INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS: LEGAL AND ETHICAL PERSPECTIVES

AUTHOR – ADITI SINGH, SCHOOL OF LAW, CHRIST UNIVERSITY, LAVASA CAMPUS, PUNE

BEST CITATION – ADITI SINGH**,** USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS: LEGAL AND ETHICAL PERSPECTIVES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 731-736, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The incorporation of Artificial Intelligence (AI) into police investigations has changed the face of modern law enforcement, making processes such as evidence analysis, predictive policing, and forensic examination more efficient. This paper examines the application of AI in criminal justice institutions, with a particular focus on its legal and moral implications. By analysing recent research, including articles by Ying Yuan and Qian Dai (2019), Richard A. Berk (2020), O. Yara (2021), and Monika Zalnieriute (2021), the paper acknowledges and delineates the significant concerns associated with the use of AI technologies in police departments. The results of the study show that, on the one hand, AI tools can make things faster and easier by automating data handling, ground crime anticipation, and accuracy of case-solving, yet, on the other hand, these same tools can be the source of bias issues, lack of accountability, challenges in data privacy, and procedural fairness. Legally, the lack of detailed regulations governing AI-funded inquiries raises questions about responsibility and the admissibility of evidence in court. From an ethical perspective, it is challenging for people to understand how decisions are made by algorithms (since their inner workings are hidden), and this also raises the possibility that the algorithms may discriminate against certain groups of people. Both these factors can violate the basic human rights of equality before the law and the right to privacy. The research advocates for the implementation of transparent and easily understandable models of AI that adhere to the principles of due process and are open to judicial verification. Furthermore, when comparing different countries, it becomes apparent that they have varying approaches to addressing this issue, which is also reflected in the extent to which regulations have evolved and the general public's response to them.

INTRODUCTION

Artificial Intelligence has swiftly become a vital component of modern policing systems, which has to an extent, altered investigative techniques and decision-making processes across the world. Law enforcement agencies are adopting AI-driven tools to manage the increasing complexity of criminal investigations as crime becomes digital, transnational, and technologically sophisticated. Police departments can now collect and process information at previously unattainable speeds, identify hidden crime trends, organise evidence processing and produce useful information which otherwise would be inaccessible. However, the same systems that strengthen the ability to conduct investigations also raise serious ethical and legal concerns. The rift between efficient technology and fundamental rights safeguards is caused by a number of variables, including the lack of transparency in computational thinking, potential bias in training datasets, breaches of privacy, and vague standards of responsibility. AI-assisted enforcement is one of the most arguable topics in modern criminal justice systems because of

the existence of both advantages and disadvantages.

The necessity to handle an enormous amount of digital evidence was the primary motivation behind the early use of artificial intelligence in criminal investigations. Conventional methods of investigation were not equipped enough to handle the volume and complexity of data that was being produced by social media platforms, mobile devices, surveillance cameras and digital financial transactions. Despite the promise of quick data sorting, pattern detection and predictive modelling, Artificial Intelligence solutions have emerged as a solution. Authorities were produced with evidence bases by systems that could trace out criminal hotspots, examine audio recordings and extract digital fingerprints and scan countless hours of CCTV footage. Over the years, machine learning models began recognizing suspects in crowds, predict future crime scenes and determine the possibility reoffending. These advancements transformed not just how investigations are conducted but also how police allocate resources, time and manpower. These changes indicate a paradigm shift in a way that policing is believed of: from reactive investigations that are started after a crime has been carried out to anticipatory policing that claims to stop criminal activity before it emerges.

Even though there are several potential advantages to this approach, the accuracy of investigative techniques cannot be solely determined by efficiency. AI systems are depended heavily on the data used to train them, as researchers have repeatedly noticed. Predictive Policing algorithms inadvertently contribute to over policing tendencies in particular neighbourhoods by concentrating police attention in areas that are already under disproportionate monitoring. The concept that crime is more prevalent in some areas is strengthened through this cyclical effect, not because those areas have traditionally had more aggressive policing. The likelihood that AI could merely automate discriminatory practices which have been criticized for unfairly targeting disadvantaged groups is shown by such feedback loops. Analyses of risk assessment tools additionally demonstrate that , despite their seeming neutrality, algorithmic predictions frequently incorporate the racial, economic or social injustices entrenched in the legal system. An algorithm may disregard socioeconomic elements that influence the context of crime when it labels people as “high risk” based on past data. The widely recognised notion that a significant portion of recorded data is produced by policing patterns instead of actual crime rates is ignored by the presumption that prior criminal records or police interactions represent objective truth. These issues highlight an essential problem: AI is developed by the very social structures that some argue may be discriminatory; it cannot be found outside of society. Due to this, AI could unintentionally perpetuate injustice under the pretence of scientific impartiality. Inaccurate projections and the tendency of society to accept algorithmic results as true, even when they contain embedded prejudices, are two risks associated with technologically mediated discrimination.

