AI & MONEY TRAIL: AN ANALYSIS

Ayush Charan, National University of Study and Research in Law, Ranchi

ABSTRACT

Due to the quick digitalization of financial institutions, the nature of economic offences has changed. Due to this the process of tracking down illegal money was made more difficult. As a result of this, in order to analyse the financial data and to build money traits across banking systems, digital payment platforms, and virtual assets, the investigation agencies have started depending upon Artificial Intelligence (AI) tools. Even though AI has improved speed, precision, and efficiency but its serious applications have presented serious evidence, legal, and constitutional issues. This article not only focuses on Indian Court system but also investigates the role of AI money trait. This study investigates the application of AI under the Bharatiya Sakshya Adhiniyam, 2023, the Income Tax Act, 1961, and the Prevention of Money Laundering Act, 2002. This article shows how AI tools are used in Prevention of Money Laundering Act, 2002, the Income Tax Act, 1961 and the Bharatiya Sakshya Adhiniyam, 2023. The study analyses how AI-enabled tools are used under statutes such as the Prevention of Money Laundering Act, 2002, the Income Tax Act, 1961, and the Bharatiya Sakshya Adhiniyam, 2023. It further evaluates judicial responses to technology-assisted investigations through key Supreme Court decisions addressing money laundering, privacy, due process, and electronic evidence. The central research problem lies in the absence of a dedicated legal framework governing AI use in financial investigations, leading to uncertainty regarding transparency, accountability, admissibility of evidence, and protection of fundamental rights. Through a comparative analysis of international practices and Indian jurisprudence, the study identifies regulatory gaps and proposes legal and institutional reforms to ensure that AI-assisted money trail investigations remain effective while conforming to constitutional principles and the rule of law.

Chapter 1: Introduction and Conceptual Framework

The rapid expansion of digital technology has fundamentally transformed financial systems across the world. Economic offences such as money laundering, corruption, fraud, and terrorist financing have become increasingly sophisticated, relying on complex banking structures, electronic transfers, shell entities, and cross-border transactions. In this evolving landscape, tracing the movement of illicit funds, commonly referred to as the money trail, has emerged as a critical component of financial crime investigations. Traditional investigative methods, which depend heavily on manual scrutiny of records and human intelligence, are often inadequate to handle the sheer volume and complexity of modern financial data.

Artificial Intelligence has emerged as a powerful technological response to these challenges. AI refers to computer systems capable of performing tasks that ordinarily require human intelligence, such as learning, reasoning, pattern recognition, and predictive analysis. In financial investigations, AI is primarily employed through machine learning algorithms, data mining tools, and network analysis systems that can process vast datasets in real time. These systems are capable of identifying unusual transaction patterns, linking seemingly unrelated entities, and predicting potential risks of financial crime. As a result, AI has become an increasingly important tool for law enforcement agencies and financial regulators seeking to strengthen their ability to trace illicit financial flows.

The concept of money trail is central to the prosecution of economic offences, particularly under anti-money laundering laws. A money trail refers to the systematic tracking of funds from their origin to their final destination to establish whether such funds constitute proceeds of crime. Money laundering typically involves three stages placement, layering, and integration each designed to conceal the illegal origin of funds. With the growth of digital banking, online payment systems, and cryptocurrencies, these stages have become more complex and difficult to detect. Establishing a clear money trail is therefore essential not only for identifying criminal activity but also for attaching property, securing convictions, and recovering illicit assets.

The intersection of Artificial Intelligence and money trail investigations represents a significant shift in the way financial crimes are detected and prosecuted. AI-driven systems enable authorities to analyse massive volumes of financial transactions, identify hidden relationships between accounts and entities, and uncover sophisticated laundering mechanisms that might otherwise remain undetected. Agencies such as the Enforcement Directorate, Financial

Intelligence Unit-India, Income Tax Department, and SEBI have begun incorporating AI-based tools into their investigative processes. While these technologies enhance efficiency and accuracy, they also raise serious legal and ethical concerns relating to transparency, accountability, and fairness in the criminal justice system.

