This paper critically examines the multifaceted facets of AI application within the criminal justice system in winching the accuracy, efficiency, and adaptability of "forensic identification procedures," such as biological examination, fingerprint analysis, facial recognition, and biometric profiling. Within Indian criminal justice system, the perspicacious application of AI modus operandi, such as machine learning (ML) and deep learning (DL) algorithms, has much potential to tremendously assist in intelligent identification of persons for the acceleration of criminal identification and investigation in criminal cases, which would subsequently intensify the accuracy and precision of evidentiary interpretation exceptionally in cases of circumstantial evidence where further identification and investigation is deemed necessary. Through the automation of repetitive tasks, such as face recognition, image analysis and data processing, AI can manumit forensic scientists from time-consuming drudgery, enabling them to devote their expertise to trickier and intellectually stimulating criminal matters. Moreover, AI-powered tools can briskly expedite the identification of subtle patterns and anomalies that may elude human perception, unsealing novel avenues for investigative inquiry in criminal cases. With the utilization of AI, law enforcement agencies could potentially accelerate the identification of suspects and victims, aggrandizing all-inclusive investigative prowess. Yet, the application of AI within the system requires a cautious and circumspect approach inter-alia, establishing the acceptable rigorous framework for the successful amalgamation of such

novel technologies, identifying and cultivating stakeholder engagement and concurrently fostering collaborative partnerships to facilitate their optimal development, cognizant of the potential pitfalls and legal, ethical and technical quandaries that may arise. Furthermore, the Criminal Procedure (Identification) Act, 2022, while groundbreaking in its endorsement of technological progress, demands a perceptive interpretation to guarantee that its provisions are in conformity with the fundamental rights of individuals, incorporated within the inviolable Constitution of India.

Keywords: Artificial Intelligence, Forensic Identification, Investigation, Criminal Justice System.

I. INTRODUCTION

The augmentation of artificial intelligence[1] has radically swayed myriad dimensions of our society in an unprecedented manner:[2] spanning from the civil justice system to the criminal justice system to justice delivery mechanism[3] and forensic science,[4] the application of this novel technology appears to be perpetually escalating in India.[5] Considering the rapid metamorphosis and extensive magnitude of the same, alongside lack of transparency and accountability associated with numerous applications,[6] adoption and implementations of novel AI tools, their implications are frequently of paramount importance which must be acknowledged and addressed immediately before it is too late in regard to fundamental rights such as equality, discrimination, personal liberty, and fair trial, within the Indian justice system. Within the context of the Criminal Procedure (Identification) Act, 2022 (hereinafter referred to as CP Act), this paper examines the story of use of "Artificial Intelligence in Forensic Identification," which is considered to be both promising and perilous.[7] As a young legal researcher, we both aim to promote "Responsible AI" for our justice delivery mechanism through a comprehensive legal, regulatory, and ethical framework in order to establish

[1] The term was initially introduced by the American pioneer in computer science, John McCarthy, in the year 1955. Artificial Intelligence (AI) AI is a branch of computer science that focuses on creating computer systems and software that can perform intricate tasks.
[2] Yadong Cui, *Artificial Intelligence and Judicial Modernization* (1st edn, Springer, Singapore 2020)
[3] Alfonso Renato Vargas-Murillo and others, 'Transforming Justice: Implications of Artificial Intelligence in Legal Systems' (2024) 13 AJIS 433
[4] Eman Ahmed Alaa El-Din, 'Artificial intelligence in forensic science: invasion or revolution?' (2022) 10 ESCTJ 20
[5] Jacob Koshy and Sandeep Phukan, 'Can Artificial Intelligence, Machine Learning put judiciary on the fast track?' *The Hindu* (New Delhi, 06 March, 2022) <https://www.thehindu.com/news/national/ai-ml-are-a-long-way-from-becoming-a-judicial-decision-making-tool/article65193656.ece> accessed 12 January 2024.
[6] Nagadivya Balasubramaniam and others, 'Transparency and Explainability of AI systems: From Ethical Guidelines to Requirements' (2023) 159 IST 107197
[7] Christopher Rigano, 'Using Artificial Intelligence to Address Criminal Justice Needs' (2018) NIJ 37

legitimacy of these technologies among masses.

This paper offers two primary contributions to the pre-existing body of scientific literature, specifically within the field of medico-legal discourse, which is intended to be a worthwhile resource for the application and integration of AI within the justice delivery mechanism and as an introductory resource for key stakeholders, encircling judges, judicial officers, litigants, and law enforcement agencies, including police personnel.

First, it provides a baseline taxonomy of the prospects and detriments mingled with AI, incorporating only minimal allusions to the Indian regime, which potentially highlights injustice as well as inequities, delineating not only the prospects and detriments in their quintessence but also expounds on the intricate technical mechanisms that buttress these advantages and adversities.

Second, it describes our perspective of how existing AI tools—including specifically Section 3 and 4 of the CP Act, can and ought to be savagely applied to address and thwart discrimination, inequalities, and injustices, and also could help significantly contribute to systematically ameliorating the detrimental effects engendered by AI decision-making processes.

