A STUDY OF AI IN AML COMPLIANCE: ADDRESSING CHALLENGES AND ESTABLISHING LIABILITY

G.Nivveditha & S.Rajasri, B.Com. LL.B. (Hons.), SASTRA Deemed to be University

ABSTRACT

The rapid integration of Artificial Intelligence (AI) in Anti-Money Laundering (AML) processes has enhanced transaction monitoring and detection of suspicious transactions. AI mechanisms such as machine learning, Natural Language Processing (NLP), and predictive analytics are central to these advancements. However, they introduce concerns related to data privacy, security breaches, and algorithmic biases, raising questions about criminal liability in case of compliance failures. The purpose of this research is to address liability concerns surrounding AI in AML, with a focus on developers and reporting entities, considering AI's growing autonomy. The research follows a qualitative methodology by examining legal frameworks, analyzing liability models, and reviewing regulatory obligations. Major findings reveal that while AI enhances AML processes, it still requires human oversight, particularly given its lack of mens rea (criminal intent). If AI fails, liability shifts to human actors, such as developers or users. India's current legal landscape lacks direct provisions for AI criminal liability, requiring reforms that could establish AI as an artificial juridical person, enabling it to bear compliance-related liabilities. The research implies that focusing solely on AI mechanisms without considering the broader scope of risk assessments and emerging technologies leaves gaps in liability frameworks. It suggests that government guidelines on human-AI collaboration are critical, emphasizing human oversight to mitigate AI's risks. Furthermore, the research recommends establishing developer accountability, enhancing data governance, and promoting in-house regulatory measures to ensure ethical AI development and secure compliance.

Keywords: AML Compliance, AI, Criminal liability, person, PMLA.

BACKGROUND:

The Prevention of Money Laundering Act, 2002, mandates reporting entities to fulfill various obligations to prevent money laundering. Initially, automated processes dealt these obligations, but inherent risks, such as human error, inefficiencies, and limited data-handling capabilities, compromised their effectiveness. These limitations hindered financial institutions' ability to detect and prevent complex money laundering schemes, leading to delays in identifying suspicious activities and increased regulatory and compliance risks. Recently, the involvement of Artificial Intelligence (AI) has transformed the compliance landscape. Reporting entities are outsourcing AI development to resolve risks associated with automated processes, enhancing the effectiveness of compliance mechanisms. However, despite AI's benefits, reporting entities and outsourced developers face penal liability for non-compliance or facilitating money laundering, even if AI is used as a tool. As AI becomes increasingly autonomous, the current liability framework will become outdated. Holding reporting entities or developers liable for AI-driven actions will be unjust. The future necessitates granting AI legal personhood to assign responsibility for harm, enabling it to be sued and held liable in its own name. This paper explores the need for reforms in current laws to accommodate AI's evolving role in anti-money laundering compliance.

LITERATURE REVIEW:

To enhance the regulatory compliance in the financial sector, AI technologies such as ML, NLP are being advently used[1]. Even though these innovations are transforming the Indian Banking sector, it poses challenges in the risk management[2]. In the case of Anti-money laundering, Regtech solutions such as data analytics, Blockchain and machine learning, help to streamline compliance processes while addressing challenges like data privacy and regulatory hurdles[3]. As there is an increase in the usage of AI in money laundering compliance, there is a need for determining accountability. The author offers a discussion on the benefits and drawbacks of penalizing AI, as well as a cost-benefit analysis of potential solutions for crimes

[1](Jain, V., Balakrishnan, A., Beeram, D., Najana, M., &Chintale, P. (2024). Leveraging artificial intelligence for enhancing regulatory compliance in the financial sector.International Journal of Computer Trends and Technology, 72(5), 124-140.)
[2]Dr. G. Yoganandham& Mr. V. Vishnuram, Balancing Innovation and Risk: The Impact of Technological Advancements, Outsourcing, and Artificial Intelligence on the Indian Banking Sector, (2024)
[3]Muhammad Rafiq& Muhammad Khalid Sohail, Anti-Money Laundering (AML) and Regulatory Technology: A Systematic Literature Review, 12 J. Asian Dev. Stud. 74 (2023))

caused by AI[4]. It examines the application of actus reus and mens rea—two conventional legal components necessary for criminal liability—to artificial intelligence. The author devolves the concept of legal personhood for AI and the need for legal frameworks to address the accountability of the parties. It also addresses the ethical issues involved in the usage of AI[5]. Also by examining AML and legal acts, contends, artificial intelligence (AI) improves money laundering detection and prevention, but it also presents privacy and regulatory compliance issues that need for a balanced approach within current frameworks in Bangladesh[6].Therefore, the authors analyze that imposing liability may reduce the risks occurred by usage of AI in AML.