One of the primary concerns arising from the use of AI in money trail investigations is the absence of a clear legal framework governing its deployment. Indian laws such as the Prevention of Money Laundering Act, 2002, the Information Technology Act, 2000, and the Indian Evidence Act, 1872 were enacted before the emergence of advanced AI technologies. Consequently, these statutes do not specifically address the legality of AI-generated financial intelligence, the standards for its admissibility as evidence, or the extent of human oversight required in AI-assisted investigations. This legal vacuum creates uncertainty regarding the validity of enforcement actions based on algorithmic analysis.

The use of AI in financial surveillance also raises significant constitutional concerns. The right to privacy, recognized as a fundamental right under [1]Article 21 of the Constitution of India, extends to financial information and personal data. AI-driven monitoring systems have the potential to enable continuous and large-scale surveillance of financial transactions, often without the knowledge of the individuals concerned. This raises questions regarding proportionality, necessity, and legality, particularly in the absence of explicit statutory safeguards. Additionally, the risk of algorithmic bias and discriminatory outcomes may implicate the right to equality under [2]Article 14, further highlighting the need for constitutional scrutiny.

Another critical issue relates to the evidentiary value of AI-generated outputs. Courts in India rely on established principles of evidence, including the admissibility of electronic records under [3]Section 65B of the Indian Evidence Act. However, AI systems do not merely store or transmit data; they actively analyse and interpret information to generate conclusions and predictions. This raises complex questions about reliability, explainability, and the ability of the accused to challenge or cross-examine AI-based findings. The lack of judicial standards for evaluating such evidence underscores the need for doctrinal clarity.

[1] Article 21 of Indian Constitution

[2] Article 14 of Indian Constitution

[3] Section 65 B of Indian Evidence Act

The significance of this study lies in its attempt to bridge the gap between technological innovation and legal regulation. As AI continues to reshape financial investigations, it is essential to ensure that its use remains consistent with the principles of rule of law, natural justice, and constitutional governance. This research seeks to critically examine the role of Artificial Intelligence in tracing money trails, analyse the adequacy of existing legal frameworks, identify emerging research gaps, and propose reforms aimed at achieving a balanced approach. By doing so, the study contributes to the evolving discourse on technology and law, emphasizing the need for responsible and rights-respecting deployment of AI in the criminal justice system.

Chapter 2: AI in Tracing Money Trail

The increasing complexity of financial crimes has necessitated the adoption of advanced technological tools capable of analysing vast and intricate datasets. Artificial Intelligence has emerged as a critical mechanism in tracing money trails by enabling automated processing and interpretation of large volumes of financial information. Unlike traditional investigative techniques, which rely on manual examination of bank records and financial statements, AI systems can simultaneously analyse millions of transactions across multiple platforms, thereby enhancing the speed and accuracy of financial crime detection.

One of the primary applications of Artificial Intelligence in money trail investigations is transaction monitoring. AI-driven systems continuously examine financial transactions to identify patterns that deviate from established norms. By learning from historical data, these systems can flag suspicious activities such as unusually large transfers, rapid movement of funds between multiple accounts, or repeated transactions just below statutory reporting thresholds. This automated detection plays a crucial role in identifying the initial placement and layering stages of money laundering, which are often concealed through complex transactional behaviour.

Artificial Intelligence also plays a significant role in network and link analysis, which is essential for uncovering sophisticated laundering structures. Financial crimes frequently involve multiple entities, including shell companies, benami accounts, and intermediaries, designed to obscure the true ownership and movement of funds. AI tools can map relationships between individuals, bank accounts, corporate entities, and properties by analysing transactional data, corporate filings, and communication records. This capability enables investigators to reconstruct the money trail and establish links between the proceeds of crime and their ultimate beneficiaries.

Another important application of AI in tracing money trails is the identification of shell companies and benami properties. Machine learning algorithms can analyse corporate databases, financial statements, and ownership structures to detect anomalies indicative of fictitious or front entities. Factors such as common directors, repeated addresses, circular transactions, and lack of genuine business activity can be identified through AI-driven analysis. This is particularly relevant in cases involving large-scale fraud and corruption, where shell entities are frequently used to launder illicit funds.