II. BRIDGING GAPS IN JUSTICE: THE EVOLVING ROLE OF AI IN FORENSIC IDENTIFICATION

The criminal justice system has tenaciously constituted one of the most propitious AI domains since the consecration of AI as a bona fide academic domain of intellectual pursuit, which could be attributable to a greater availability of heterogenous data sets, increased computational power and more evolved mathematical algorithms that can further be used to extract valuable insights from data which would otherwise be difficult for humans to perform these tasks alone and the AI-assisted tools, in turn, can aid in pre-emption of criminal offenses and the maintenance of public tranquillity while also allowing AI system to function sui generis.[8] Owing to the inherent applicability in criminal and civil applications, along with their vast potential in ameliorating the justice delivery mechanisms, having been recognized, the Indian Government is currently exploring a variety of strategies to have computational assistance for

[8] Kelly Hannah Moffat, 'Algorithmic risk governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates,' (2018) 23(4) Theor. Criminol. 453.

officials from investigating agencies who are tasked with duty in carrying out investigation further to detect heinous crimes.[9] It should be noted here that while application of AI in the system has only taken off in the last 8 years in India,[10] it has been in existence worldwide in countries like Argentina,[11] China,[12] Finland,[13] Japan,[14] South Africa,[15] and the United States,[16] for decades even before the Government of India decided to chalk out its strategies for the system.

In India, the integration and use of AI in the system has been strongly influenced by several challenges such as corruption in police administration, a huge backlog of cases, lack of accountability and transparency, overcrowded prisons, poor quality of investigations, police and public mistrust, and shortage of police personnels, judges, and forensic scientists, and thus has seen extensive involvement from both the Union and the State Governments for its application in various different operations within the system. However, the questions remain – What is the current role of AI in forensic identification? Does it truly enhance the efficiency of our Criminal Justice System or is its impact still limited by other intricate factors involved therein?

This question becomes especially relevant, in age of technology and absence of essential legal framework, where measurements including biometric profiling, biological samples and so on have to be collected under specific laws, such as the BNSS, the CP Act, the Digital Personal Data Protection Act etc., wherein the former two are partially tilted in favour of executive by granting law enforcement agencies the power to collect such measurements or data even in absence of consent of an accused in exceptional cases, while the later emphasis on data to be

[9] NITI Ayog, 'National Strategy for Artificial Intelligence #AIFORALL' (*NITI Ayog,* June 2018) <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>accessed 28 January 2025.
[10] Ibid.
[11] Zachary Amos, 'How Countries Are Using AI to Predict Crime' (*Swiss Cognitive* 23 December 2024) < https://swisscognitive.ch/2024/12/23/how-countries-are-using-ai-to-predict crime/#:~:text=The%20United%20States%20and%20South,this%20technology%20into%20their%20policing> accessed 26 January 2025.
[12] Changqing Shi and others, 'The Smart Court – A New Pathway to Justice in China?' (2024) 12(1) IJCA 1.
[13] Pia Puolakka, 'Smart Prisons and Artificial Intelligence Systems Expand in Finland' (*Justice Trends* 26 April 2023) < https://justice-trends.press/smart-prisons-and-artificial-intelligence-systems-expand-in-finland/#:~:text=Pia%20Puolakka,women's%20facility%20housing%20100%20inmates> accessed 23 January 2025.
[14] Kaie Hamaguchi, 'AI Governance and Initiatives for Implementing AI Systems in Law Enforcement: Introduction of the Interpol/UNICRI Toolkit and its Implications for Japan' (*The University of Tokyo* 20 November, 2023) < https://www.tc.u-tokyo.ac.jp/en/ai1ec_event/10769/ > accessed on 19 January, 2025.
[15] Zachary n (11).
[16] Ibid.

collected with the consent of data principal, and data related to criminal activities, which may be collected and be disclosed without the consent of the accused.

If AI is touching everything in our modern life including administration of justice, then it is inconceivable that it would exclude the criminal justice system. When it comes to the current role of AI in forensic identification, there are certain crucial aspects of AI that make it particularly useful within the justice system. For instance, AI, in crime scene analysis, can meticulously analyze data from various sensors to detect, predict, and even interpret details of crime scene, which not only reduce the traditional painstaking process but also make the facts of a crime clearer, subsequently making the evidence more reliable and sufficient.[17] And, for this purpose, Named Entity Recognition (NER), entity relation analysis, and machine extraction and manual annotation can be used in trials to review and judge evidence chain and evidence of the whole in both criminal or civil cases.[18] This, as one can imagine, will be massively useful in not only in identification but also in court trails, where prosecution may usually fail to establish a case due to absence of sufficient evidence due to poor quality of investigation. Additionally, AI can be used, with the help of Deep Neural Network (DNN), to pinpoint defects in evidence during forensic identification in high-profile cases, making it useful for such stakeholders to pay their attention during the trial and verify the relevant information.[19] Already, AI-enabled tool has been employed in Shanghai Court with the intent to reduced huge pendency of cases and prevent wrongful convictions, thus positioning it as the pioneering judicial institution in China to fully adopt such technology within the framework of case management.[20] It is also being used in facial recognition and biometrics with the help of machine learning to decode the intricate nuances etched upon the human visage.[21] In addition, cyber-crimes domain is filled with complex issues and challenges that need to reckoned with. Consider difficulty in accurately identifying criminals due to the use of anonymizing tools like VPNs, Tor, and spoofed IP addresses, rapid loss or alteration of digital evidence, increasing use of encryption and advanced obfuscation techniques to hide criminal activities, difficulty in accessing and analyzing data stored in cloud environments, and use of anti-forensic tools and