Further complicating matters is algorithmic decision making’s opacity. Because of their dependence on proprietary models developed by private corporations, may AI techniques used by law enforcement have not been open to public or court review. Although, these technologies are “black box”, investigators may depend on findings without understanding how an algorithm generated its recommendation. In legal terms, this is called into question whether AI generated evidence can be admitted in court. Defendants cannot effectively cross-examine an algorithm whose logic is not accessible, while maintaining the constitutional right to contest the foundation of the evidence used against them. Due process safeguards are undermined by this tension, and it also runs the risk of transferring fundamental human judgement to autonomous systems devoid of moral and legal accountability. Courts must make the difficult decision of whether to rely on

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

complex technical structures that are unable to completely comprehend, which might lead to justice becoming reliant on unquestionable digital protocols.

Concerns about ethics emerge similarly. For example, facial recognition systems are frequently used without the public's consent and have demonstrated high error rates for ethnic minorities, women and children. Unwarranted arrests, invasive searches and inappropriate surveillance can result from misidentification. The widespread use of biometric tools in public places- such as airports, train stations, streets and shopping centres creates an environment of constant surveillance that undermines the right to privacy, even when those tools are correct. When citizens are constantly examined, assessed and categorized by automated systems, a long-standing democratic value, the ability to move anonymously in public is undermined. In civilizations where political opposing parties or minority communities are under greater scrutiny, this information has especially grave consequences. The normalizations of surveillance runs the risk of turning democratic nations into security driven settings where the state uses pervasive technology to exert its power.

Human dignity is another concern that goes beyond bias and accuracy. By reducing people into data points, algorithmic policing reduces the complexity of human behavior to stastical probability. Predictive systems run the potential of stigmatizing people without hard proof of misconduct when they classify people as "high risk" based on opaque data patterns. Increased police stop, surveliance targeting, or implicit bias in officer behavior could result from such classification. Inaccurate forecasts are not the only concerns; interpreting risk ratings as objective scientific facts might have structural repercussions. The possibility that pre-emptive policing violates rights like the presumption of innocence increases with the degree to which police reply on prediction. The core principles of criminal jurisprudence are undermined by a legal system that starts to review people as potential threats rather than agents of free will based on statistical modelling.

The legal issues regarding AI in investigations extend far beyond admissibility. Accountability is a key concern. It becomes challenging to determine who is at fault when an AI tool contributes to a wrongful arrest, discriminatory action or breach of rights. The algorithm itself, the software business that developed it, the department that implemented the program, or the police officer who employed it should bear the responsibility. AI systems challenge traditional casual theories, but criminal law and tort law depend on the precise attribution of culpability. Police agencies function without sufficient safeguards, and victims of algorithmic injury encounter considerable challenges in pursuing remedies in the absence of legislative certainty. Because of this ambiguity, a hazardous environment is created where mistakes in technology might result in serious harm with little chance of recovery.

Regulations pertaining to AI assisted investigations differ greatly between nations. Precautionary frameworks that emphasize explainability, transparency and stringent restrictions on biometric surveillance have been implemented by some countries, including the European Union. According to the EU's artificial intelligence act, real time facial recognition and predictive policing are considered high risk technologies that need strict regulation. The United States, on the other hand, lacks a single federal framework, which results in different state and local policies. While some communities have embraced predictive policing methods to lessen resource costs, others have completely prohibited facial recognition due to concerns about accuracy and human rights. AI is widely used in law enforcement by countries like China as part of larger social governance plans, where data analysis and monitoring are essential to upholding official authority while in the meantime, a lot of developing countries quickly adopt AI technologies without simultaneously

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

creating a robust legal protection, putting their population in serious risk of abuse.