Artificial Intelligence has also become increasingly relevant in tracking cross-border transactions and international money flows. Financial crimes often involve the transfer of funds across jurisdictions to exploit regulatory gaps and hinder enforcement efforts. AI systems are capable of analysing international transaction data, currency movements, and correspondent banking relationships to detect suspicious cross-border fund flows. This has enhanced cooperation between domestic enforcement agencies and international financial intelligence units, thereby strengthening the global fight against money laundering and terrorist financing.

The emergence of digital currencies and virtual assets has further expanded the scope of AI in money trail investigations. Cryptocurrencies operate on decentralised platforms and provide varying degrees of anonymity, making them attractive tools for laundering illicit funds. AI-based blockchain analytics enable investigators to trace cryptocurrency transactions by analysing transaction histories, wallet addresses, and behavioural patterns. These tools help identify illicit crypto activities and link virtual assets to real-world identities, thereby extending the reach of money trail investigations into the digital domain.

In India, several enforcement and regulatory agencies have begun incorporating Artificial Intelligence into their investigative frameworks. The Financial Intelligence Unit–India utilises AI-based analytics to process Suspicious Transaction Reports submitted by banks and financial institutions. The Enforcement Directorate and Income Tax Department rely on data analytics and AI tools to identify high-risk cases, trace proceeds of crime, and attach assets under applicable laws. Similarly, SEBI employs algorithmic surveillance systems to detect insider trading and market manipulation, which often involve complex money trails.

Despite its effectiveness, the use of Artificial Intelligence in tracing money trails is not without limitations. AI systems are heavily dependent on the quality and completeness of the data they process. Inaccurate or biased datasets can lead to false positives, wrongful suspicion, or selective targeting. Additionally, excessive reliance on automated systems may reduce human oversight, increasing the risk of errors and misuse. The opacity of certain AI algorithms further complicates the ability of investigators, courts, and accused persons to understand and challenge the basis of AI-generated conclusions.

The application of Artificial Intelligence in money trail investigations represents a significant advancement in financial crime enforcement. It enhances the capacity of authorities to detect, analyse, and reconstruct complex financial transactions with greater efficiency and precision. However, the growing dependence on AI also underscores the need for legal safeguards, transparency, and accountability. The following chapters examine whether existing legal frameworks in India are adequate to regulate these technological applications and ensure that their use remains consistent with principles of fairness, due process, and constitutional governance.

Chapter 3: Legal Framework

The legal framework governing money trail investigations in India is principally anchored in the Prevention of Money Laundering Act, 2002 (PMLA), which was enacted to prevent the legitimisation of illicitly obtained money and provide for the confiscation of property derived from or involved in money laundering. Under PMLA, the offence of money laundering is defined in [4]Section 3, which criminalizes the process of concealing the origins of proceeds of crime, disguising them as legitimate income. The term proceeds of crime is defined in [5]Section 2(1)(u) and refers to any property derived or obtained directly or indirectly from criminal activity. Enforcement agencies such as the Enforcement Directorate (ED) are empowered to investigate, arrest, attach, and confiscate properties under PMLA, making this Act central to tracing money trails in financial crime investigations.

PMLA's procedural architecture grants substantial powers to the ED, allowing it to enter, search, and seize properties under [6]Section 17 and attach properties provisionally under

[4] Section 3 of PMLA
[5] Section 2(1)(u) of PMLA
[6] Section 17 of PMLA

[7]Section 5. Once attached, including movable and immovable assets, the onus shifts to the accused to prove that such properties do not constitute proceeds of crime. The rigorous nature of this regime was affirmed by the Delhi High Court in [8]Aditya Krishna v. Directorate of Enforcement (2025), where the court reiterated that once a person is charged under [9]Sections 3 and [10]4 of PMLA, the law presumes that proceeds of crime are involved unless the accused can rebut the presumption under [11]Section 24. In that case, the High Court observed that financial records, WhatsApp communications, and transactional data could form the basis of the ED's case, reflecting judicial acceptance of digital evidence in tracing money trails under PMLA.

Another important aspect of the PMLA regime is found in [12]Section 50, which empowers authorised officers to summon persons and compel production of documents relevant to an investigation. Although Section 50 empowers summons, the ED's power to arrest is expressly provided under [13]Section 19, subject to conditions like reasonable belief and recorded reasons, even as courts have scrutinised these powers in various contexts. Further procedural safeguards exist in [14]Section 8 and [15]Section 20, which lay down adjudication and confirmation processes for attached properties, requiring reasoned orders and multi-tiered checks to prevent arbitrary action.