[17] MA Sacco and others, 'The artificial intelligence in autopsy and crime scene analysis' 2024 175 Clin Ter 192.
[18] Yadong Cui, *Artificial Intelligence and Judicial Modernization* (Springer, Singapore 2019).
[19] Ibid.
[20] Jiang Wei, 'China uses AI assistive tech on court trial for first time' *China Daily* (China, 24 January 2019) < https://www.chinadaily.com.cn/a/201901/24/WS5c4959f9a3106c65c34e64ea.html#:~:text=Guide%20on%20evidence%20collection%20of,provinces%20and%20cities%20in%20China> accessed 21 January, 2025.
[21] Partha Pratim Sarangi and others (trs), *Machine Learning for Biometrics: Concepts, Algorithms and Applications* (Academic Press, 2022).

methods by criminals to erase, alter, or hide digital evidence.[22] It is an intricate puzzle that necessitates considering various factors – forensic experts from different domains, human power, etc. and potential changes in offence such as lack of standardized protocols. To thwart such intricate issues in forensic identification, behavioural analytics can be applied to develop and implement methodologies capable of robustly identifying and characterizing the complex, often subtle, behavioural variations that distinguish individuals, coalesce within groups, and ultimately shape population-level trends.[23] Beside these areas, AI is also being used in predictive policing to focus on less readily apparent crimes by training AI models that utilize extensive datasets derived from a multitude of heterogeneous sources. This enabled them to put more effort towards addressing illicit activities associated with white-collar offenses and the proliferation of cyber hate speech. Although we have enumerated the role of AI in forensic identification in a broad sense, it will be a formidable oversight to overlook a pivotal truth: AI-driven tools are best to be used *in conjunction* with human forensic scientists.

III. GOVERNMENTAL INITIATIVES IN AI ADOPTION: TRANSFORMING INDIA'S CRIMINAL JUSTICE SYSTEM THROUGH TECHNOLOGICAL INTEGRATION

The growing footprint of AI in India's justice delivery mechanism is becoming clearly evident. Illustrating this trend is the Telangana Police's pioneering Smart RoboCop, a sophisticated AI platform which has been introduced in 2017. More than just a mobile unit, this resourceful machine has been equipped with advanced sensors and GPS, serving as an ever-vigilant set of eyes and ears in crowded public spaces.[24] Its multifaceted role extends beyond simple surveillance. It can also proactively recognize suspects, accept formal complaints from the public, and even interact with people conversationally, offering a glimpse into a future where technology and law enforcement work hand-in-hand. That is to say, it is going to intertwine with each other. As a critical component of the justice system, law enforcement agencies are experiencing a profound and engineered shift toward technological integration. It has represented a strategic initiative to modernize the tools and methods used to enforce laws and ensure maintenance of law and order in the society. Spearheading this change, "Jarvis"

[22] Nickolaos Koroniotis and others, 'A New Network Forensic Framework Based on Deep Learning for Internet of Things Networks: A Particle Deep Framework' (2020) 110 FGCS 91.
[23] C.H. Ngejane and others, 'Digital Forensics Supported by Machine Learning for the Detection of Online Sexual Predatory Chats' (2021) 36 FSIDIIN
< https://www.sciencedirect.com/science/article/abs/pii/S2666281721000032 >accessed 28 January, 2024.
[24] Suresh Dharur, 'India's first 'Robocop' launched in Hyderabad' *The Tribune* (Hyderabad 30 December 2017) <https://www.tribuneindia.com/news/archive/nation/india-s-first-robocop-launched-in-hyderabad-521123/> accessed 27 January, 2024.

platform has been deployed by the State of Uttar Pradesh wherein the platform employs AI-driven video analytics to revolutionize prison management and inmate oversight.[25] Concurrently, the formidable "Trinetra" application, pioneered by start-up Staqu, is deploying an advanced facial recognition mechanism for police forces in multiple states, enabling field officers to swiftly identify criminals by tapping into a centralized database of images and documents. The entire system has been underpinned by the essential "Crime and Criminal Tracking Networks and Systems" (CCTNS), a critical network ensuring vital crime-related intelligence is disseminated among various departments. Complementing these State-led efforts, at the same time, private sector is playing a pivotal role; the "Artificial Intelligence Based Human Efface Detection" ABHEDA system is markedly enhancing police capacity by enabling immediate mobile-based offence registration and introducing biometric verification, a feature that fosters unprecedented operational accountability.[26] A formidable tool in modern law enforcement agencies, the National Automated Face Recognition System (NASRS) was launched by the Ministry of Home Affairs, utilizing complex algorithms to delve into a vast repository of facial data.[27] This system stands as a sentinel for justice, expertly engineered to unmask criminals by piercing through deliberate obfuscations like face coverings, cosmetics, or surgical alterations, and therefore give significant push to the standards for criminal identification and investigation within the system. In a parallel development, various States and Union Territories like Bihar, Chandigarh, Delhi, Gujarat, Haryana, Uttar Pradesh, and Telangana are also being fortified through the integration of similar facial recognition and complementary biometric solutions. These different AI-enabled mechanism adopted by various States assists investigating officers to effectively solve the intricate existing in the trial practice of either criminal or civil cases, such as preservation of crucial direct or circumstantial evidences, continuity of evidence, proper flow of information management, security to personal sensitive information, thus reducing the arbitrariness of the investigating agencies, judiciary and improving the quality of case handling. So, based on available sources, it is quite

