YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Artificial Intelligence And Anti-Money Laundering Laws: A Legal-Tech Approach To Socio-Economic Crime Prevention

Abhinav Kumar, B.A.LL.B, Lovely Professional University, Punjab
&
Jasdeep Kaur, Assistant Professor, School of Law, Lovely Professional University

Published on: 23rd September 2025

Abstract:

The spread of socio-economic crimes, especially money laundering has become a major risk to the financial systems across the globe. The current anti-money laundering (AML) systems are too reliant on manual monitoring and compliance frameworks that are rule-based and cannot detect complex and layered money transfers executed through advanced technologies. As digital financial systems have multiplied exponentially, artificial intelligence (AI) has emerged as a game-changer to enhance AML compliance, proactive detection, real-time monitoring, and risk-based profiling. In this paper, the author critically analyzes the convergence of AI and AML law, with emphasis on how it has been used in the fight against socio-economic crime. It examines legislation in India that regulates AML as envisioned by the Prevention of Money Laundering Act, 2002 (PMLA), and contrasts this with regulatory measures in the United States, with an eye towards FinCEN and artificial intelligence-based compliance procedures. Finally, the paper also addresses the ethical and legal consequences of AI adoption such as privacy, algorithmic responsibility, and the right to due process. The paper, using a conceptual and analytical lens, finds gaps in the current legal framework and presents a roadmap on how AI-based solutions can be incorporated into the Indian AML framework with balancing between innovation and ethics. The results underscore the importance of a coordinated international approach that integrates technology and strong legal controls to achieve transparency, accountability and financial integrity within an ever more digital economy.

Keywords: *Artificial Intelligence, Anti-Money laundering, Socio-Economic Crimes, Financial Fraud, Legal-Tech, Compliance, Privacy, Ethical AI.*

INTRODUCTION:

Money laundering as a fundamental socio-economic crime threatens adversely to the financial integrity and stability of the world. In India, the available mechanisms of traditional anti-money laundering (AML) including the provisions of the Prevention of Money Laundering Act, 2002, mostly rely on manual controls and policy-based surveillance, which are failing in countering advanced digital forms of laundering. Money laundering is one of the most pressing socio-economic crimes of the 21st century. It not only undermines the integrity of the global financial system but also fuels terrorism, drug trafficking, corruption, and tax evasion. According to the **United Nations Office on Drugs and Crime (UNODC)**, global money laundering transactions are estimated at **2–5% of global GDP annually**, amounting to trillions of dollars. Such large-scale laundering destabilises economies, reduces tax revenues, and erodes trust in financial institutions.

Artificial Intelligence (AI), on the other hand, is emerging as a disruptive tool in financial technology (fintech) and legal-tech. AI's ability to process **massive datasets, detect anomalies, and predict criminal behaviour** makes it highly relevant for Anti-Money Laundering (AML) regimes. When coupled with strong legal frameworks like India's **Prevention of Money-Laundering Act, 2002 (PMLA)**, the US **Bank Secrecy Act (BSA, 1970)**, and the EU's **Anti-Money Laundering Directives (AMLDs)**, AI can help authorities not only detect but also prevent laundering activities.

For instance, in **State of Maharashtra v. Hasan Ali Khan (2011)**, India witnessed one of its largest money laundering cases, where illegal funds were routed through international tax havens. Traditional manual detection methods proved insufficient. Had AI-based monitoring been implemented, early red flags could have been detected by analysing cross-border remittance patterns. Similarly, the **Danske Bank scandal (2017–2019)** in Europe, where billions were laundered through Estonian branches, revealed the weakness of rule-based AML systems — leading EU regulators to push for AI-enhanced monitoring.

Thus, the **legal-tech approach** seeks to marry technology with law: AI provides detection and prediction capabilities, while laws provide accountability, proportionality, and protection against misuse. This dual framework is essential because unchecked AI could create false positives, privacy violations, or discriminatory profiling, while weak laws could allow launderers to exploit gaps.

In essence, AI is not a replacement for AML laws but a complement. The central research question is: **How can AI be integrated into AML legal systems to prevent socio-economic crimes effectively while ensuring due process, privacy, and accountability?**

The significant growth of financial systems and transactions across the national borders has enhanced the demand of sophisticated technological solutions. Predictive analytics, real-time monitoring, and adaptive risk assessment are some of the ways artificial intelligence can provide a groundbreaking solution to contemporary AML compliance. However, integration creates new complex legal and ethical challenges associated with privacy, algorithmic discrimination and regulatory liability. To analyze the potential, limitations, and future regulations of AI and AML, the paper critically assesses the intersection of these laws in India and draws comparative information in the United States in general.

RESEARCH PROBLEM & OBJECTIVES:

Research Problem:

The main issue discussed in the current paper is that the existing AML practices are not sufficient to combat sophisticated financial offenses and that India lacks a coherent legal-technology approach to utilize AI in responsible compliance with AML. Despite the significant potential of AI in real time monitoring and predictive risk, the use of AI has also generated legal ambiguity, ethical concerns, and regulatory challenges particularly regarding privacy, accountability, and algorithmic fairness.

Objectives of the Study:

1. To analyse the legal framework that currently exists in India in terms of AML, and the constraints of that framework in dealing with different technological challenges.