RESEARCH PROBLEM:

The Prevention of Money Laundering Act (PMLA) outlines various obligations to ensure compliance with anti-money laundering regulations, and with the rise of AI in fulfilling these obligations, reporting entities and their clients face both advantages and disadvantages. The risks associated with AI, particularly its potential to facilitate financial crimes, have been highlighted in various studies. But the steps to resolve the risk with a help of legal intervention is not being addressed. A significant gap exists in establishing a regulatory framework that assigns clear accountability to reporting entities and outsourcing service providers.

RESEARCH QUESTION:

1. Whether the risks associated by using AI in AML compliance be addressed within the existing legal framework?

2. How can the reporting entities and AI developers, be criminally liable for harm caused by AI?

3. Whether AI to be granted the status of an artificial juridical person to hold it accountable for failures in AML compliance?

[4]C.S. Jani & Prof. Dr. S.P. Rathor, A Legal Framework for Determining the Criminal Liability and Punishment for Artificial Intelligence, 45 Tuijin Jishu 1 (2024).)
[5]Hifajatali Sayyed, Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges, 10 Cogent Soc. Sci. 2343195 (2024), https://doi.org/10.1080/23311886.2024.2343195.
[6]Md Noor Uddin Milon, Gravitating Towards Artificial Intelligence on Anti-Money Laundering: A PRISMA Based Systematic Review, Int'l J. Religion, vol. 5, no. 7, 2024, pp. 303–315, doi:10.61707/py0fe669.

RESEARCH OBJECTIVE:

- To mitigate the risks faced by the usage of AI in AML compliance through the current legal framework
- To assign the criminal liability to reporting entities and AI developers for the harm caused by AI
- To examine the potential of granting AI the status of an artificial legal person to ensure accountability in AML compliance.

RESEARCH METHODOLOGY:

This study employs doctrinal methodology, analyzing primary and secondary sources such as statutes, case law and scholarly articles as to the type of AI used in compliance and its associated risks, obligations of reporting entities, holding AI criminally liable as to harmonize with the usage of AI in money laundering compliance and inform policy making and practice.

OBLIGATIONS OF REPORTING ENTITIES

As already mentioned, India passed the PMLA in 2002 with the intention of preventing money laundering and establishing a number of sanctions in connection with it. The Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and the PMLA establish the fundamental legal framework that governs Customer Due Diligence, Maintenance of records and reporting of suspicious transaction that financial institutions are required to carry out.

Under the PMLA, regulated entities[7]—referred to in legal terms as "reporting entities[8]" —must adhere to certain client identification measures when establishing an account-based commercial connection or when the client is carrying out particular kinds of transactions. Every reporting entity must verify the identity of its clients and beneficial owners using one of the following methods: (a) Aadhaar-based authentication for banking companies, (b) offline Aadhaar verification, (c) passport verification, or (d) other valid documents as notified by the Central Government.

[7]See Section 11A, PMLA and Rule 9 of the PML Rules
[8] Section 2(wa), PMLA

The author analyzes three main obligations for the compliance of AML as follows which are being deliberated under Chapter IV of the act and the said rules:

- Maintenance of records of identity of clients
- Client due diligence
- Maintenance of records of transaction

Maintenance of records of identity of clients[9]:

Reporting entities are required to maintain records of their clients' identities in accordance with rules 9 and 10, and submit an electronic copy to the Central KYC Records Registry. They must keep these identity documents, along with business correspondence, for a minimum of five years from the date of the transaction or the closure of the account. These records are to be kept confidential and can only be disclosed when legally mandated.