[25] DC Correspondent, 'India\'s own JARVIS AI to monitor prison activities across 70 Indian jails Technology' *The Deccan Chronicle (New Delhi,* 07 November 07, 2019)

<https://www.deccanchronicle.com/technology/in-other-news/071119/indias-own-jarvis-ai-to-monitor-prison-activities-across-70-indian-ja.html> accessed 20 February, 2025

[26] Shubham Singh, 'This Gurugram-based startup is helping law enforcement agencies nab criminals with Artificial Intelligence' *CNBC TV18* (26 June, 2019) < https://www.cnbctv18.com/technology/this-gurugram-based-startup-is-helping-law-enforcement-agencies-nab-criminals-with-artificial-intelligence-3812261.htm> accessed 18 February, 2025.

[27] Vidhushi Marda, 'Facial recognition is an invasive and inefficient tool' *The Hindu* (27 July, 2019) <https://www.thehindu.com/opinion/op-ed/facial-recognition-is-an-invasive-and-inefficient-tool/article62109426.ece> accessed 15 February, 2025.

clear that the role of AI in the criminal justice system is gigantic.

IV. EXPLORING THE OPPORTUNITIES OF ARTIFICIAL INTELLIGENCE TO IMPROVE FORENSIC IDENTIFICATION PROCESSES

As we all know that the future of forensic identification isn't just about microscopes and test tubes anymore; it is now all about algorithms and data. We're on the brink of a new era where artificial intelligence (AI) can assist in some of the most challenging identification tasks. This section outlines the possibilities and benefits of integrating AI into our forensic processes, paving the way for smarter, more effective investigations.

A. ***Efficiency:*** AI accelerates and automates data processing, significantly improving the efficiency of forensic identification. Traditionally, forensic investigators must painstakingly sift through vast amounts of evidence, including fingerprint databases, surveillance footage, and DNA samples. Even though this procedure is comprehensive, it takes a lot of time and is prone to human errors. To ensure that detectives can match suspects to evidence rapidly, AI uses sophisticated ML algorithms to evaluate enormous datasets. While human detectives would need significantly more time to review video footage, facial expressions, and even micro-expressions, AI systems, especially those that use DL for image and video identification, can do so in seconds. Additionally, AI can cross-reference data from multiple sources, such as digital and physical evidence, to provide holistic insights, further enhancing investigative speed. The **National Automated Fingerprint Identification System (NAFIS)** is an advanced biometric technology developed to facilitate the efficient collection, storage, and analysis of fingerprint data for law enforcement agencies, judicial bodies, and national security institutions. The NAFIS initiative has greatly improved the efficacy and efficiency of criminal identification and investigation processes by creating a centralised database of criminal fingerprints that law enforcement agencies nationwide can access.[28]

B. ***Accuracy:*** AI intensifies the propensity to detect subtle patterns in biometric markers that are key to identifying suspects, such as facial features and fingerprint ridges. These algorithms can identify people even with incomplete or poor-quality biometric samples,

[28] PIB, 'National Automated Fingerprint Identification System (NAFIS)' *Government of India* (Delhi, 4 December, 2024).

allowing for quick, extensive comparisons against large databases with high accuracy. AI systems can examine and compare biometric data thousands of times faster than human experts, greatly reducing the chances of misidentification and scope for human error. In 2013, the Next Generation Identification (NGI) system implemented new latent capabilities, ultimately replacing IAFIS completely in 2014. This NGI system was developed and tested extensively and is maintained by the FBI's Criminal Justice Information Services Division. It is one of the largest biometric databases in the world and provides enhanced casework capabilities for latent prints, including searching palm prints.[29] In several high-profile investigations, artificial intelligence has transformed forensic identification globally. A recent initiative by the Government of Canada and the Royal Canadian Mounted Police (RCMP) to improve public safety measures has led to the nationwide digitalization of biometric records, enabling more efficient and accurate checks of both criminal and civil identities. The Department of National Defence (DND) of Canada is the latest to update its capabilities. Gemalto, a subsidiary of Thales, will implement the first Automated Fingerprint Identification System (AFIS) for DND, enhancing the security and dependability of fingerprint record collection and verification.[30]

C. ***Better Handling of Complex Data:*** One crucial component of contemporary forensic investigations is the processing of huge and complicated datasets, which AI excels at. Digital footprints, surveillance footage, social media data, DNA, fingerprints, and other forms of evidence are frequently processed by investigators. It might be difficult to analyze such data manually, particularly when comparing many databases. AI systems, particularly ML algorithms, are built to effectively handle and interpret massive amounts of information. AI is capable of automatically identifying faces in crowds, extracting important aspects from surveillance film, and even cross-referencing facial recognition data with databases throughout the country or other countries. Additionally, AI can identify new criminal activities or questionable behaviours by analyzing behavioural data, such as digital footprints or communication patterns.