These contradictions are strongly illustrated in the Indian setting. Through programs like the National Automated Fingerprint Identification System (NAFIS), Automated facial Recognition System (AFRS), Crime and Crime Tracking Network System CCTNNS), and many state level predictive police tools, India is witnessing a surge in the use of AI. Large scale modernization is supported by these tools, but they also bring up important constitutional issues with regard to responsibility, equality, privacy as a basic right, requiring state acts to be lawful, necessary and appropriate. However, AI tools are frequently used without independent monitoring and clear legal clearance. A framework for safeguarding personal data is provided by the Digital Personal Data Protection Act, but extensive exemptions for government institutions run the risk of weaking these safeguards in the case of law enforcement. AI may allow for excessive data collection, widespread surveillance and unrestricted profiling in the absence of well-defined limitations.

The administration and quality of the data needed to train AI systems is another significant issue. Erroneous conclusions may result from incomplete, out of date or inaccurate datasets. For instance, the algorithm may mistakenly treat particular caste or minority groups as statically more likely to commit crimes if a crime database contains a disproportionate number of records from those groups as a result of discriminatory enforcement techniques. Algorithmic outputs can be further distorted by poor data hygiene, such as duplicate records, incorrectly labelled entries, or inaccurate demographic data. Therefore, ensuring data quality is not only a technical requirement but also an ethical obligation that has an impact on actual results.

Complexities arise when AI is included into digital forensics. Automated smartphone data extraction and internet activity analysis tools can create vast digital trails that may violate privacy beyond what is required for an inquiry. Network mapping, automated sentiment analysis, and behaviour prediction based on social media activity can all quickly turn into unwarranted surveillance. The inability of the law to keep up with these technological advancements raises important concerns of necessity and proportionality.

The use of AI in law enforcement ethically compels societies to reevaluate what justice and fairness are. The human values that are the foundation of criminal justice systems cannot be replaced by efficiency. AI cannot replace empathy, moral judgment, or contextual awareness, even though it might increase accuracy in some situations. The danger is that human investigators would rely too much on algorithmic recommendations rather than that AI will completely replace them. Police officers may prioritize automated outputs over these types of evidence when they seem objective or scientific, even in situations where caution is advised. Automation bias has the potential to skew investigations, affect prosecution tactics, and mold judicial opinions as it is thought to be error-free, a seemingly neutral technological system may have disproportionate effect.

In spite of the deeply complex and problematic issues that are involved in the deployment in AI technology in criminal investigations, it is neither usable or desirable at all in terms of refraining from it's complete adoption. This is because technological advancement is deeply woven into contemporary governance and law enforcement, and therefore, AI technology as an application of data analysis and pattern recognition, offers undeniable potential in terms of improving criminal justice institutaions. Indeed, it is not technology that needs to be resisted, but its direction and control so that it is associated positively with justice rather than being against it.

Essentially, the normative agenda must be to ensure that artificial intelligence assists human decision making proceses and does not replace

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

or subvert them. The criminal justice system, as opposed to administrative justice, involves decision making mandates which directly bear upon liberty, dignity, and the life of human beings itself. As the supreme court of India clearly asserted in the case of Maneka Gandhi v. Union of India[1232] from 1978, "just fair and resonable" standards must be followed in all procedures which deprive a person of his or her personal liberty. The hazard of doing so applies to the use of artificial intelligence-based investigation systems which function independently or with opaque process.

This worry has been reflected with the related literature on comparative jurisprudence. In the case of State v. Loomis (2016), while allowing the use of algorithmic risk assessment for the purpose of sentencing a defendant, the Wisconsin State Supreme Court cautioned the need not to reply on algorithms for the purpose of determining the fate of the defendant. This has been followed by other legal scholars like Richard A. Berk, who writes "Predictive analytics appears to formalize uncertainty rather than dispel it; it is the unconditional surrender to algorithmic forecasts pd sentences and decisions can make formal procedure itself procedurally unfair". [1233]

Transparency in this regard is not an nicety that courts might indulge in if technically possible, but an imperative laid down by the constitution itself. The courts cannot effectively carry out effectively carry out judicial review over the methods employed in investigations if the underlying logic behind the use of AI is beyond their comprehension. The doctrine of open justice holds that the reasonableness of the actions taken by the state must be comprehensible not only to the courts but also to any affected litigant. Moreover, the argument is made that the rule of law could be replaced by the rule of code where the complexity of code would render the rule of law meaningless. Consequently, the use of AI systems in criminal investigations must be made in such a way that the results are understandable and verifiable.