Client due diligence[10]:

Reporting entities are obligated to conduct client due diligence (CDD) under Rule 9 of the PML rules to confirm the identity of clients and beneficial owners prior to initiating any business relationship or transactions. They must verify clients' identities through official documentation and retain these records. When facing higher risks of money laundering or terrorist financing, they are required to implement enhanced due diligence, which may involve gathering more detailed information about the client or the specifics of the business relationship.

eKYC[11]an essential part of the broader CDD process, focuses on the digitization and simplification of identity verification. While CDD covers a range of activities, including risk assessment and continuous monitoring, eKYC specifically accelerates the identity verification process. Many organizations incorporate eKYC into their CDD frameworks to boost compliance, reduce processing times, and enhance data accuracy. By enabling real-time verification, eKYC helps prevent the onboarding of clients with false identities. Regulatory

[9]Rule 10, Prevention of Money Laundering (Maintenance of Records) Rules, 2005
[10]Rule 9, Prevention of Money Laundering (Maintenance of Records) Rules, 2005
[11]Reserve Bank of India, *Master Direction - Know Your Customer (KYC) Direction, 2016*, at 1, RBI (2016), https://www.rbi.org.in/commonman/English/scripts/notification.aspx?id=2607

authorities in several countries, such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI), now allow eKYC as a valid method for identity verification, as long as it complies with data privacy and security standards.

Maintenance of records of transaction[12]:

Each reporting entity is required to retain records of their customers' transactions to be kept for at least five years after the conclusion of the business relationship or the date of the transaction. This includes transactions such as a series of cash transactions that are connected and exceed ₹10 lakhs in a month, transactions involving counterfeit currency or forged documents and suspicious transactions, whether they involve cash or not. Reporting entities are also obligated to report certain transactions to the Financial Intelligence Unit-India (FIU-IND). Every reporting entity that is part of a group must implement group-wide anti-money laundering (AML) and counter-terror financing (CTF) policies including the policies for sharing client due diligence and risk management information by ensuring adequate confidentiality safeguards. The reporting entity is required to furnish information to the Director (presumably the Director of the FIU-IND) such as details of attempted or executed transactions and the value of such transactions within the prescribed time frame.

Usage of AI in fulfilling these obligations

AI integration has become a standard component in this rapidly developing era of technology developments, helping to streamline work and improve accuracy in a variety of sectors.

Artificial Intelligence (AI) refers to the system capable of performing tasks that typically require human intelligence. AI can range from simple algorithms to advanced systems like machine learning that enable machines to analyze complex data, adapt to new information, and even make decisions.

[12]Section 12, Prevention of Money Laundering Act, 2002

The application of specific AI technologies in regulatory compliance

AI	USAGES	ISSUES
Machine learning-Algorithm-(Learn from data and make decision)	Maintenance of records of transaction	False positives, negatives and false misrepresentation(lack of continual updates)
	Maintenance of records of identity of clients	Risk to individual privacy and data security Potential for Bias in AI algorithm
Natural language processing-(Analyze and interpret the unstructured data and make meaningful)	Customer due diligence	Data privacy and security (Unauthorized access or misuse of personal data) (outsourcing)
Predictive analytics	Maintenance of records of identity of clients	False positives or negatives

1. Machine learning[13]:

- The automation of detecting non-compliant behavior and abnormalities related to money laundering in financial transactions heavily relies on machine learning. It allows systems to learn from historical data, improving accuracy over time without human intervention. This improves detection rates and minimizes false positives, allowing for better resource allocation in investigations. AI-driven (Machine learning) AML systems excel at integrating various data, essential for creating accurate profiles of potentially risky clients.

  Issue: Privacy concern- AI systems pose serious hazards to user privacy and data security, particularly when they are used for huge amounts of data analysis and

[13](Jain, V., Balakrishnan, A., Beeram, D., Najana, M., & Chintale, P. (2024). Leveraging artificial intelligence for enhancing regulatory compliance in the financial sector.International Journal of Computer Trends and Technology, 72(5), 124-140.)

monitoring. Additionally, there is a chance that AI will add or perpetuate bias in the compliance process.

- By employing machine learning algorithms, AI systems can analyze millions of transactions to detect complex patterns to identify irregularities and fraudulent activities that human analysts might overlook. It analyzes the transaction and report in case of any suspicious activities before it results in financial loss.

  Issue: False positives, False negatives and False misrepresentation-Even though it significantly simplifies the compliance process by identifying complex patterns, its lack regular updates and training to recognize new fraud strategies increasing the likelihood of false positives, negatives, and misrepresenting transaction facts.

