

Deployment of AI Tools in Forensic and Criminal Investigations Critical Examination of the Problem Statement and Literature Gaps

Dr. Monika Thakur, Sailesh Suryanarayan Iyer
Lincoln University College Malaysia.

Abstract

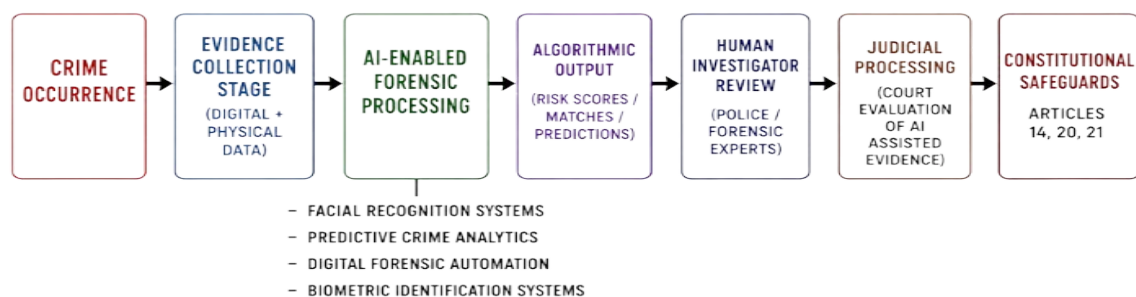
The justice systems are still behind even as computers acquire skills to identify suspects among the masses. Computers crunch numbers to forecast trouble spots - but humans make sluggish laws to operate fast technology. Imagine an inflexible court that confronts algorithms, rulebooks that are even older than the internet. In the event code is misidentified, who is at fault? There are no definite answers. The instruments busied in the absence of supervision. The judgments that were once determined by eyes and notebooks are now based on concealed mathematics. Without evidence trust is established. Complicated designs contain errors. Doom machines are subject to the laws of men. Advancement is galloping forward - legislators are mired in paper. Most overlooked? A good system to ensure algorithms behave in line with the Constitution, as humans do. Research - national and international - demonstrates that there are gaps, not just in legislation but in the real evidence of fairness results. It is not something which is going to break all at a sudden: high tech equipment with outdated systems can go wrong. This is significant and, in the absence of regulation, it is fair to say that using AI in investigations will most likely breach the very basic Indian Constitutional provisions—Articles 14, 20 and 21 of the constitution. The absence of movement without warning; constitutional law can be the element of sanity between order and freedom.

Keywords: Artificial Intelligence; Criminal Investigation; Digital Forensics; Constitutional Law; Procedural Fairness; Algorithmic Accountability

Introduction

The use of computers has taken over the functions of humans, particularly in law enforcement. The departments do not rely solely on officers but also on the face-scanning software, which can identify potential criminals. Crime predictors are derived from programs examining the pattern of occurrence of old crimes - where are the areas where new ones can happen. Looking at gadgets such as phones and laptops? The latter is a quicker work, which is possible thanks to the digital detective tools. Globally - in cities in Europe to parts of Asia - the change is reflected in the way investigations operate. In India, command centres, which are connected, host fingerprints, ID systems, and watchful cameras for better faster tracking and response.

AI-ENABLED CRIMINAL INVESTIGATION WORKFLOW



In spite of the rapid technological developments, the legal procedure in India continues to be biased towards using old-fashioned techniques that include people-centered investigations and typical evidence collection. However, the new issues have arisen with the introduction of artificial intelligence, which is lack of understanding of how it works, prediction-based information, and lack of transparency in the decision-making process. There were no such problems in the past. This separation has created virtual antagonism: the high tech crime solving against the rights of basic protection, and that is what is dug up here.

Review of Literature

In today's times, it has been shown that AI is much more often utilized in the field of crime solving, such as face scan, crime whereabouts prediction, searching digital information or face matching. Given the work and discoveries of Perry et al. (2013) and Berk (2021) at the AI Now Institute, it would seem that machines can make things faster and get things right. In India, cops and laboratories are rushing into these tools at a faster rate than ever before, researchers find. But then there are large questions, embedded biases in codes, grey decision making, and threats of surveillance, as well as policies regarding evidence in court that still remain unconstrained. What's missing? Thoughtful considerations about whether technology like this is in keeping with key rights enshrined in Articles 14, 20 and 21 of the Indian Constitution.