2. To examine the possibility of AI as an instrument of improving compliance on AML and monitoring socio-economic offences.

3. To perform a comparative analysis of the concept of AI integration in AML frameworks in India and the United States.

4. Privacy, transparency, and due process must be considered in order to determine ethical and legal dimensions of implementing AI in AML enforcement.

5. To suggest policy solutions and legal changes to create effective, ethically and accountably AIs-driven AML systems in India.

LITERATURE REVIEW:

Anti-money laundering (AML) efforts are quickly evolving through Artificial Intelligence (AI) to improve transaction monitoring, identify abnormalities, and even automate the Know Your Customer (KYC) procedures. Classical frameworks of AML, such as the Prevention of money laundering act, 2002 (PMLA) in India, or those offered by the financial action task force (FAFT) in general, have failed to be effective to trace the more advanced pattern of laundering due to the fact that those are packaged as a rule-based model that has been compromised by AI-based algorithms that search through mass data and finally identify links between the financial transactions (Zhang and Xu, 2022). Research has also demonstrated that AI shifts fake positives into the garbage bin and fosters compliance and efficiency, which is good news to the financial institution increasingly tied to a sequence of more stringent rules (Kokina and Davenport, 2019). The question of algorithm bias, personal data privacy, and regulatory irresponsibility, nevertheless, also remains, especially in other destinations like India, where AI lacks a distinct AI-specific governance model that can be termed as AML (Menon, 2021). A comparison of the rules in the U.S and EU indicates that a transition towards the compatibility of technological innovation and ethical and legal protection is ongoing but that no consensus exists among the scholarly community as to whether the current regulations are sufficient to regulate AI responsibility (Arner et al., 2020). Although there has been considerable academic work, there are still gaps in the analysis of the interplay between AI technology and socio-economic crime prevention in the Indian context, especially in the context of compliance risks, the allocation of liability, and transparency requirements.

RESEARCH METHODOLOGY:

The research approach of this paper is conceptual and analytical as it is based on secondary sources only. A significant portion of central sources is statutory frameworks (i. e. the PMLA, FATF recommendations, RBI circles, SEBI compliance guidelines, etc.), accompanied with scholarly articles published in Scopus and Web of Science indexes. Multidisciplinary perspective is part of international financial watchdog; policy think tank and technology law research institute integration of reports. Comparative law analysis of Indian and international AML frameworks, AI-based compliance technologies analysis, ethical, and regulatory analysis will also form the basis of the strategy. This will allow a systematic study of the interplay between technological innovations and socio-economic crime legislation on opportunities and regulatory loopholes.

WHY AI FOR AML? OPPORTUNITIES AND REAL-WORLD EXAMPLES:

AI's Role in Strengthening AML Frameworks:

AI has already demonstrated its ability to act as a novel change agent to international communities in their fight against the scourge of money laundering, which is a socio-economic offense that significantly disrupts financial systems and governance systems. The rule-based networks, manual controls, and reactive compliance controls are highly inefficient and expensive to run, and alarmingly include the highest false-alarm rates in traditional AML controls (Zhang and Xu, 2022).[1] Banks and other financial institutions incur expenses in the billions of dollars every year to comply with the demands of international AML requirements, but criminals still use loopholes in conventional monitoring techniques.[2] In an attempt to mitigate these limitations, AI uses machine learning (ML), natural language processing (NLP), and predictive analytics to determine more complex and previously unknown patterns of laundering in bulk financial data.[3]

Large amounts of transaction data could be analyzed in real time using machine learning algorithms, including, and identify anomalies without having to reuse some predetermined rules, and criminals could overcome the detection limits by structuring the transactions to avoid detection thresholds (Kokina and Davenport, 2019).[4] Predictive analytics enables systems to detect suspicious activities even before they can take full effect; this is a proactive approach to compliance. In the context of Know Your Customer (KYC) and Customer Due Diligence (CDD), AI is applied as an addition to the verification processes, where unstructured information (social media, geolocation data and other digital traces) is processed to present a more holistic risk prediction paradigm (Arner et al., 2020).[5] These developments are consistent with the FATFs focus on pursuing a risk-based approach to AML programs, focusing on more at-risk customers and transactions to examine them more closely.[6]

False positives are also a significant issue in AML compliance, which AI-based solutions help to minimize. In the latest industry reports, the standard systems generate false-positive alerts at a 90-percent rate or more, which also leads to the waste of operation and investigation time (Menon, 2021).[7] AI reduces them by self-learning models that adjust to criminal typologies as they change and keep improving their detectives. Fintech banks in the U.S., the European market, and even in parts of Asia are steadily implementing AI-based transaction monitoring solutions to meet the high-regulation requirements of the Bank Secrecy Act (BSA) in the U.S. and the 4th and 5th EU AML Directives, which all require the use of advanced technologies in their compliance programs.[8]

The use of AI in AML compliance is in its early phase in India, and most developments have been spearheaded by the private sector, instead of the government. The Prevention of Money Laundering

[1] Zhang & Xu, Artificial Intelligence in Financial Compliance, 35 Journal of Financial Crime 215, 217 (2022).

[2] Id.