2. Natural Language Processing (NLP)[14]:

Natural Language Processing (NLP) aims to enable computers to understand, interpret, and generate human language in ways that are both meaningful and functional, particularly in analyzing large volumes of unstructured data and optimizing workflows.

- In the context of customer due diligence (CDD), NLP significantly enhances the automation processes, especially for organizations handling vast amounts of unstructured information. NLP can automatically extract, analyze, and verify customer data from various documents, such as passports, licenses, and financial statements, during onboarding. It also plays a crucial role in evaluating risk profiles by analyzing reports, social media posts, and other textual data sources to assess the reputational risk of customers or entities. Furthermore, NLP is essential for continuous monitoring, enabling the scanning and tracking of public records and documents to ensure ongoing evaluation of customers for new risks or adverse media.

  Issue: Data privacy and security—Even though it increases automation and efficiency for CDD, it also raises challenges about data security and privacy. As NLP processes large amounts of sensitive information from documents mentioned above there is a heightened risk of unauthorized access or misuse of personal data. Additionally,

[14] Ibid.

continuous monitoring of public records and social media posts can result in the collection of more data than necessary, potentially violating privacy regulations.

- NLP is widely used in Anti-Money Laundering (AML) efforts to analyze communications within financial institutions, ensuring adherence to regulations. It monitors emails, chats, and documents for suspicious communication or content and it also pinpoint the transactions which are vary from the normal pattern that may signal money laundering activities, raise flag for further investigation thereby enhancing detection and preventing potential AML violations.

  Issue: AI systems require large amounts of data to operate effectively, leading to concerns about data privacy and security and particularly regarding biases in algorithms. Such biases can result in unfair treatment or incorrect compliance decisions, disproportionately impacting certain groups and violating ethical standards and regulatory norms.

3. Predictive analytics[15]:

- Predictive analytics uses statistical methods and machine learning to analyze past data and predict future events or trends. In regulatory compliance, it helps anticipate potential risks, detect developing patterns of non-compliance, and enhance strategies for ensuring compliance. Predictive analytics leverages historical AML data and AI algorithms to identify potential money laundering activities before they happen. This proactive approach helps financial institutions mitigate risks, implement preventive measures early, and reduce the chance of costly regulatory penalties.

  Issue: In the context of AML compliance, the use of predictive analytics introduces certain risks and obligations for authorized personnel. It necessitates for accurate and high-quality data, as poor data can lead to false positives or negatives, impacting the effectiveness of compliance efforts. Authorized persons are also accountable for the system's performance, and failure to detect suspicious activities can result in regulatory penalties.

[15]Muhammad Rafiq& Muhammad Khalid Sohail, Anti-Money Laundering (AML) and Regulatory Technology: A Systematic Literature Review, 12 J. Asian Dev. Stud. 74 (2023))

Criminal liability of AI and its related parties

Reporting entities, including their directors and employees, face criminal liability by fines or imprisonment, for failing to comply with the PMLA, which is enforced by the RBI and FIU. As AI-driven systems increasingly conduct compliances, if it leads to algorithmic biases, false negatives, privacy breaches, or failure to fulfill obligations lead to money laundering, a serious financial crime. Liability will be determined by analyzing the role of AI, the reporting entities responsibility, and the developers' involvement in system failures are explained below.

Models of AI's criminal culpability:

Criminal liability of deterrence and punishment as attributed to entities will, the same, be applied to AI if violating the provision of the act. Also the autonomous AI complicates the issue further.

Professor Gabriel Hallvey, an Israeli criminal law expert, has proposed three models of AI culpability[16], based on the role of AI.

1. AI as a tool[17]: AI systems with limited decision making capabilities merely act as an instrument/ tool used by human to commit a crime. AI performs the actus reus but the mensrea lies with the human by which they are seen as the actual perpetrator akin to using an animal or an object for criminal purpose.

2. Liability for Foreseeable Crimes[18]: In this second model, AI developers or users may not intend to commit a crime but are negligent if they fail to foresee that their AI system could commit an illegal act and prevent the same. The principle of negligence holds that individuals are liable if a crime is a foreseeable and natural consequence of their actions.