In addition to PMLA, related substantive offences under the Indian Penal Code, 1860 (IPC) are often invoked to establish predicate offences that generate proceeds of crime. For instance, offences such as criminal breach of trust (Sections 405–409 IPC), fraud (Section 420 IPC), criminal conspiracy (Section 120B IPC), and forgery (Sections 463–471 IPC) frequently serve as the underlying scheduled offences whose proceeds are laundered and pursued under PMLA. The interplay between cyberspace frauds and conventional IPC offences underscores the evolving nature of money trail investigations in the digital age, where electronic data often forms part of the predicate offence evidence.

[7] Section 5 of PMLA

[8] Aditya Krishna v Directorate of Enforcement CRL.M. (BAIL)-2021/2024 (Delhi High Court, 28 January 2025)

[9] Section 4 of PMLA

[10] Ibid

[11] Ibid

[12] Section 50 of PMLA

[13] Section 19 of PMLA

[14] Section 8 of PMLA

[15] Section 20 of PMLA

The role of digital evidence in money trail investigations is governed by the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into effect in July 2024 and modernises the law of evidence to address technological advancements. The BSA enumerates that nothing in the law shall deny admissibility of electronic or digital records, thereby broadening the scope for digital evidence in judicial and quasi-judicial proceedings. [16]Section 63 of BSA mirrors the erstwhile [17]Section 65B of the Indian Evidence Act, codifying requirements for admissibility of electronic records, such as computer outputs, with appropriate certificates regarding integrity and reliability. The new framework also includes legal presumptions about electronic signatures and secure electronic records under Sections 90 to 93 of BSA. These provisions allow courts to treat electronic records as authentic unless their validity is actively challenged, which is particularly significant in tracing money trails that are based on digital transaction data.

The Information Technology Act, 2000 continues to be relevant, especially where offences involve computer systems, network security breaches, or digital manipulation. While the IT Act does not specifically regulate money laundering, its provisions on unauthorized access, data tampering, and cyber offences often intersect with investigations into laundered funds derived from cybercrime. Additionally, regulatory frameworks for financial markets such as the SEBI Act, 1992 impose obligations on intermediaries and market participants, and algorithmic surveillance tools under SEBI can generate alerts that feed into money trail inquiries.

Recent case law illustrates the judiciary’s evolving approach to digital evidence and money laundering jurisprudence. In [18]Adnan Nisar v. Directorate of Enforcement, a Delhi High Court decision involving cryptocurrency laundering, the court held that foreign cybercrimes can trigger PMLA proceedings in India if the offence corresponds to a scheduled offence under Indian law and the proceeds enter the Indian financial system, emphasizing the extraterritorial reach of PMLA in an interconnected digital economy. Although this decision did not directly involve AI analytics, it highlights how courts are adapting statutory interpretation to encompass digital transactions, which is relevant where AI tools generate digital linkages used as evidence.

Moreover, high-profile enforcement actions such as seizures and attachments by the ED—

[16] Section 53 of BSA
[17] Ibid
[18] Adnan Nisar v Directorate of Enforcement (Delhi HC, 17 Sep 2024)

ranging from shell company attachments in the Amrapali Group money laundering cases to raids where digital evidence and transactional records are seized reflect practical law-enforcement applications of the legal framework to pursue money trails in complex financial frauds and Ponzi schemes.

Together, the statutory provisions and case law indicate a comprehensive legal framework in India that empowers authorities to trace and prosecute money trail cases. However, the rapid adoption of digital technologies and AI analytics poses fresh challenges, particularly with respect to the admissibility, reliability, and transparency of algorithm-generated insights. Although BSA's updated evidentiary framework provides a statutory basis for digital records, there is a notable absence of jurisprudence specifically addressing AI-generated evidence. This gap necessitates a careful examination of the interplay between existing legal norms and emerging technologies, which will be explored in subsequent chapters.