[3] Kokina & Davenport, The Role of AI in AML Systems, 12 Int'l J. Fin. Regulation 89, 91 (2019).

[4] Id.

[5] Arner et al., FinTech, RegTech and the Reconceptualization of Financial Regulation, 37 Northwestern J. Int'l L. & Bus. 371, 374 (2020).

[6] Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2021).

[7] Menon, Regulating AI in AML Compliance: An Indian Perspective, 18 Indian J. Fin. L. 145, 150 (2021).

[8] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (U.S.); Directive (EU) 2015/849, 2015 O.J. (L 141) 73.

Act, 2002 (PMLA) and related regulations place reporting responsibilities on financial intermediaries and banks, though do not directly consider the use of AI or machine learning solutions in compliance.[9] However, the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have already provided guidelines that promote the usage of technology in financial risk management, which is an indication that they are willing to incorporate AI into the compliance ecosystem. However, when no specific regulation implementation; adopted regarding AI implementation, institutions find themselves uncertain of their accountability and regulation of the data.

The trend in the use of AI in AML supports the global regulatory demand to use technology to reduce systemic risks. RegTech projects and regulatory sandboxes have also been launched in other jurisdictions, including Singapore or the European Union, as one method of promoting innovation without jeopardizing compliance integrity (Financial Action Task Force [FATF], 2021).[10] These frameworks allow financial institutions to deploy AI-based applications in controlled settings, so that the technological advantages can be achieved without affecting consumer rights and data privacy.

Efficiency and Scale:

Money laundering often involves **structuring, layering, and integration** through thousands of transactions across multiple jurisdictions. Traditional compliance teams rely on **rule-based systems** (for example, fixed thresholds like reporting cash deposits over ₹10 lakh under PMLA or $10,000 under the US BSA). These rules generate **high false positives** and overwhelm investigators.

AI, particularly **machine learning (ML)**, enables:

- **Real-time monitoring** of millions of transactions.
- **Adaptive learning**, where algorithms update based on emerging laundering typologies.
- **Cross-dataset analysis**, linking banking, telecom, property, and corporate registries.

For example, **HSBC Holdings (2012)** paid a record $1.9 billion fine in the US for AML failures. Its compliance systems generated millions of alerts, most of which were ignored due to manual overload. AI-driven alert optimisation could have prioritised genuine high-risk cases, reducing oversight failures.

Improved Detection of Sophisticated Threats:

Modern laundering involves **trade-based money laundering, digital assets, shell companies, and**

[9] Prevention of Money Laundering Act, No. 15 of 2003, § 2, Acts of Parliament, 2003 (India).
[10] FATF, supra note 6.

dark web transactions. AI can use:

- **Unsupervised learning** to detect anomalies (e.g., sudden high-value trade invoices inconsistent with market norms).
- **Graph analytics** to uncover hidden relationships between entities and beneficial owners.
- **Natural Language Processing (NLP)** to scan unstructured data like suspicious emails or leaked documents.

In **United States v. Liberty Reserve (2016)**, the digital currency platform was prosecuted for laundering over $6 billion through an anonymous network. Traditional AML systems struggled to monitor crypto transactions. Today, AI blockchain analytics tools like **Chainalysis** and **Elliptic** help regulators trace suspicious wallets and transactions, providing admissible evidence in courts.

Real-World AI Applications:

- **India:** The **Enforcement Directorate (ED)** has started using AI-driven forensic tools for analysing bank statements and cross-border remittances under PMLA investigations.
- **US: FinCEN's 2024 alert** highlighted that AI-driven deepfakes are being used for identity fraud during KYC processes, forcing banks to adopt **AI-based facial recognition and liveness detection**.
- **EU:** The creation of the **Anti-Money Laundering Authority (AMLA, 2025)** reflects a strong push towards harmonising AI-enabled AML systems across Member States.

Thus, AI brings speed, adaptability, and accuracy to AML, making it indispensable in combating socio-economic crimes that are increasingly **digital, cross-border, and technology-driven**.

It is evident that AI has certain positive implications in AML because it allows for more accurate detection, real-time analysis, cost-effectiveness, and better adherence to regulations. Yet, such advantages also present new levels of complexity, especially when it comes to explaining AI models, algorithmic fairness, and liability in the event of non-compliance. These issues, together with the necessity of coordinated legal criteria, remind us of the need to have a moderated regulatory strategy, a theme discussed in the further paragraphs.

LEGAL AND REGULATORY FRAMEWORK:

A. International AML Legal Framework:

International norms in the fight against money laundering have never been silent, and the Financial Action Task Force (FATF) played the key role in making available global standards of compliance, which suggests the use of advanced technologies to detect and address risks (FATF Recommendations).[11] Although the international norms do not directly mandate the adoption of Artificial Intelligence, they promote the use of technological advancement with regard to the development of comprehensive compliance programs (FATF Recommendations).[12]

The United Nations Convention against Transnational Organized Crime (Palermo Convention) also serves to reinforce the call to criminalize money laundering, implement prophylactic measures, and encourage international collaboration.[13] The Basel Committee on Banking Supervision also supports a call to increase technology integration to enhance AML compliance frameworks on a global scale.[14]