3. Direct Liability Model—AI as a Legal Person[19]: Advanced AI systems, capable of making independent decisions, can fulfill both *actus reus* and *mens rea*, making AI

[16]Gabriel Hallevy, The Criminal Liability of Artificial Intelligence Entities - From Science Fiction to Legal Social Control, 4 AKRON INTELL. PROP. J. 171 (2010).
[17]): CS Chaitali Jani & Prof. Dr. S.P. Rathor, A Legal Framework for Determining the Criminal Liability and Punishment for Artificial Intelligence, 45 Tuijin Jishu/Journal of Propulsion Technology 1 (2024)
[18] Ibid
[19] Ibid

itself criminally liable for its actions by modifying the same legal standards applied to humans.

In the case of money laundering, AI culpability is understood via the natural probable cause model, which takes into account AI's partial autonomy while emphasizing human oversight. According to the Financial Action Task Force (FATF), financial institutions use automated methods in conjunction with human judgment and analysis, to assess risk, placing human actors responsible for identifying risks that AI may overlook for efficient AML compliance[20]. The EU AI Act requires regular human review of high-risk AI operations under article 14[21]. Noncompliance, such as failing to supervise AI, can result in fines of up to €30,000,000, or 6% of annual revenue, holding developers and users accountable[22]. As a result, people in charge of AI's deployment and management are held liable for its involvement in money laundering.

Preferable criminal liability as to strict liability for developers

The accountability of developers in the realm of AI is a critical issue that must be addressed. Several frameworks propose for no-fault liability for harm produced by AI. European Parliament[23] measures and the California AI safety bill, highlights strict liability for developers. The former distinguishes operators as front-end and backend, where the developers lie in the aspect of backend operators, who are held strictly liable, only if product liability rule doesn't apply[24], whereby acts as an escape for the operators from liability. Strict liability may have severe consequences for AI developers, such as the prohibition or destruction of their AI systems, unfairly penalizing those who have invested heavily in these technologies, as only the element of actus reas is considered and not the mens rea[25], thereby infringing human rights. It is preferable to impose criminal liability since Section 39 of the IPC allows for the assessment

[20]Financial Action Task Force (FATF), Opportunities and Challenges of New Technologies for AML/CFT (July 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.
[21]Council Regulation 2023/206, art. 14, 2023 O.J. (L 141) 1 (EU).
[22]Umut Turksen, Vladlena Benson & Bogdan Adamyk, Legal Implications of Automated Suspicious Transaction Monitoring: Enhancing Integrity of AI, 25 J. Banking Reg. (2024), https://doi.org/10.1057/s41261-024-00233-2.
[23] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))
[24]European Commission, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, pp. 39-42
[25]Artificial intelligence and criminal liability in India: exploring legal implications and challenges Hifajatali Sayyed

of voluntary acts, meaning that criminal liability would only be imposed in circumstances of negligence[26].

Criminal liability takes an elegant approach by placing the burden of proof with the prosecution to prove a causal link between human acts and AI[27]. By this, the culpability can be determined based on the developer's level of control and the degree of autonomy, which ultimately lies with the judiciary depending on each case. Since AI depends on historical data for KYC's and CDD's continuous compliance, developers may address algorithmic biases and fix flaws like false positives in the development phase. Enforcing criminal penalties on them will improve adherence and lower the risks related to AI's deficiency.

The Role of Criminal Liability in Reducing Risks and Enhanced Compliance Management

Preventing crime is a core responsibility of the state, traditionally accomplished through punitive measures designed to deter criminal behavior, incapacitate threats, and facilitate reform. These theories of punishment extend to AI systems to promote responsible usage in Anti-Money Laundering (AML) compliance[28].

Deterrence theory asserts that punishment serves as a deterrent for AI systems and their developers, users, and owners. If AI systems are involved in financial crimes like money laundering, imposing severe penalties—such as significant fines or even the destruction of the AI—can deter developers from creating harmful systems[29]. The considerable investment of time and resources in AI development makes the prospect of financial ruin a powerful incentive for creators to focus on socially beneficial and ethical AI solutions. Retribution is another theory that offers justice to victims by punishing wrongdoers, particularly in cases where AI systems facilitate crimes like money laundering[30]. Although AI lacks emotions and intentions, penalizing AI-related offenses can satisfy victims and reinforce public trust in the legal system that the state will not tolerate these crimes, thereby fostering a safer environment. Conversely, allowing AI systems to operate without punishment may instill fears of uncontrollable

[26]C.S. Jani & Prof. Dr. S.P. Rathor, A Legal Framework for Determining the Criminal Liability and Punishment for Artificial Intelligence, 45 Tuijin Jishu 1 (2024).)
[27]Ibid, 13
[28]Ibid,14
[29] Ibid.
[30] Ibid

innovations in the future. Ensuring AI accountability prevents the emergence of unchecked power, where AI could commit crimes without facing consequences[31].