Chapter 4: Evidentiary, Constitutional and Ethical Challenges

The integration of Artificial Intelligence into money trail investigations enhances analytical capacity but simultaneously raises profound challenges concerning evidentiary standards, constitutional rights, and ethical governance. Financial investigations frequently depend on digital data and algorithmically generated insights. Under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), digital records and electronic evidence have expanded statutory recognition through provisions such as [19]Section 63 and related presumptions regarding electronic signatures and secure records. While BSA's modernized provisions aim to ease the admissibility of digital materials, they were not conceived with advanced AI analytics in mind. AI outputs are not mere electronic records, but analytical interpretations and predictions derived from complex machine learning algorithms operating on large datasets. This nuance raises questions regarding reliability, explainability, and the ability of a court to treat such outputs as evidence on the same footing as traditional electronic documents.

Despite statutory reforms, courts have continued to grapple with AI-adjacent evidentiary problems, particularly concerning digital evidence obtained or processed via automated systems. While Section 63 of BSA provides for admissibility of electronic records where proper certification is furnished, neither BSA nor prior provisions like Section 65B of the

[19] Section 63 of BSA

Indian Evidence Act, 1872 explicitly address analytical evidence produced by AI. In [20]"State NCT of Delhi v. Navjot Sandhu (2005)", the Supreme Court recognised the evolving nature of electronic evidence, emphasising the need for judicial adaptation, but subsequent adjudication on AI-generated outputs remains sparse. More recently, in [21]Aditya Krishna v. Directorate of Enforcement (2025), the Delhi High Court accepted digital transactional data including messaging records and bank statements as part of the ED's evidence in a money laundering case, but the court did not directly validate algorithmically inferred conclusions as standalone proof. These decisions suggest judicial willingness to rely on digital data, yet they also underscore a gap in jurisprudence regarding how courts should evaluate and weigh algorithm-derived analytics in the absence of clear legal standards.

A principal constitutional challenge arises from the right to privacy, now firmly entrenched under [22]Article 21 of the Constitution of India, following the landmark judgment in [23]Justice K.S. Puttaswamy v. Union of India (2017). The Supreme Court held that privacy includes informational privacy, which extends to financial data. AI-enabled surveillance systems used in money trail detection, whether by law enforcement or regulatory authorities may involve large-scale processing of personal financial information. Without clear statutory safeguards, such surveillance could amount to disproportionate intrusion into individual privacy. Furthermore, the doctrine of proportionality adopted in Puttaswamy demands that state action be lawful, necessary, and proportionate. Automated analyses that sweep vast amounts of financial data for AI pattern detection must therefore satisfy these constitutional tests, yet existing enforcement statutes such as the Prevention of Money Laundering Act, 2002 (PMLA) do not expressly regulate algorithmic profiling or the thresholds for automated analysis, creating regulatory ambiguity.

A related constitutional concern involves the right to equality under [24]Article 14, particularly where AI systems exhibit bias or differential impact. AI algorithms trained on historical financial data may inadvertently reflect systemic biases, leading to discriminatory outcomes against certain demographics or economic actors. Such bias undermines the equal protection guarantee and may result in disproportionate targeting or investigation based on factors

[20] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 (SC)
[21] Ibid
[22] Article 21 of Indian Constitution
[23] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)
[24] Ibid

unrelated to actual criminality. The Supreme Court in [25]Zee Telefilms Ltd. v. Union of India (2005) underscored that state action must be non-arbitrary, a principle that extends to the use of automated systems. When AI flags suspicious activity, the absence of transparency in its decision-making can render enforcement actions arbitrary, unless explainability and review mechanisms are instituted.

Fair trial and procedural due process rights also come into tension with opaque AI systems. The principles of natural justice audi alteram partem and reasoned decision-making require that accused persons be given an opportunity to understand and challenge the basis of evidence against them. Yet many AI algorithms operate as "black boxes", generating risk scores or alerts without intelligible reasoning accessible to laypersons, defence counsel, or even judicial fact-finders. In [26]State of Telangana v. M. Saleem Basha (2022), the Supreme Court reiterated that evidence must be capable of being tested in cross-examination; however, AI outputs, particularly deep learning-based inferences, defy straightforward cross-examination unless accompanied by transparent documentation of algorithmic logic and training data. This evidentiary opacity not only impedes defense rights but also compromises the court's ability to assess reliability and probative value.