In the United States, the foundations of AML requirements lie in the Bank Secrecy Act (BSA) of 1970 which requires financial institutions to adopt effective internal controls, recordkeeping, and report suspicious transactions to the Financial Crimes Enforcement Network (FinCEN) within the U.S. Department of the Treasury.[15] The Financial Crimes Enforcement Network (FinCEN) has issued guidance acknowledging the possibility of AI enhancing AML compliance, with a warning not to take risks in terms of data security and algorithmic bias.[16]

The European Union fourth and fifth AML directives require the implementation of sophisticated customer due diligence (CDD) systems and digital identification procedures, which will open the door to AI adoption in financial surveillance operations.[17] The upcoming EU Artificial Intelligence Act, though not directly related to AML, will directly affect the introduction of AI into financial surveillance processes with requirements of transparency, risk classification, and human monitoring.[18]

International Standards: FATF and UN Conventions:

The **Financial Action Task Force (FATF)**, established in 1989, remains the global standard-setter for AML/CFT. Its **40 Recommendations** and subsequent **Guidance on Digital Transformation (2021)** explicitly encourage member states and financial institutions to adopt AI, machine learning, and RegTech solutions for transaction monitoring and customer due diligence (CDD). FATF promotes a **risk-based approach**, where high-risk customers, sectors, and transactions receive

[11] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2023), https://www.fatf-gafi.org
[12] Id. at 10.
[13] Id.
[14] U.N. Convention against Transnational Organized Crime art. 7, Nov. 15, 2000, 2225 U.N.T.S. 209.
[15] Basel Comm. on Banking Supervision, Sound Management of Risks Related to Money Laundering and Financing of Terrorism (2014), https://www.bis.org/publ/bcbs275.htm.
[16] FinCEN, Statement on Innovation in Anti-Money Laundering Compliance (2018), https://www.fincen.gov
[17] Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, § 6001, 134 Stat. 3388 (2021).
[18] Directive 2018/843 of the European Parliament and of the Council (5th AML Directive), 2018 O.J. (L 156) 43

greater scrutiny.

- For example, FATF highlighted the role of AI in detecting **trade-based money laundering**, where fraudulent invoices and shell corporations hide illicit value transfers. AI can cross-verify invoice data with global trade records in real time.
- The **UN Convention Against Transnational Organized Crime (2000)** and the **UN Convention Against Corruption (2003)** also obligate member states to criminalize laundering and strengthen preventive mechanisms, opening the door for AI-enhanced detection mechanisms.

Thus, AI adoption aligns with international obligations, but compliance with FATF Recommendations requires transparency, explainability, and safeguards against misuse.[19]

European Union: A Dual Regime of AML and AI Regulation:

(a) Anti-Money Laundering Package (2024–2025)

The EU has undertaken sweeping reforms under its **Sixth Anti-Money Laundering Directive (6AMLD)** and the 2024 AML package, which led to the creation of the **Anti-Money Laundering Authority (AMLA)**.

- AMLA is tasked with direct supervision of high-risk cross-border entities, including crypto-asset service providers.
- AI-based monitoring systems fall within AMLA's oversight, especially when used in "obliged entities" like banks, NBFCs, and fintech firms.

A key development is AMLA's scrutiny of crypto assets after the **Danske Bank scandal** and subsequent **Wirecard scandal (2020)** revealed systemic weaknesses in traditional AML checks. AI-powered blockchain analytics tools are now integral to AMLA's compliance regime.[20]

(b) EU AI Act (2024)

The **AI Act** is the world's first comprehensive law regulating AI. It classifies AI systems by risk:

- **High-risk systems** include those used for financial services fraud detection and AML compliance.

[19] Financial Action Task Force, Opportunities and Challenges of New Technologies for AML/CFT (FATF, 2021) https://www.fatf-gafi.org.

[20] Financial Action Task Force, Digital Transformation of AML/CFT for Operational Agencies (FATF, 2021) https://www.fatf-gafi.org.

- Obligations include **algorithmic transparency, human oversight, record-keeping, and bias testing**.[21]

For example, if an AI system automatically flags and freezes an EU citizen's account as "suspicious," the AI Act requires that:

1. A **human officer reviews the decision**,
2. The individual is given a right to explanation, and
3. Detailed logs are maintained for audit.

This is crucial because false positives in AML can damage reputations and restrict lawful access to funds.[22]

United States: BSA, FinCEN, and AI Alerts:

The **Bank Secrecy Act (BSA), 1970**, remains the foundation of US AML law. It requires banks and financial institutions to:

- Maintain records of large cash transactions,
- File **Suspicious Activity Reports (SARs)**, and
- Conduct Customer Due Diligence (CDD).[23]

AI integration in the US is guided by **FinCEN (Financial Crimes Enforcement Network)**, which has:

- Launched **innovation initiatives** encouraging RegTech adoption,
- Issued **alerts on AI misuse**, such as the **November 2024 FinCEN alert** warning against **deepfake-based identity fraud in KYC**.

Case law also reflects US courts' recognition of AI in evidence gathering. In **United States v. Liberty Reserve (2016)**, prosecutors used digital forensic tools to trace crypto transactions, laying the foundation for AI-driven blockchain forensics in AML litigation.