Another aspect, also paramount is the need for independent audit and impact assessments. The institutional commentaries by institutions such as the Organisation of Economic Co-operation and Development (OCED)[1234] or the United Nations High Commissioner for Human Rights have always argued that it is necessary for there to be an ongoing evaluation where AI systems are used in highrisk areas. The OCED AI principles adopted in 2019 pay particular emphasis on the need of AI systems to be transparent, robust and accountable especially where such AI systems have an impact on fundamental rights. The UN Report issues in 2021 on Artificial Intelligence and Human Rights indicated that predictive policing tools and facial recognition systems gave serious potential dangers if not strictly controlled by tight safeguards.

No discrimination is one of the most contentious ethical and constitutions concerns. This is because machine learning models trained on crime data tend to reproduce structural injustices rather than actual criminal activity. This is a threat to the principle of equality in the application of law in Article 14 of the Constitution of India. The doctrine on arbitrariness as defined in the E.P. Royappa vs. the State of Tamil Nadu (1974) [1235]is now a classic in the Indian Supreme Court jurisprudence, clearly clarifying arbitrariness as the antithesis of equality. Profiling by machine learning systems that discriminates adversely against social minorities designated by caste, class, religion or geography can be deemed unconstitutional state action.

Another such pillar is the issue pf privacy. The right to privacy a right now considered a basic right is assessed through a rigorous scrutiny of the state's ability to monitor individuals in the

[1232] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[1233] Richard A. Berk, 'An Impact Assessment of Machine Learning Risk Forecasts on Parole Board Decisions' (2020) 17 *Journal of Empirical Legal Studies* 193.
[1234] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (OECD Publishing 2019).
[1235] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3

judgement of Justice K.S Puttaswamy v. Union of India (2017)[1236]. Biometric and AI driven tools such as facial recognition, biometric profiles and predictive analytics have remarkably enhanced the state's ability to monitor citizens, including without their knowledge and consent. In the absence of specific legislation and narrowly drafter regulations the use of AI driven tools of state monitoring can render a commitment under Article 21.

Comparative human rights jurisprudence also supports such concerns. The European Court of Human Rights in S. and Marper V. United Kingdom (2008) declared that the indefinite storage of non-convicted individuals biometric information was incompatible with a person's right to privacy. More recently, in Big Brother Watch v. United Kingdom (2021) this same court underscored how a system of comprehensive surveillance requires robust oversight. The line of jurisprudence indicates a growing global consensus on a principle technological capacity is never a basis for state absolutism.

Other than the rights perspective, the question of accountability is ever relevant. One of the more unsettling aspects of the impact of AI in criminal investigations is the problem of accountability that the latter raises. For instance, where there is negative impact that is emanating from decisions that are made by an algorithm the problem of accountability that is placed squarely at the door of the police, the government and the technology provider become fractured. However, the Indian Constitution and the decisions of the Indian Judiciary will not countenance the problem of accountability that us being referred to. For instance, Niibati Behra v. the State of Orissa (1993), [1237]the Indian Supreme Court held that the state is liable for all human rights violation.

To meet these challenges, legal frameworks with specific legal structures are essential. It is not appropriate to leave AI practices in criminal investigations in executive departments or those within law enforcing agencies. Schnapp has argued "some lae enforcement AI systems may be viewed as high risk with serious repercussions. Regrettably this is currently not prohibited in most legal jurisdictions, on the contrary efforts are being made to openly promote this form of AI. It is high time to regulate high risk AAI including law enforcement AI through stricter regulation and regulation based on high standards. The European Union AI Act is one successful example. The role of democratic monitoring should not be substituted by legislative regulation. On the positive note, AI has the capacity to increase efficiency in investigations, improve forensic analysis and support law enforcement in dealing with complex and tech savvy crimes. However, it also has the danger of perpetuating inequalities in society, undermining privacy, due process and accountability. The key to understanding this intersection is to find a delicate balance between innovation and rights, or between efficiency and justice and between technological progress and restraint. The faster the state embraces AI technology, the more pressing becomes it's need for transparent regulation, ethical oversight and protective constitutionalism. It is only when AI is circumscribed by such normative parameters that it can become a constructive, and not a destructive force in justice. Technology can prove a very effective ally of justice, not it's sharpes critic if it is so supervised and regulated.

[1236] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC
[1237] *Nilabati Behera v. State of Orissa*, (1993) 2 SCC 746