Ethical concerns extend beyond courtrooms to the governance of AI systems used in financial investigations. Accountability for errors or unintended consequences of AI analysis remains unclear under current law. When an AI system generates false positive or erroneous linkages, there is no statutory mechanism assigning responsibility to the software provider, the deploying agency, or individual investigators who rely on such outputs. The doctrine of reasonable satisfaction by a magistrate or judge, intrinsic to the Criminal Procedure Code, cannot be substituted by machine outputs without human oversight and accountability. Ethical frameworks in data protection laws such as those proposed in the Digital Personal Data Protection Act offer potential guidance, but they lack enforceable mandates specific to law enforcement analytics.

The judiciary has recently addressed related concerns in cases involving digital evidence, though not always directly confronting AI. In [27]Arnesh Kumar v. State of Bihar (2014), the Supreme Court stressed that procedural safeguards must be strictly followed before arrest,

[25] Zee Telefilms (2005) 4 SCC 649

[26] Mohammed Saleem v State of Telangana W.P. No. 11592 of 2022 (High Court of Telangana, 16 March 2022)

[27] Arnesh Kumar v State of Bihar (2014) 8 SCC 273 (SC)

recognising that automated arrest triggers if based on algorithmic flags could contravene procedural fairness. Similarly, in money laundering cases, high courts have quashed ED proceedings where procedural requirements under the criminal justice code were violated, as seen in the Patna High Court's quashing of PMLA cognizance due to non-compliance with hearing rights. These decisions highlight the ongoing role of courts in upholding procedural and constitutional rights in technologically infused investigations.

Taken together, the evidentiary, constitutional, and ethical challenges presented by AI in money trail investigations reveal a tension between technological potential and legal safeguards. While digital evidence enjoys statutory recognition and courts increasingly accept electronic records, there is a pressing need for explicit standards governing AI-generated analytics, transparency in algorithmic processing, and mechanisms to protect privacy, equality, and fair trial rights. The subsequent chapter will explore research gaps and offer recommendations to bridge these legal and technological divides.

Chapter 5: Research Gaps, Comparative Perspective and Recommendations

Despite the rapid adoption of advanced analytical technologies in financial investigations, the existing legal and regulatory frameworks in India reveal significant research gaps that demand examination and reform. One of the principal gaps lies in the absence of explicit legislative recognition and regulation of Artificial Intelligence in the context of money trail investigations. Although statutes such as the Prevention of Money Laundering Act, 2002 (PMLA) and the Bharatiya Sakshya Adhiniyam 2023 offer mechanisms for tracing proceeds of crime and admitting electronic evidence, they do not contain provisions that expressly identify or govern the use of machine learning, predictive analytics, or algorithmic decision-support systems. Consequently, investigators and courts are left to apply traditional evidence law to novel AI outputs, often without sufficient guidance regarding reliability, validation standards, provenance of algorithms, or the need for human oversight. This lacuna creates uncertainty regarding the legal status of AI-generated conclusions and the procedural safeguards necessary to ensure that such technologies do not undermine fairness and due process.

A related research gap arises from the emergent nature of AI explainability and accountability in the context of legal adjudication. Current evidentiary law emphasises admissibility and relevance, but it does not comprehensively address the burden of proof, cross-examination protocols, or standard operating procedures for the disclosure of AI-related processes and training data. The opacity of many AI models, particularly deep learning systems, poses challenges to the principles of natural justice, especially the right to an effective defence. Indian courts have accepted transactional data and digital logs as evidence, but they have not yet articulated a judicial standard for the evaluation of AI-derived inferences, making this a pivotal area for doctrinal research and legal innovation.