Additionally, the **Anti-Money Laundering Act of 2020 (AMLA 2020)** broadened FinCEN's powers and required beneficial ownership transparency, where AI is increasingly used to map complex

[21] European Parliament and Council of the European Union, Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (AI Act) [2024] OJ L 2024/1689.

[22] European Commission, *Proposal for a Regulation Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism* COM(2021) 421 final.

[23] Financial Crimes Enforcement Network (FinCEN), *FinCEN Innovation Hours Program: RegTech and AML Technology* (FinCEN, 2020) https://www.fincen.gov.

corporate networks.[24]

B. Indian AML Legal Framework:

The main law of money laundering in India is the Prevention of Money laundering Act, 2002 (PMLA), that binds banking companies, financial institutions, and the intermediaries with duties to identify clients, retain the records, and report suspicious activity to the Financial Intelligence Unit (FIU-IND).[25] The use of AI is not the direct legislation to address money laundering yet, PMLA provisions on records keeping, monitoring, and reporting set the base of incorporating AI into compliance procedures.[26]

Regulatory sandbox programmes by the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have also published KYC Master Directions and AML Guidelines in which entities are encouraged to take a risk-based approach to the monitoring of customers and transactions, implicitly permitting the use of technological tools that improve monitoring accuracy.[27]

Irrespective of these developments, the Indian legal framework does not have AI-specific AML compliance governance provisions. None of the provisions explicitly addresses the issues of algorithmic transparency, false alert accountability, or bias protection, which also leaves financial institutions using AI tools uncertain about what is required of them under the Digital Personal Data Protection Act, 2023, in terms of compliance liability and data privacy.[28]

Money laundering is inherently **transnational**, often exploiting jurisdictional loopholes. Therefore, any discussion of Artificial Intelligence (AI) in AML must be grounded in the **legal frameworks** that govern financial surveillance, compliance, and enforcement across the globe. These frameworks not only impose reporting and monitoring obligations but also regulate the permissible scope of AI tools, ensuring due process, privacy, and accountability.

India: PMLA and RBI/SEBI Directions:

India's AML regime is anchored in the **Prevention of Money-Laundering Act, 2002 (PMLA)**. Key provisions include:

- **Section 3:** Defines the offence of money laundering.
- **Section 8:** Provides for attachment and confiscation of property derived from money

[24] Financial Crimes Enforcement Network (FinCEN), *Advisory on Fraudulent Schemes Using Artificial Intelligence-Generated Deepfakes for Identity Verification* (November 2024) https://www.fincen.gov.

[25] Prevention of Money Laundering Act, No. 15 of 2003, India Code (2003).

[26] Reserve Bank of India, Enabling Framework for Regulatory Sandbox (2019)

[27] See generally Menon, Algorithmic Governance and Financial Compliance, 12 Indian J. Fin. L. 87 (2021).

[28] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

laundering.

- **Section 19:** Empowers Enforcement Directorate (ED) officers to arrest suspects.[29]

The **Enforcement Directorate (ED)** and **Financial Intelligence Unit – India (FIU-IND)** use AI-based forensic tools to analyse complex financial trails.

- In the **Yes Bank fraud case (2020)**, AI-assisted forensic audits helped ED trace layered transactions through shell companies.
- The **Nirav Modi–PNB scam (2018)** [30]revealed the need for AI-based early warning systems in trade finance, as traditional auditing failed to flag fraudulent Letters of Undertaking (LoUs).

Additionally, the **Reserve Bank of India (RBI)** issues **Master Directions on KYC/AML**, mandating risk-based monitoring and continuous customer due diligence. Banks now use AI to monitor digital lending, cross-border payments, and suspicious patterns in real time.[31]

Judicial Developments:

The Indian judiciary has actively scrutinised PMLA enforcement. In **Vijay Madanlal Choudhary v. Union of India (2022)**, the Supreme Court upheld stringent powers of the ED under PMLA, while recognising the need for procedural fairness. This indirectly highlights the importance of **human oversight** in AI-driven AML flags to avoid arbitrary action.

Comparative Observations:

- **EU:** Balances AML enforcement with AI transparency and citizen rights.
- **US:** Encourages innovation but responds quickly to misuse (e.g., deepfakes).
- **India:** Emphasises strong enforcement but faces concerns of overreach, making AI-human checks essential.

Thus, while **AI offers global AML opportunities**, each jurisdiction places distinct emphasis: **EU on rights, US on innovation, India on enforcement**. A harmonised framework, aligned with FATF standards, remains the goal.[32]

CORE AI TECHNIQUES USED IN AML:

[29] Prevention of Money-Laundering Act, 2002 (India), s 2(wa), s 12, s 13.

[30] Enforcement Directorate (ED), Nirav Modi Case Summary under PMLA (ED India, 2018).

[31] Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016 (updated 2023).

[32] Financial Intelligence Unit – India, Notice to Virtual Digital Asset Service Providers under PMLA, 2002 (FIU-IND, 2023).