Ex-Ante Deterrence and Ex-Post Compensation: Encouraging Responsible Development[32]: Imposing accountability on AI systems and their developers has two primary goals: ex-ante deterrent and ex-post compensation. Ex-ante deterrence encourages developers and users to anticipate potential risks and implement safeguards to prevent harm. Knowing that legal penalties may be imposed, entities are driven to invest more in safety measures and responsible behavior. In contrast, ex-post compensation assures that people responsible for AI-caused damage face responsibilities after the act. This fosters a culture of accountability and trust, especially in sensitive areas such as AML compliance, where AI system failures can result in inaccurate reporting or even facilitate money laundering. When developers are aware that they could be held accountable for such errors, they are motivated to produce safer, more reliable AI systems.

Granting Personhood for AI

By providing criminal liability may reduce some risks, but overtime, it may cause developers and reporting entities to focus on avoiding lawsuits rather than providing critical safety features. For Hart, "the punishment must involve pain, suffering, and unpleasant experiences." To manage the complications of accountability for reporting entities and creators, one possible approach is to give AI systems personhood[33]. The European Parliament has encouraged the European Commission to develop laws addressing 'Civil Liability of Robots,' including the grant of electronic personhood to simplify tort liability attribution[34]. Furthermore, simply imposing liability will be insufficient therefore, integrating AI into the regulatory framework as an artificial juridical person may provide a more comprehensive solution by minimizing unfair liability[35] on creators or users who lack mens rea (guilty intent).As defined in the Federal Dictionary Act of 1871[36], personhood extends beyond natural persons, it is an artificial

[31] Ibid
[32]European Parliament, Directorate-General for Internal Policies, Policy Department for Economic, Scientific and Quality of Life Policies, Artificial Intelligence in Criminal Law and Its Use by the Police and Judicial Authorities in Criminal Matters (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf
[33] Ibid
[34] Ibid
[35] Ibid
[36]Dictionary Act, 1 U.S.C. § 1 (1871).

construct of law that confers rights and obligations on entities based on certain criteria such as capacity and legal conduct.[37]The conferral of legal personality is based on three major factors: the purpose of granting legal status, historical issues and, legal need and convenience. This status bestows specific rights and duties on artificial entities, effectively representing the interests of natural persons. For example, ships, deities, and companies have all been granted legal personality in various situations to address issues that are not sufficiently addressed by current legal frameworks. Granting this designation to AI, it fosters interactions between natural persons and AI. As advancements across several areas from chatbots to regulatory compliance and risk management & prompt conversations, highlights the need to grant AI legal personhood in order to tackle fundamental legal issues such as accountability for AI caused harm, granting of same rights as of humans and other ethical issues[38]. This framework may facilitate a more harmonized relationship between AI and the legal system, especially in the case of autonomous AI. But concerns about AI abusing legal privileges, akin to companies hiding behind the corporate veil, may prevail.

Once AI's legal personality is recognized, the notion of corporate criminal culpability becomes important as it emphasizes the necessity to hold companies accountable for acts committed in the course of business, even without mensrea. The maxim "actus non facit reum nisi mens sit rea" underlines this limitation. Nonetheless, corporations incur vicarious liability for the conduct of their employees, for the act that benefit the organization. Section 11 of the Indian Penal Code (IPC) of 1860[39] defines companies as "persons" accountable for offenses, enabling them to be penalized for wrongdoing. If AI is granted legal personhood, it may be held responsible for compliance violations, notably in Anti-Money Laundering (AML) activities like due diligence and reporting suspicious transactions even though it lacks intention. Courts can impose fines and penalties, as in Standard Chartered Bank v. Directorate of Enforcement[40] (2005), which demonstrates corporate accountability by imposing penalties without imprisonment. However, this approach has several drawbacks. AI, like corporations, is a dependent entity, and the advantages or repercussions of its actions eventually influence the natural person behind it. While AI can be held liable, the primary beneficiaries—humans—continue to benefit or suffer as a result of its actions, raising concerns about true responsibility.