Comparative perspectives from other jurisdictions further illuminate both the urgency and possible contours of reform. In the European Union, the proposed AI Act seeks to classify AI applications according to risk levels and impose legal obligations for transparency, human oversight, and documentation, particularly for systems that affect fundamental rights. Similarly, the General Data Protection Regulation (GDPR) emphasises data subject rights, including explanations of automated decision-making and meaningful information about logic involved in profiling. While not directly targeted at financial crime, these frameworks offer principles relevant to AI governance, such as algorithmic accountability, impact assessments, and risk mitigation, that could inform Indian policy. In the United States, regulatory guidance from agencies such as the Consumer Financial Protection Bureau and the Financial Crimes Enforcement Network highlights the importance of human in the loop controls and periodic audits for automated monitoring systems, although the U.S. lacks comprehensive federal AI legislation. These comparative examples demonstrate that jurisdictions are increasingly recognising the need to couple AI deployment with rights-protecting safeguards.

Considering the identified research gaps and comparative insights, several recommendations emerge as integral to strengthening the legal framework governing AI and money trail investigations in India. First, there is a need to enact AI-specific legal provisions within existing statutes or through standalone legislation that clearly delineates permissible uses of AI in law enforcement, require documentation of algorithmic logic, and mandate standards for reliability and validation. These provisions should be accompanied by statutory directives for algorithmic transparency and explainability, ensuring that AI outputs used in investigations can be interpreted, challenged, and tested in adversarial proceedings.

Second, the law should require independent audits and certification of AI systems deployed by enforcement agencies. This would involve periodic technical evaluations to detect bias, errors, and unintended consequences, and to verify compliance with constitutional guarantees such as the right to privacy and equality before law. The establishment of a specialised technical authority or oversight body, possibly within the Data Protection Board envisaged under the Digital Personal Data Protection Act, could bolster accountability and provide expert oversight.

Third, judicial and prosecutorial capacity must be enhanced through training programmes that equip legal professionals with foundational knowledge of AI systems, risks of algorithmic bias, and methods for assessing digital and AI-generated evidence. Such training would enable courts to make informed decisions regarding admissibility, weight, and probative value of complex technological evidence.

Fourth, procedural rules should be amended to integrate human-in-the-loop requirements, ensuring that final investigative decisions are not based exclusively on automated systems but are subject to meaningful human review. This would preserve human judgment in critical phases such as arrest decisions, asset attachment, and evidentiary submissions, thereby aligning with constitutional principles of due process.

Finally, data protection and privacy safeguards must be strengthened to provide individuals with clear rights regarding their financial data, including notice, access, and correction rights, especially where AI systems process personal information for investigative purposes. This would harmonise money trail enforcement with the right to privacy under Article 21 and the emerging data protection regime in India.

Taken together, these reforms would address central research gaps identified in this study by bridging the divide between technological innovation and legal regulation. By incorporating comparative lessons, ensuring procedural safeguards, and fortifying accountability mechanisms, India can develop a balanced and rights-respecting regime for the use of Artificial Intelligence in tracing money trails. Such a regime would not only enhance the effectiveness of financial crime enforcement but also uphold the rule of law, transparency, and fundamental rights in a rapidly digitizing legal landscape. The conclusion that follows summarizes the key findings of this research and reflects on future directions for scholarship and policy.

Conclusion

The present study has undertaken a comprehensive legal analysis of the application of Artificial Intelligence in tracing money trails, situating technological advancement within the broader framework of criminal justice, constitutional governance, and evidentiary law. It has demonstrated that AI-driven analytical tools possess significant potential to strengthen the detection and prosecution of complex financial crimes by enabling authorities to process vast datasets, identify concealed transactional networks, and uncover proceeds of crime that would otherwise remain undetected. In an era characterised by digital finance, cryptocurrencies, and cross-border transactions, traditional investigative mechanisms are increasingly inadequate, making AI a critical instrument in modern financial regulation and enforcement.

At the same time, the research has highlighted that the Indian legal system is not yet fully prepared to regulate or evaluate the use of AI in money trail investigations. Statutes such as the Prevention of Money Laundering Act 2002 and the Bharatiya Sakshya Adhiniyam, 2023 provide a statutory foundation for dealing with financial and electronic evidence, yet they do not explicitly contemplate the unique nature of AI-generated analytics. The absence of clear legal standards governing admissibility, reliability, and judicial assessment of algorithmic outputs creates uncertainty and risks inconsistent application by investigative agencies and courts. This gap is particularly significant given that AI output often involves probabilistic inferences rather than direct factual assertions, challenging traditional evidentiary principles.