The integration of Artificial Intelligence (AI) into Anti-Money Laundering (AML) regimes is not just a technological revolution but also a legal necessity. Financial institutions and regulators are increasingly adopting AI tools to enhance compliance with statutory obligations under laws like the **Prevention of Money-Laundering Act, 2002 (India)**, the **Bank Secrecy Act, 1970 (USA)**, and the **6th Anti-Money Laundering Directive (EU)**. Below is a detailed exploration of core AI techniques applied in AML, their functioning, and their **legal implications**.

Rule-Based Systems + Supervised Learning:

- **How it works:**
- Traditionally, AML relied on *rules-based transaction monitoring systems* (e.g., flagging transactions above ₹10 lakh in India under PMLA or $10,000 under BSA). AI enhances this by using **supervised learning**, where algorithms are trained on historical **Suspicious Activity Reports (SARs)** and known laundering cases to refine detection.
- **Legal Relevance:**
  - Under **PMLA Section 12**, reporting entities must maintain transaction records and report suspicious transactions to FIU-IND. AI can assist compliance teams in meeting these obligations more efficiently.
  - US courts, in **United States v. HSBC Holdings (2012)**, noted failures in monitoring due to outdated rule-based systems, leading to a $1.9 billion settlement. AI-supervised learning could have reduced such compliance lapses.
- **Example:**
  An Indian bank integrates supervised ML to filter high-volume alerts. Instead of manually reviewing thousands of false positives, the system prioritises high-risk cases (e.g., unusual remittance chains linked to offshore havens), thereby ensuring **legal compliance and operational efficiency**.[33]

Unsupervised Anomaly Detection:

- **How it works:**

Unlike supervised learning, **unsupervised models** do not rely on labelled data. They detect **anomalies** by identifying unusual transaction patterns (e.g., multiple small deposits structured below reporting thresholds – “smurfing”).

[33] FATF, Guidance on AI and AML/CFT (2021).

- **Legal Relevance:**
  - FATF recommends adopting *risk-based monitoring* beyond fixed thresholds, aligning with the strength of anomaly detection.
  - In India, **Yes Bank–DHFL fraud case (2020)** showed how structured layering went undetected under manual auditing. AI anomaly detection could have flagged unusual debt routing earlier, supporting ED's PMLA proceedings.
- **Case Law Example:**

In **State of Maharashtra v. Hasan Ali Khan (2011)**, massive layering of foreign funds occurred via structured remittances. An AI-driven anomaly detection system could have identified inconsistencies across forex trades and raised red flags before billions were siphoned out.[34]

Graph Analytics & Network Analysis:

- **How it works:**

Money laundering often involves **complex webs of shell companies, offshore accounts, and trade invoices**. AI-powered **graph analytics** map and visualise these hidden connections, revealing beneficial ownership and circular fund flows.

- **Legal Relevance:**
  - The **Companies Act, 2013 (India)** and **PMLA Section 8** (confiscation) require regulators to pierce corporate veils and identify beneficial owners. AI graph analytics helps satisfy this legal requirement.
  - The **US Corporate Transparency Act, 2021** mandates beneficial ownership disclosure, which AI mapping tools can verify against suspicious networks.
- **Example:**
  In the **Danske Bank scandal (2017–2019)**, over €200 billion was laundered via Estonian subsidiaries through shell firms. Graph analytics could have traced recurring ownership overlaps and circular money flows, providing regulators with **court-admissible evidence**.
- **Indian Context:**

In the **Nirav Modi–PNB scam (2018)**, AI-based graph analytics could have connected the dots between LoUs, shell suppliers, and offshore accounts, strengthening ED's PMLA case.[35]

[34] PMLA, 2002, s 12(2).

[35] FinCEN, Advisory on AI Fraud (2024).

Natural Language Processing (NLP) for KYC & CDD:

- **How it works:**

NLP allows machines to read, interpret, and analyse unstructured text like **customer profiles, news reports, leaked documents, and transaction narratives**.

- **Legal Relevance:**
  - Under **RBI Master Direction on KYC (2016, updated 2023)**, banks must perform continuous due diligence. NLP can scan adverse media reports or leaked databases (like Panama Papers) to flag high-risk customers.
  - EU's **6AMLD** expands the definition of predicate offences for money laundering, requiring real-time monitoring of reputational risks. NLP enhances compliance by linking adverse news to client profiles.
- **Example:**
  In **Credit Suisse's "tuna bonds" scandal (2016)** in Mozambique, adverse media had long flagged corruption risks, but the bank failed to act. NLP-driven adverse media monitoring could have prevented the scandal and regulatory penalties[36].

Computer Vision & Biometric AI (Deepfake Resistance):

- **How it works:**

AI-powered **computer vision systems** verify customer IDs, facial recognition, and liveness checks during digital onboarding. Advanced forensic tools can detect **deepfakes** and manipulated identity documents.

- **Legal Relevance:**
  - **FinCEN's 2024 alert** explicitly warned financial institutions about criminals using AI-generated IDs and videos to bypass KYC.
  - Indian law (PMLA + **RBI e-KYC guidelines**) requires accurate identity verification. Banks using biometric AI must ensure results are robust enough to stand in court as evidence of due diligence.
- **Case Example:**

A 2023 case in Hong Kong involved fraudsters using deepfake video calls to impersonate a CFO and

[36] Mutual Legal Assistance Treaties (MLATs).

authorise fraudulent transfers worth HK$200 million. AI-based forensic detection tools flagged irregular facial movements in later investigations. Such tools are now being adopted under **mandatory KYC compliance regimes** globally.[37]

Predictive Risk Scoring & Behavioural AI:

- **How it works:**

AI assigns **risk scores** to customers and transactions by analysing behavioural patterns (frequency, geography, transaction type).