[29] Kyle R. Tom, Kathryn B. Knorr and Christine E. Davis, 'Next Generation Identification system: Latent print matching algorithm and casework practices' [2022] 332 FSI.

[30] 'Canada Enhances Public Safety with Gemalto Fingerprint Identification Solution' (*Thales,* 9 May, 2019) <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/press-release/canada enhances-public-safety-with-gemalto-fingerprint-identification-solution > accessed 11 February 2025.

D. ***Cost Efficient:*** AI technologies can lower the total cost of investigations by automating repetitive forensic activities. Conventional forensic identification techniques can entail time-consuming and costly manual processes that involve reviewing vast volumes of data. On the other hand, AI can finish these jobs quickly and with little assistance from humans, which lessens the need for a large workforce. AI, for instance, can analyse and compare vast datasets far more quickly than human analysts in fingerprint analysis, which lowers the overall cost of matching suspects. Additionally, mundane jobs like picture scanning, object detection in movies, and even tracking criminal behaviour trends on social media may be handled by AI, freeing up human specialists to work on more complex tasks.

V. THE DOUBLE-EDGED SCALPEL: EXPLORING THE COMPLEX CHALLENGES OF AI-DRIVEN FORENSIC IDENTIFICATION

As noted above, the promise of AI in forensic science has been incredibly compelling, suggesting a future where human error is minimized and accuracy is extremely important. However, the reality of implementing these systems is proving to be far more complicated than we had initially envisioned. We will now be exploring the intricate challenges that have been emerging as AI takes on a more central role in forensic identification.

A. ***Data Quality and Availability:*** High-quality data is essential for AI systems to work efficiently.[31] Data must be precise, consistent, and unambiguous for forensic identification. However, in actual forensic investigations, the data are subject to inconsistency, incompleteness, and degradation owing to issues caused by improper collection practices or compromising difficulties such as image or sample resolution. For example, a fingerprint sample might be smudged or incomplete, or a facial recognition image might be blurry or taken from an unfavorable angle. Inaccurate outputs from AI algorithms trained on poor-quality data might result in misidentification or a failure to recognise important evidence. Moreover, forensic data is subject to many adherences' requirement, including strict chain-of-custody practices and incontestable procedures. Furthermore, reports and footage from different sources, such as video surveillance, biometric identification, and textual evidence, may not always conform or be standardized enough, further complicating the task of training robust AI models.

[31] Yashna Bawa, 'The Importance of High-Quality Training Data in AI' (*Mindkosh*, 13 July 2024) < https://mindkosh.com/blog/the-importance-of-high-quality-training-data-in-ai/ > accesses on 9 February, 2025.

B. ***Due Process and Privacy Concerns:*** AI-based forensic identification systems often require the collection and analysis of large amounts of personal data, such as facial images, voice recordings, or even behavioral patterns. This raises significant concerns about privacy and the potential for surveillance overreach.[32] Under the principles of due process, individuals must have control over how their personal information is collected, stored, and used. Without proper safeguards, AI systems could infringe on privacy rights by collecting data without consent or by using data for unintended purposes, such as expanding surveillance beyond its initial scope. Countries are struggling to strike a balance between protecting privacy and using AI for security. The United States and the European Union have been discussing methods to limit the use of technologies such as Automated Facial Recognition Technology (AFRT). San Francisco has passed a law mandating that governmental agencies specify the "necessary circumstances" that would justify the purchase and usage of AFRT.[33] In India, governmental actions that can violate a person's right to privacy are governed by the proportionality standard set by the Supreme Court in the *Puttaswamy* ruling.[34] According to this test, such interventions must be legally grounded, pursue a legitimate state interest, and include safeguards to prevent the misuse of state surveillance powers. However, the current deployment of AFRT appears to fall short of at least two of these criteria. This must be addressed through a future regulatory and statutory framework that governs and restricts its use to only essential situations.

C. ***Bias and Discrimination:*** AI bias, often known as *algorithm bias* or *machine learning bias*, describes AI systems that generate biased outcomes that mirror and reinforce societal biases held by humans, such as historical and contemporary socioeconomic inequity. The original training data, the algorithm, or the predictions the algorithm generates, can all contain bias. AI systems, particularly those used for facial recognition and predictive policing, have been found to exhibit biases based on the data they are trained on. Such biases can manifest in various ways, including disproportionately targeting certain demographic groups or failing to accurately identify individuals from minority populations. Studies have shown that facial recognition software tends to have higher errors when recognizing members of specific racial groups, especially individuals of

[32] Ibrahim Raji and Damilola Bartholomew Sholademi, 'Predictive Policing: The Role of AI in Crime Prevention' [2024], 13 IJCATR 66.
[33] Ameen Jauhar, 'Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement [2020], 16 IJLT 1.
[34] *K.S. Puttaswamy v. UOI* [2017] 10 SCC 1.