Review of Literature: Deployment of AI Tools in Forensic and Criminal Investigations

S.No.	Author / Source	Area of Study	Key Findings	Literature Gap
1	Berk, 2021	Predictive policing and risk assessment	AI helps forecast crime locations and offender risk. (Annual Reviews)	Limited focus on constitutional safeguards in India.
2	Perry et al., RAND, 2013	Crime forecasting	Predictive policing supports resource allocation. (eucpn.org)	Insufficient safeguards against biased historical data.
3	Hardyns&Rummens, 2018	Predictive policing challenges	AI can assist policing but raises ethical and accuracy concerns. (eucpn.org)	Lack of judicial admissibility standards.
4	Ugwudike, 2022	Predictive justice systems	Algorithms increasingly influence criminal justice decisions. (crimejusticejournal.com)	Limited transparency in algorithmic decision-making.
5	AI Now Institute, 2018	Algorithmic accountability	Public agencies need auditability and accountability mechanisms. (AI Now Institute)	Indian law lacks strong audit requirements for police AI.

6	Verma, 2026	AI in criminal justice	AI assists policing, surveillance, and judicial processes. (humanrightlawreview.in)	Needs stronger rights-based legal regulation.
7	Kumar, 2025	Indian criminal justice	AI can improve investigation through facial recognition, digital forensics, and social media monitoring. (Artefacts Discovery)	Empirical evidence on accuracy remains limited.
8	Bharati, 2025	AI-powered forensic analysis in India	AI may improve forensic accuracy and case processing. (ResearchGate)	Courtroom admissibility of AI evidence remains unclear.
9	IJRTI Study, 2026	AI in forensic investigations	Discusses AI use in cybercrime, facial recognition, and forensic laboratories. (IJRTI)	Does not fully address constitutional remedies.
10	IJCRT Study, 2026	AI in forensic science	AI improves speed, precision, and reliability in forensic work. (IJCRT)	Overlooks risks of automation bias.
11	Arthanari, 2025	AI applications in forensic science	AI supports forensic identification and evidence analysis. (Lippincott Journals)	Limited India-specific legal analysis.
12	Reference Global, 2025	AI and fundamental rights	AI tools raise concerns about privacy, equality, and fair trial rights. (Paradigm)	Needs deeper connection with Articles 14, 20, and 21.
13	DAKSH India	Smart policing in India	India is increasingly using AI-based tools in policing. (Daksh)	Lack of uniform national governance model.
14	Washington Post, 2025	Facial recognition misuse	Wrongful arrests occurred where police relied heavily on facial recognition matches. (The Washington Post)	Shows need for mandatory human verification and disclosure.
15	Financial Times, 2025	Facial recognition bias	UK authorities acknowledged bias in police facial recognition systems. (Financial Times)	Highlights risk of discriminatory outcomes in India too.

Problem Statement

Although there is an increase in the number of experts utilizing artificial intelligence, India has not completely developed a set of laws that govern how AI ought to be used in crime investigations. Without concrete directives, there is concern about the legality of such tools - raising profound concerns relating to constitutional rights. When AI is allowed to work in criminal cases unchecked, fair trial requirements may be lost, evidence can lose its credibility, but the protections guaranteed by Articles 14, 20, and 21 may be eroded. There are five related problems that underlie this main gap:

1. Legality and Statutory Authorization

Most of the face scanners or crime guessers are not legally sound. Usually, there must be a clear law or an exercise of a state power for arrests or searches to occur but silently, “automatic surveillance” permeates with common administrative decisions. This anomaly raises the issue whether there is possibility of safeguarding individual liberty and privacy guaranteed under Article 21 in view of these intrusions which have to be based on some legal grounds. The Puttaswamy case of 2017 had held that checks and balances, just cause, proportional impact and a valid law have to be put in place in order to ensure that the restrictions on privacy are met. AI in policing, without a proper legislative framework, immediately gives a constitutional cause for concern.

2. Evidentiary Reliability and Admissibility

When software recognises faces, predicts actions or reveals hidden patterns, things get complicated in court. The top decisions in India since “Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473) call on severe measures with respect to digital records - such as requiring a paper under Section 65B of the Indian Evidence Act, 1872. Machines provide answers; but scepticism is evident - not whether they are correct, but whether anyone can test how they came to such conclusions. One of the risks becomes particularly relevant if systems like these are still unclear in terms of law: the courts could be too willing to go with the machine's decision, which may lead to wrongful decisions.

3. Constitutional Compatibility

If the information on which officers ask questions is false, it is as if it were unequal treatment guaranteed by the law. In case outcomes of pressured body scans have been achieved, security measures surrounding individual guilt come into the picture. Dignity and private life are safeguards of article 21. The prejudice can be even without intention to harm, hidden within the functioning of digital systems. Neutral looks like old-fashioned prejudice. Suddenly, the forced thoughts inspection collides with fundamental freedoms, judges used to make it straight. One of the big decisions ruled out any mind reading possibilities, thus giving a firm line. Choice, they said. So when it comes to headspace, do you have say-so? Machines, in the silence, redefine what seems like fairness, to individuals who are dragged into their embrace. Then there was the decision in Manohar Lal Sharma v. And then there was a case in which restrictions on spy technology were in the limelight. But when gadgets get too far, the justices noted, the courts should step in. Without stringent legislation, surveillance can be taken to extremes. It is not the instrument which is most burdened - but the bridle which restrains it. Power free to run far, far off the legislative leash.