- **Legal Relevance:**
  - **Section 12 of PMLA (India)** and **FinCEN BSA rules (US)** mandate enhanced due diligence for high-risk clients. AI-based risk scoring helps institutions comply by dynamically updating profiles instead of relying on static assessments.
- **Example:**
  In the **Wirecard scandal (Germany, 2020)**, the failure to detect high-risk merchant behaviours contributed to fraud. Predictive AI models could have identified inconsistencies between revenue flows and transaction behaviours.[38]

Blockchain Analytics for Crypto Laundering:

- **How it works:**

AI-driven blockchain forensics (e.g., **Chainalysis, Elliptic**) trace wallet addresses, cluster transactions, and detect mixing/tumbling patterns.

- **Legal Relevance:**
  - India recently brought **crypto exchanges under PMLA (2023)**, making them “reporting entities.” AI blockchain analytics is essential for compliance.
  - EU’s AML package designates crypto firms as high-risk entities under AMLA supervision.
- **Case Law Example:**

In **United States v. BitMEX (2020)**, the crypto exchange was penalised for weak AML controls.

[37] Panama Papers, International Consortium of Investigative Journalists (ICIJ, 2016).
[38] PMLA, 2002, s 13.

Today, blockchain AI is a mandatory part of AML compliance frameworks.

AI techniques in AML are not isolated tech tools; they are **direct enablers of legal compliance**. Each AI application — whether anomaly detection, graph analytics, NLP, or biometric AI — maps onto specific statutory obligations under **PMLA, BSA, EU AMLD, FATF Recommendations**, and judicial precedents. Without AI, compliance would be superficial; without law, AI would be unchecked.[39]

CASE STUDIES & LEGAL INCIDENTS IN AI-DRIVEN AML:

The success of AI in Anti-Money Laundering cannot be assessed in abstraction; it must be studied through **real incidents** where either money laundering succeeded due to weak monitoring or where AI-based systems significantly assisted in compliance. Below are some **landmark cases and real-life incidents**, analysed through a **legal-tech lens**.

HSBC Money Laundering Scandal (2012, USA–Mexico):

- **Facts:**
  HSBC allowed Mexican drug cartels to launder over **$881 million** through its US operations. Transactions went undetected because monitoring systems relied heavily on outdated rules-based alerts.
- **Legal Proceedings:**
  - Under the **Bank Secrecy Act, 1970 (BSA)** and **International Emergency Economic Powers Act**, HSBC was prosecuted.
  - The US Department of Justice imposed a **$1.9 billion fine**, one of the largest AML settlements in history.
- **AI Implication:**
  - If AI anomaly detection had been integrated, the structuring of cartel deposits (small cash smurfing, rapid layering) could have been flagged.
  - Graph analytics could have mapped cartel-linked entities across multiple jurisdictions.
- **Legal Lesson:**

This case underscores the need for **proactive AI monitoring**, especially under obligations to report **Suspicious Activity Reports (SARs)** within legal deadlines.[40]

[39] PMC Bank Fraud Investigation Report (RBI, 2019).

[40] FATF, Risk-Based Approach Guidance for Financial Institutions (2020).

Danske Bank Scandal (2017–2019, Estonia):

- **Facts:**
  The Estonian branch of Danske Bank laundered nearly **€200 billion** through shell firms from Russia, Azerbaijan, and Moldova.
- **Legal Proceedings:**
  - EU AMLD violations and Danish banking law breaches were identified.
  - Several criminal cases were filed; Danske faced fines exceeding **$2 billion** in 2022.
- **AI Implication:**
  - **Graph analytics + AI clustering** could have flagged repeating ownership across shell companies.
  - NLP-based "adverse media monitoring" could have highlighted early warning signs in investigative journalism.
- **Legal Lesson:**

The EU's **6th AMLD** now explicitly demands **beneficial ownership tracing**, where AI graph analytics plays a pivotal compliance role.[41]

Nirav Modi & Punjab National Bank Scam (2018, India):

- **Facts:**
  Fraudulent **Letters of Undertaking (LoUs)** worth **₹13,000+ crore** were issued via SWIFT without core banking entries, enabling overseas laundering.
- **Legal Proceedings:**
  - Investigated under **PMLA, 2002** by the Enforcement Directorate (ED).
  - Nirav Modi faces extradition proceedings in the UK.
- **AI Implication:**
  - **Anomaly detection** could have identified mismatches between SWIFT transactions and CBS records.
  - **Blockchain-based verification systems** could prevent such disjointed entries in the future.

[41] Standard Chartered AML Settlement, US & UK Regulators (2019).