colour. The technology is frequently tested and trained on datasets that mostly comprise people from Western nations, especially white or lighter-skinned populations, it may falsely identify or fail to recognize individuals, leading to wrongful accusations or surveillance errors. This is especially problematic in a country like India, which has a diverse population with varying skin tones, facial features, and cultural backgrounds. Gender bias is another significant problem. Research has shown that FRT systems are more likely to misidentify women as compared to men. This is primarily because the algorithms are often trained on male-centric datasets or fail to properly account for gender-specific features. As a result, women are disproportionately affected by the errors of these systems, potentially leading to wrongful arrests or other forms of discrimination, especially when they belong to marginalized communities or minority groups. Research by Joy Buolamwini and Timnit Gebru, published by MIT Media Lab in 2018, shows that the error rate for light-skinned males is 0.8%, while it is 34.7% for darker-skinned women.[35] Additionally, facial recognition technology has trouble identifying women with diverse features, especially those from rural or lower socio-economic backgrounds, further exacerbating the issue. Therefore, AI has the potential to exacerbate systemic discrimination, leading to unjust outcomes where certain groups are subjected to more severe punitive measures, thereby perpetuating inequality within the justice system. Errors made by AI systems can have life-altering consequences for individuals, particularly in criminal cases. In the US, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool is used to assess defendants' likelihood of reoffending. However, it has faced criticism for exhibiting racial bias, often categorising African American defendants as high-risk at a higher rate than their white counterparts.[36] This situation highlights the ethical concerns surrounding bias and fairness in AI systems used in criminal justice.

D. ***Regulatory Standards:*** Establishing uniform legal and moral guidelines is a major obstacle to using AI in forensic identification. The principle of legality, encapsulated in the Latin maxim *Nullum Crimen Sine Lege,* asserts that no conduct can be deemed illegal or prohibited unless explicitly outlined by law. This implies that, in the context of

[35] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' [2018] 81 PMLR 1.
[36] Jeff Larson and others, 'How We Analyzed the COMPAS Recidivism Algorithm' (*Pro Publica,* 23 May 2016) < https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> accessed 25 January 2025.

developing technologies, the use of AI systems - which could be extremely dangerous - is frequently not prohibited or criminalized until legal frameworks step in to control and limit their application, protecting society, individual liberties, and fundamental legal precepts. The field of technology is developing quickly. However, the law's inherently slow and cautious pace means that legal frameworks struggle to keep up with the swift evolution and societal impacts of these emerging technologies. International efforts to regulate AI have already commenced in the interim. Notably, the OECD established AI guidelines in May 2019. According to these guidelines, the broad use of AI -including FRT - must respect human rights, the rule of law and democratic ideals.[37] In the case of *Big Brother Watch and Others v. the United Kingdom*[38], the European Court of Human Rights (ECHR) ruled that the UK's bulk data gathering program violated human rights legislation. The case questioned the legitimacy of the UK's widespread monitoring methods in the wake of Edward Snowden's 2013 disclosures, namely in light of Article 8 (right to respect for private and family life) and Article 10 (freedom of speech) of the European Convention on Human Rights. The Court found serious shortcomings in the program's supervision procedures and safeguards, highlighting the necessity of strong protections and proportionality in state monitoring activities.[39]

E. ***Accuracy and Reliability:*** The accuracy and reliability of AI-based forensic identification systems are crucial when applied in legal contexts. These systems rely on algorithms that learn from large datasets to identify patterns and make decisions. These systems must meet high precision standards to avoid misidentifications, which could result in wrongful convictions or failures in criminal investigations. False positives or false negatives could seriously damage the credibility of the justice system, particularly when these tools are used as crucial evidence in courtrooms.

AI technologies frequently yield complicated conclusions that are hard to explain simply, which raises questions about the reliability and openness of the decisions made in these situations. The potential contributions AI might make to criminal investigations are diminished since courts may reject evidence derived from AI because its results are not

[37] OECD, 'OECD Principles on Artificial Intelligence' [2019] <https://www.oecd.org/going-digital/ai/principles/> accessed 14 February 2025.
[38] Big Brother Watch and Others v. the United Kingdom (App No 58170/13) (European Court of Human Rights, 13 September 2018).
[39] Parkkavi E and Yadharthana, 'Artificial Intelligence in Criminal Justice: Balancing Efficiency with Fairness and Accountability' [2023] 6 IJIRL 483.

always entirely explicable. The necessity for precise norms or guidelines pertaining to the interpretability of AI and the disclosure of its usage during trials is developing as the legal profession incorporates AI more and more into its everyday operations. Clear regulations are increasingly needed to guarantee that AI's involvement in court cases stays open and responsible.

F. ***Transparency and Accountability:*** The "black box" aspect of many AI algorithms is a significant obstacle for forensic identification using AI. These systems frequently function via intricate procedures that are difficult to comprehend or describe. The lack of transparency in forensic identification raises severe issues since judements based on AI may have a substantial influence on people's lives. For instance, it could be hard to figure out why an AI system made a mistaken identification that resulted in an erroneous arrest or conviction, which would make it harder to contest the evidence in court. As AI systems grow more autonomous and effective, the risk of misuse or adverse effects increases. These systems have the potential to seriously damage people or society at large if appropriate accountability procedures are not in place. The conduct of an act is a basic component of criminal offences, and identifying and holding accountable the major creators of AI can help address accountability for flaws in AI systems within the legal realm. Defects resulting from errors in AI system design, training, or programming (such as biased algorithms, corrupted data, or inaccuracies) should be the responsibility of the developers.