4. Algorithmic Opacity and Due Process

Most AI systems are black boxes, which provide an output without revealing what data they used to train them, how they believe they got their output, and the error rate. This opacity leads to a lack of due process since an accused should be aware of and be able to counter the evidence against him. It would make cross-examination even more challenging when the prosecution is founded on an algorithm, and lacks the answer on how it originated. This sabotages adversarial fairness and may be tantamount to the violation of the right to a fair trial entrenched in Article 21. This should be followed by the courts requiring transparency, independent verification and disclosure prior to the acceptance of evidence generated by AI. The Constitution of India art. 21, Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Selvi v. State of Karnataka, (2010) 7 SCC 263.

5. Accountability Deficit

AI policing results in a big accountability problem. AI could produce a false facial match or miscalculate the risk, the liability of which might be jointly held by the developers, vendors, forensic experts, and investigating officers. The question is difficult to answer who is legally responsible in case of wrongful arrest, illegal surveillance or miscarriage of justice. The classic way of criminal procedure is founded on the premise that the state takes care of the investigation, which is not applicable in the case of AI. The statutory regulation of certification, audit, disclosure, liability and supervision is thus needed in India. Unless such safeguards exist, the AI may pose a risk to the rule of law and the fair criminal procedure.

Identification and Analysis of Literature Review

AI policing results in a big accountability problem. The liability of AI producing a false facial match or a wrong risk forecast might be distributed among developers, vendors, forensic scientists, and law enforcers and investigators. Who is to be held legally responsible in the case of wrongful arrest, illegal surveillance or miscarriage of justice is difficult to tell. The conventional method of criminal process assumes the state to take charge in the investigation, an assumption that will not be applicable in the case of AI. The statutory regulation of certification, audit, disclosure, liability and supervision is thus needed in India. In case of the absence of these safeguards, AI might endanger the rule of law and fair criminal procedure.

1. Algorithmic Governance and Opacity

A line of research holds that algorithms are constrained by invisible rules. Every day, despite being invisible, such setups steer big choices. Secrecy in software undermines trust in public institutions, Pasquale's book argues. Ordinary people lose ground when they do not have access to inner workings. Calculative tools can exacerbate social disparities, O' Neil shows. Whether you like it or not, hidden patterns exist within their design. Instead of reasoning about rules, computers learn from a vast sea of data. What drives them isn't reason - it's frequency, as Surden explains. Judges tend to be confused with algorithmic methods, not as much for lack of ability as lack of foundations per Surden and Williams (2023). Systems operate without fanfare, pushing outcomes along a particular path; sometimes, systems operate without careful scrutiny but just trust the output. As this happens, concepts of justice or transparency begin to slip away, especially in relation to Article 21. Although these texts skirt the fringes of legal issues, they cannot grab hold of the rights that are inherent in this provision.

2. Predictive Policing and Surveillance

Not all agree that predictive tools are beneficial for the police. In this study on data and patrols, as Ferguson indicates, systems tend to uphold old patterns instead of breaking them. Different, Joh examines the effect numbers can have on decisions made by cops when investigating crimes. Findings like these emerge in the work of Garvie, Bedoya, and Frankle - examples show facial recognition systems made mistakes in U.S. law databases. Bennett Moses and Chan (2023) illustrate how algorithmic tools influence prosecutors' decision-making processes well prior to the filing of formal charges. These findings, while of course providing tangible evidence, are more of a product of the U.S. constitutional environment, and thus Indian constitutional standards are not tackled by comparison.

3. Evidentiary and Forensic Concerns

In one paper, the authors examine how AI is revolutionizing the traditional approach to gathering evidence in court. Millennials, who aren't mired in tradition, are now digging into problems offered by Internet clues. Read Casey on computer crimes - challenges us on how we trace computer tracks, maintain consistency in results, how human judgment affects technological investigations. The machines that creep into the crime analysis make it more difficult to do repeat tests - precisely what Casey and Jaquet-Chiffelle have beaten home lately. When intelligent systems provide answers without explaining how, faith in a fair trial is undermined - that was uncovered by Mantelero last year. Nonetheless, these writings refer to reliability but in fact not connected to the laws of India on proof. The remarkable aspect of the same is that they do not take into account Section 65B of the Indian Evidence Act of 1872. Then we had that of Anvar P.V. versus P.K. Basheer - scarcely to be heard of in this place. Yet, another judgment that was ignored is Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal.