The study further establishes that the use of AI in financial surveillance and money trail detection directly engages fundamental constitutional rights. The right to privacy under [28]Article 21, as recognised in the [29]Puttaswamy judgment, imposes a duty on the State to ensure that data-driven investigations satisfy the requirements of legality, necessity, and proportionality. Similarly, the guarantee of equality before law under [30]Article 14 demands that AI systems used in enforcement do not perpetuate bias or arbitrary decision-making. The opacity of many AI models poses a serious challenge to procedural fairness and the right to a fair trial, as accused persons may be unable to effectively understand or challenge the basis on which investigative conclusions are drawn.

Ethical considerations form an equally important dimension of this inquiry. The deployment of AI without adequate safeguards raises concerns regarding accountability, transparency, and human oversight. The current legal framework does not clearly assign responsibility for errors, biases, or wrongful implications arising from AI-based analysis, nor does it mandate independent audits or ethical compliance mechanisms. This lack of accountability threatens to

[28] Ibid

[29] Ibid

[30] Ibid

undermine public confidence in both law enforcement institutions and the justice delivery system, particularly when automated tools influence decisions with serious consequences such as arrest, attachment of property, or prosecution.

Through comparative analysis, the research illustrates that other jurisdictions are progressively moving towards structured AI governance frameworks that emphasize explainability, oversight, and rights protection. These developments underscore the need for India to adopt a proactive regulatory approach that balances technological innovation with constitutional safeguards. The recommendations proposed in this study advocate for AI-specific legal recognition, enhanced evidentiary standards, judicial capacity building, and strengthened data protection mechanisms to ensure that AI functions as a decision-support tool rather than a substitute for human judgment.

In conclusion, this research affirms that Artificial Intelligence, when deployed within a clear and accountable legal framework, can significantly enhance the effectiveness of money trail investigations and contribute to combating financial crime in an increasingly complex economic environment. However, unchecked or inadequately regulated use of AI poses serious risks to fundamental rights, procedural fairness, and the rule of law. The future of AI in financial investigations must therefore be guided by principled regulation, judicial vigilance, and ethical responsibility, ensuring that technological progress reinforces rather than erodes the foundational values of the legal system.

References

A. Case Laws

1. Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC).
2. Vijay Madanlal Choudhary v Union of India (2022) 10 SCC 386 (SC).
3. Y.S. Jagan Mohan Reddy v Central Bureau of Investigation (2013) 7 SCC 439 (SC).
4. P. Chidambaram v Directorate of Enforcement (2019) 9 SCC 24 (SC).
5. State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 (SC).
6. Zee Telefilms Ltd v Union of India (2005) 4 SCC 649 (SC).
7. Arnesh Kumar v State of Bihar (2014) 8 SCC 273 (SC).
8. Anvar P.V. v P.K. Basheer (2014) 10 SCC 473 (SC).
9. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (SC).
10. State of Gujarat v Mohanlal Jitamalji Porwal (1987) 2 SCC 364 (SC).
11. Aditya Krishna v Directorate of Enforcement CRL.M. (BAIL)-2021/2024 (Delhi High Court, 28 January 2025).
12. Adnan Nisar v Directorate of Enforcement Bail Appln No 3056/2023 (Delhi High Court, 17 September 2024).
13. Mohammed Saleem v State of Telangana W.P. No 11592 of 2022 (High Court of Telangana, 16 March 2022).

B. Comparative / Foreign Case Law

14. *State v Loomis* 881 NW 2d 749 (Wisconsin Supreme Court, 2016).

C. Statutes and Legislations

15. The Constitution of India.
16. Prevention of Money Laundering Act 2002.
17. Income Tax Act 1961.

18. Benami Transactions (Prohibition) Act 1988.

19. Bharatiya Nagarik Suraksha Sanhita 2023.

20. Bharatiya Sakshya Adhiniyam 2023.

21. Bank Secrecy Act 1970 (United States).

22. USA PATRIOT Act 2001 (United States).

23. General Data Protection Regulation (EU) 2016/679.

24. Data Protection Act 2018 (United Kingdom).

25. Proceeds of Crime Act 2002 (United Kingdom).