When decisions are made based on errors from artificial intelligence, it raises significant challenges in determining who should be held accountable for mistakes, especially in cases of wrongful convictions. This problem raises difficult moral and legal questions about who is responsible for AI systems and their results - the engineers who create them, the law enforcement organizations that use them, or perhaps the AI itself. The important thing is that any accountability system needs to be open enough for people to seek compensation when judgements made by AI produce unfair results. Legal professionals, engineers, and ethicists must thus work together to create guidelines that precisely define responsibility and liability in the real-world use of in forensic science.

VI. FROM POLICY TO PRACTICE: A CRITICAL ANALYSIS OF THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

The CP Act was enacted to modernize law enforcement by expanding the collection of

identifiable data for criminal investigations, replacing the outdated **Identification of Prisoners Act, 1920.** While the 1920 Act focused primarily on collecting photographs, fingerprints, and footprints from prisoners, the 2022 Act broadens the scope to include **DNA samples, biometrics, iris scans, voice samples,** and **signatures** in response to advancements in forensic technology. The *Ram* ***Babu Misra judgement***[40] and the 87th **Law Commission report** highlighted the need for reform to equip law enforcement with modern tools. The Act allows for a **centralized digital database,** improving the accessibility of criminal records. Additionally, the 2022 Act enables the collection of data not only from prisoners but also from accused individuals, addressing gaps in criminal investigations and enhancing the potential for higher conviction rates. However, the Act raises concerns about privacy and the protection of fundamental rights, especially with the extensive collection of sensitive data. Balancing law enforcement objectives with the safeguarding of individual freedoms will require continuous scrutiny and careful implementation.

The **Act** raises concerns about physical autonomy and privacy, as it criminalizes refusal or resistance to providing measurements, thus allowing intrusion into an individual's physical autonomy.[41] While previous laws permitted the collection of measurements and biological samples in specific cases such as **rape** or **sexual offences**, the 2022 Act extends this power to all individuals within its scope, including those accused of less serious crimes. This intrusion conflicts with the **right to privacy.** Section 4 of the Act authorizes the collection of sensitive data, including fingerprints, palm impressions, iris scans, and behavioral attributes, but fails to define a clear, legitimate purpose for such collection. While the Preamble suggests the data may be gathered for 'identification' and 'investigation' in criminal matters[42], Section 4 broadens this to include 'prevention', 'detection', 'investigation', and 'prosecution', creating ambiguity regarding the law's intent and raising concerns over whether enforcement agencies could access personal digital spaces, like mobile devices with biometric protections, without clear legal grounds. This lack of clarity is further compounded by Section 5, which grants Magistrates the power to order data collection from anyone, even those not involved in the legal proceedings, making the law susceptible to privacy invasions. Moreover, the Act allows the NCRB to share collected personal data with law enforcement agencies nationwide[43], violating the principle of purpose limitation, which restricts data use to its original intent. This

[40] *State of U.P. v. Babu Ram Misra* [1980] 2 SCR 1067.
[41] The Criminal Procedure (Identification) Act, 2022, s 6.
[42] The Criminal Procedure (Identification) Act, 2022, Preamble.
[43] The Criminal Procedure (Identification) Act, 2022, s 4(1)(d).

grants law enforcement broad discretion to gather data indiscriminately, threatening the privacy of individuals, including those not convicted of a crime, and violating their rights under Article 21 of the Constitution. The law's expansion to include anyone arrested or detained, even under preventive detention[44], further exacerbates these concerns. Additionally, the use of "may" in the proviso[45] to allow measurements from individuals arrested for lesser offenses undermines the provision's intended benefits, giving Magistrates discretionary power that nullifies its protective aspects.

In ***Selvi v. State of Karnataka***[46], the **Supreme Court** previously emphasized the importance of consent for scientific tests. However, the 2022 Act does not require consent for individuals accused of crimes punishable by more than seven years of imprisonment or crimes against women and children. The law allows a magistrate to order the collection of measurements from these individuals, and resistance can lead to punishment under **Section 221** of the **BNS.**

The Act lacks clarity in several critical areas, particularly regarding the collection of "biological samples."[47] The term is not defined, creating ambiguity about which bodily invasions, such as blood or DNA extraction, may be permitted. Additionally, the term "behavioral attributes"[48] is vague and undefined, leading to various interpretations. It is unclear who will be authorised to collect such data - whether police officers, forensic psychologists, or licensed professionals.[49] Furthermore, the word "analysis" is ambiguous and vague when employed in reference to measurement.[50] The Act does not specify the process or framework for how these measurements will be used or analysed in criminal investigations, raising concerns about privacy and misuse. The lack of clear guidelines in the Act raises significant concerns regarding its implementation and the potential for misuse.