4. Constitutional and Human Rights Perspectives

The relevance of procedural safeguards in the AI context has been noted by constitutional scholars. Danielle Citron and Frank Pasquale, in the article, *The Scored Society*, (2014) 89 Washington Law Review 1) affirm that due process should be incorporated in automated decision-making mechanisms. According to Tal Zarsky in his article *The Trouble with Algorithmic Decisions* (2016) 14 Colorado Technology Law Journal 131, algorithmic governance erodes archaic concept of accountability and procedural justice in the law. The post-Puttaswamy scholarship by D.Y. Chandrachud and Bhandari (2021) discusses issues of privacy, proportionality and constitutional morality in India. However, little has been done in terms of applying such doctrines to the specific application of AI to criminal investigation and policing.

5. Indian Scholarship and Emerging Gaps

Research Gap

Review of literature reveals that there is a lot of theoretical criticism on the use of AI in police work and very little research work in India focusing on investigation. There is no existing scholarship that provides a thorough picture of constitutional doctrine and the actual practice of investigation with AI. Likewise, there is a lack of discussion regarding the testing of AI generated evidence under the Indian evidentiary rules, such as in the context of electronic evidence and forensic reliability. Moreover, the literature lacks sufficient recommendations of procedural safeguards, which are appropriate in the context of Indian policing practices such as transparency, auditability, judicial oversight and accountability mechanisms. The New initiatives attempt to examine AI within the Indian legal system. In 2020, Kumar speculated it could assist in running the courts more effectively - yet solid evidence remains elusive. In 2024, Singh

started doubting things, shortly thereafter, Rai joined the investigation of the facial scans and online tracking against the new privacy regulations. These instruments are hitting the law in a hurry, but responses are on the surface. Combining thoughts and practice? Not yet observed anywhere. When robots excavate personal rights - such as fairness, self-defense, life - the ground becomes shaky, without concrete decisions to stand. Here are a few of the foreign cases, sneaking up smarter rules. To keep his feet on the ground, filling the gap, this work resorts to legal documents as well as real-life observations. The gap in research is therefore the point of convergence of the four areas of constitutional law, criminal procedure, forensic science, and technology governance.

Conclusion

AI is showing transformative potential in the field of forensic and criminal investigation, but also a great constitutional danger. The focus is not the use of AI, but how it is being used in a form of 'unregulated deployment' that could erode legal, fair, private, and accountable use. Since time immemorial, Indian constitutional jurisprudence has laid emphasis that intrusive technologies need to meet legality, necessity and proportionality, as well as procedural safeguards. Without clear laws and standards that are legally enforceable, however, the reliability of evidence could be compromised and the fairness of criminal proceedings could be undermined by investigations conducted with the help of AI. Hence, the current study is oriented towards the urgent doctrinal and normative space. It aims to promote the use of technology in a way that reinforces the administration of criminal justice while preserving the rule of law, constitutional norms of morality, and due process.

References

1. Bennett Moses, L., & Chan, J. (2023). Algorithmic investigations and the reshaping of criminal justice. *Modern Law Review*, 86(4), 812–842.
2. Bhandari, V. (2021). Surveillance, technology and the right to privacy in India. *Indian Journal of Constitutional Law*, 15, 45–78.
3. Casey, E. (2011). *Digital evidence and computer crime*. Academic Press.
4. Casey, E., & Jaquet-Chiffelle, D. O. (2024). Artificial intelligence in digital forensics: Risks, reliability, and evidentiary challenges. *Digital Investigation*, 48, 301–315.
5. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89, 1–33.
6. Ferguson, A. G. (2017). Predictive policing and reasonable suspicion. *Emory Law Journal*, 62, 259–325.
7. Garvie, C., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law Center on Privacy & Technology.
8. Joh, E. E. (2019). Policing by machine. *Harvard Law Review*, 128, 172–210.
9. Kumar, V. (2020). Artificial intelligence and criminal justice administration in India. *Journal of the Indian Law Institute*, 62(3), 389–412.
10. Mantelero, A. (2024). Artificial intelligence, criminal justice and fundamental rights: The role of explainability. *Computer Law & Security Review*, 52, 105845.
11. O'Neil, C. (2016). *Weapons of math destruction*. Crown Publishing.
12. Pasquale, F. (2015). *The black box society*. Harvard University Press.
13. Singh, S. (2024). Facial recognition technology and criminal policing in India. *NLU Delhi Law Review*, 11(1), 55–88.
14. Surden, H. (2019). *Artificial intelligence and law: An overview*. Cambridge University Press.
15. Surden, H., & Williams, M. (2023). Technological opacity, predictive algorithms, and due process in criminal justice. *Harvard Journal of Law & Technology*, 36(2), 345–392.
16. Zarsky, T. (2016). The trouble with algorithmic decisions. *Science, Technology & Human Values*, 41(1), 118–132.