[37]Paton, Jurisprudence* (3rd Edn.)
[38]Turner, Jacob. Robot Rules: Regulating Artificial Intelligence. Palgrave Macmillan, 2017, p.37.
[39]The Indian Penal Code, § 11, No. 45 of 1860, India Code.
[40]Standard Chartered Bank v. Directorate of Enforcement, (2006) 4 S.C.C. 278 (India).

Connection with various acts:

For the risks stated in the preceding sections—such as false positives and data privacy/security breaches—if AI is granted personhood, or until then, the reporting entity will be held accountable or required to pay penalties under the applicable sections. If AI gains personhood, it will be considered an artificial juridical person under Section 2(s) of both the Prevention of Money Laundering Act (PMLA) of 2002 and the Digital Personal Data Protection (DPDP) Act of 2023. As a result, the appropriate legal laws would apply directly to AI, holding it accountable for failures in compliance, privacy violations, or erroneous reporting under the regulations.

Risk/Issue to be addressed	**Name of the Act**	**Section Referred**	**Exact Provision of the Act and**
False positives in AML detection	PMLA	Section 3[41]and 4[42]	Includes the person who indirectly or assist in money laundering for a rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine.
Non fulfillment of obligations	PMLA	Section 13[43]	The director of FIU - impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to Rs. One lakh for each failure.

[41]Prevention of Money Laundering Act, § 3, No. 15 of 2003, India Code.
[42]Prevention of Money Laundering Act, § 4, No. 15 of 2003, India Code.
[43]Prevention of Money Laundering Act, § 63, No. 15 of 2003, India Code.

Furnishing False Information	PMLA, 2002	Section 63	Imposes penalties for providing false information related to money laundering activities.
Risk to Data Privacy and Security, Unauthorized Access and Misuse	IT Act	Section 43A[44] and 66[45]	Controls sensitive data and negligent in imposing security practices should pay Compensation for failure to protect data. If done that act dishonestly or fraudulently punishable with imprisonment extending to three years or fine of 5 lakh rupees or both
Data security and Privacy Breach	Digital Personal Data Protection Act (DPDP), 2023	Section 8(5)[46]	A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.- Punishment- May extend to two hundred and fifty crore rupees

SCOPE & LIMITATION:

The research addresses liability upto the creation of autonomous AI for anti-money laundering, focused only on three main AI mechanisms. It eliminates risk assessment and causation factor for criminal culpability, lacks case law due to the evolving nature of AI, and ignores

[44]Information Technology Act, § 43A, No. 21 of 2000, India Code.
[45]Information Technology Act, § 66, No. 21 of 2000, India Code.
[46]Digital Personal Data Protection Act, § 8(5), No. 22 of 2023, India Code.

other evolving AI mechanisms.

CONCLUSION:

Artificial intelligences like machine learning, NLP, and predictive analytics, enhance transaction monitoring and identify suspicious transaction to improve compliance processes, particularly in AML. However, they pose concerns such as data privacy, security breaches, and false negatives, which can erode consumer trust. If AI fails due to programming faults or misuse, it is critical to hold developers and users accountable for two reasons: first, human monitoring is still necessary despite AI's autonomy; and second, AI's absence of mens rea shifts culpability to human actors. India currently lacks laws attributing direct criminal liability to AI or developers, necessitating reforms to establish frameworks for developer liability, potentially granting the status of an artificial juridical person and allowing it to bear liability for compliance lapses. Thus, a balanced legal framework is needed to reduce AI risks in AML.

SUGGESTION:

The author recommends that the government should examine human monitoring when collaborating with AI and develop guidelines for assigning accountability based on the degree of human control over AI systems. Focus on human-AI collaborative models is required that improve compliance, emphasizing human oversight to mitigate AI errors. The developer's liability to be emphasized distinctly based on their degree of control for strong data governance in financial institutions to address AI-related privacy and security concerns, ethical AI development, and human-AI collaborative models to improve transparency, security, and compliance across industries. The paper suggests investing in training and creating In-house regulators to enhance system functionality and ensure ethical, secure AI deployment.