Section 4 of the Act empowers the NCRB to collect, store, share, and dispose of records collected under its provisions, with these records being kept in digital form for up to seventy-five years[51]. However, a proviso allows for the destruction of data from individuals who are not convicted, provided they are acquitted, discharged, or released without trial after exhausting

[44] The Criminal Procedure (Identification) Act, 2022, s 3(c).
[45] The Criminal Procedure (Identification) Act, 2022, proviso to s 3.
[46] [2010] 7 SCC 263.
[47] The Criminal Procedure (Identification) Act, 2022, s 2(1)(b).
[48] The Criminal Procedure (Identification) Act, 2022, s 2(1)(b).
[49] The Criminal Procedure (Identification) Act, 2022, s 4(3).
[50] The Criminal Procedure (Identification) Act, 2022, s 2(1)(b).
[51] The Criminal Procedure (Identification) Act, 2022, s 4(2).

all legal remedies. Still, this exception can be overridden if a Magistrate justifies retention in writing. Unfortunately, this option to delete data before seventy-five years applies to a narrow group of individuals. Such broad provisions make it difficult for exemptions to be genuinely implemented. In practice, almost all offenders, regardless of the crime's severity or the sentence, would have their data stored for seventy-five years. The rationale behind long-term data retention is to create offender profiles for future surveillance and detection. A blanket retention period of seventy-five years for all offenses, with no distinction, appears excessive, giving the government wide-reaching power to maintain detailed personal data. Similar issues have arisen in other countries, such as the Philippines, where a proposed national ID system was struck down for being overly broad and vague. Additionally, DNA data can reveal sensitive information about an individual's health, family, and character traits, including those of relatives not involved in the crime. The Act also allows data to be stored for people connected to the crime incidentally, like witnesses, which further complicates the issue. Given these concerns, lawmakers should reconsider the seventy-five-year retention period and consider setting different retention times based on the nature of the offense. If long retention periods are to be kept, there must be adequate safeguards in place to protect the data and justify this exception.[52]

The collection and preservation of such data raises several concerns about the safety and maintenance of in digital form. These measurements are personal and must be kept and stored as digital data without raising concerns about privacy violations. The largest obstacle, however, is that India lacks a strict and efficient legal framework for data protection.[53] Another significant concern is the possibility of mass monitoring as the database established by this Act may be linked to other databases already in existence, such as the Crime and Criminal Tracking Network and Systems (CCTNS). Combining this new data with the CCTNS, which was once intended to be a component of the Common Integrated Police Application (CIPA), might create a massive, networked monitoring system that raises the possibility of abuse and privacy rights violations.

[52] Aaryan Mithal and Abhina Gupta, 'Scrutinising the Criminal Procedure (Identification) Act, 2022, and its Conformity with Privacy Principles' [2022-2023] 15 *The NUJS Law Review.*

[53] Shaifali Dixit and Chandrika, 'The Legal Implications of The Criminal Procedure (Identification) Act, 2022: A Comprehensive Analysis of Constitutional, Criminal, and Forensic Dimensions' [2022] 5 SLR < https://www.hpnlu.ac.in/PDF/f4bff912-42e2-472d-be46-1b3d45af508f.pdf> accessed 12 January 2025.

VII. CONCLUSION

As AI is achieving deeper levels of assimilation within the criminal justice system particularly in context of forensic identification, the velocity of decision-making accelerates, thus amplifying the importance for algorithmic decision-making capabilities. Highlighting the opportunities and challenges, all stakeholders involved must be prepared for tough measures in order to thwart major issues stemming from the integration that targets the fundamental rights of its citizens. The speed, which is a part of everyday justice system, must be made mandatory for fruitful intervention where detestable criminality often outdo the capacity of human decision-makers to answer with sufficient criminal information in exceptional cases. Beyond this, a vital consideration lies in the comprehensive acknowledgment of the increasing reliance on AI for decision-making processes that give rise to concerns about the possibility of misguided choices or those made even without a full appreciation of their consequences. Indubitably, the use is poised for growth, but its trajectory will depend on how both the Union and the States tackle the challenges that may arise in the future.

The road, however, to thwart these formidable obstacles is long, it, therefore, is essential to implement standardized data collection and storage protocols, which will be crucial in ensuring accuracy and reliability, and in conjunction with this, it is important to modernize forensic laboratories, which should be equipped with 'state-of-the-art hardware' and 'cloud-based platforms,' thus enabling AI-driven analysis. Additionally, it is also necessary to introduce comprehensive skilling programs that must not only impart requisite knowledge and skills to forensic experts and law enforcement personnel but must also facilitate a synergistic alliance between academia, industry, and governmental institutions. Moreover, the creation of sophisticated ethical and legal frameworks is sine qua non for establishing transparency and accountability in the AI systems. In addition to this, in order to optimize efficacy and establish unified governance, it is also extremely sine qua non to strengthen inter-agency collaboration, which will culminate in the formation of a centralized oversight entity. Meanwhile more attention is also needed to combat misinformation, the spread of public awareness campaigns, in this case issue, can aim to enhance trust in the application of AI within this field by preventing harmful apprehensions about the use of AI in this field. To banish the smog filled clouds further, India can, through the strategic implementation of measures, substantially amplify its forensic identification capabilities, bolster the efficacy of criminal investigations, and ultimately ensure the fair administration of justice.