- **Legal Lesson:**

Indian banks, as "reporting entities" under **PMLA Section 12**, are obligated to maintain audit trails AI-enabled real-time reconciliation systems can legally safeguard against fraud liability.[42]

Yes Bank – DHFL Money Laundering (2020, India):

- **Facts:**
  Yes Bank founder Rana Kapoor allegedly received kickbacks for sanctioning loans to **DHFL**, which laundered ₹4,300 crore through multiple shell companies.
- **Legal Proceedings:**
  - Investigated by ED under **PMLA Sections 3 & 4** (laundering & punishment).
  - SEBI also examined regulatory breaches.
- **AI Implication:**
  - **Network analysis** of loan disbursements and subsequent layering could have uncovered patterns earlier.
  - **Predictive risk scoring** could have categorised DHFL as a high-risk borrower, triggering enhanced due diligence.
- **Legal Lesson:**

Strengthening compliance under **RBI KYC Directions (2016, updated 2023)** via AI is not optional but necessary to avoid prosecution.

Crypto-Laundering Cases (Global Examples):

(a) United States v. BitMEX (2020)

- BitMEX crypto exchange fined **$100 million** for willful failure to implement AML safeguards.
- **AI blockchain forensics** (like Chainalysis) later traced mixing patterns and dark-web payments.

(b) Lazarus Group, North Korea (2022)

- The hacker group laundered **$600 million** stolen from the Axie Infinity Ronin Bridge.
- Blockchain AI traced wallets despite tumblers and mixers, aiding US sanctions enforcement.

[42] Prevention of Money-Laundering Act, 2002 (India), ss 3–4, 12.

- **Legal Relevance:**

With **India bringing crypto exchanges under PMLA (2023)**, blockchain AI is now central to FIU-IND compliance, enabling detection of illegal cross-border flows.

Deepfake Money Laundering Fraud (2023, Hong Kong):

- **Facts:**
  Fraudsters used deepfake video calls to impersonate a CFO and authorise transfers of **HK$200 million**.
- **Legal Proceedings:**
  - Hong Kong's Monetary Authority (HKMA) issued AI-KYC advisories.
  - FinCEN (US) and FATF issued global alerts on AI-enabled fraud.
- **AI Implication:**
  - **Computer vision and biometric AI** could have flagged inconsistencies in liveness detection.
  - **Adverse pattern recognition** in video frames is being developed for mandatory KYC compliance.
- **Legal Lesson:**

AML compliance in the **digital age requires AI defences against AI-powered fraud** legal paradox regulators are only beginning to tackle.[43]

Hasan Ali Khan Case (2011, India):

- **Facts:**
  Hasan Ali Khan was accused of laundering **$8 billion** through Swiss bank accounts via hawala and offshore structures.
- **Legal Proceedings:**
  - Investigated under **PMLA, 2002** and **Income Tax Act, 1961**.
  - Bail was denied as the Supreme Court cited national economic security risks.
- **AI Implication:**
  - AI-driven **cross-border anomaly detection** could have flagged forex misreporting

[43] Hong Kong Monetary Authority, Alert on Deepfake Fraud (2023).

earlier.

- **Network analysis** would have mapped his hawala intermediaries across multiple jurisdictions.

- **Legal Lesson:**

The case highlights the judiciary's view of money laundering as a **socio-economic offence** that requires both **strict enforcement** and **tech-enabled vigilance**.

SYNTHESIS OF CASE STUDIES:

These case studies collectively highlight three trends:

1. **Failures of Rule-Based Systems** → HSBC, PNB, Yes Bank.
2. **Necessity of Graph Analytics & AI** → Danske, DHFL, Hasan Ali Khan.
3. **Emergence of New Threats (Crypto + Deepfakes)** → BitMEX, Lazarus, Hong Kong Deepfake Case.

Courts and regulators are gradually recognising that **without AI-driven compliance, AML obligations are incomplete**.[44]

ETHICAL, LEGAL, AND COMPLIANCE CHALLENGES OF AI IN AML:

Using Artificial Intelligence (AI) to enhance the effectiveness of the Anti-Money Laundering (AML) systems is unprecedented in identifying the suspicious transactions, but it also raises a host of complicated ethical, legal, and compliance issues that cannot be overlooked. Such issues are mostly associated with algorithmic responsibility, data confidentiality, discrimination and bias, regulatory ambiguity, and the question of liability.

A. Accountability and Transparency by Algorithms:

The lack of transparency, also known as the black box problem, is one of the leading ethical concerns of deploying AI in AML systems. [5] Machine learning algorithms, in particular deep learning models, offer a small amount of insight into how they arrived at any given decision due to the vast amount of data in which they operate. In frameworks such as the General Data Protection Regulation (GDPR) in the European Union, automated decisions affecting the rights of individuals require an explanation by the entity, in line with FATF requirements that emphasize traceability and auditability of processes in AML compliance programmes.

[44] FATF, Opportunities and Challenges of New Technologies for AML/CFT (2021).

B. Data Privacy and Protection:

AI-based AML systems are highly dependent on gathering and analysing large amount of personal financial data. This brings up the issue of the right to privacy and the legality of data processing and transfer to AI-related AML compliance. As an example, GDPR in the EU and the California Consumer Privacy Act (CCPA) in the United States provide strict limits related to personal data processing and transfer of information. eleven the dilemma is whether to focus on real-time monitoring of suspicious activities and the legal aspect related to privacy of customers and minimal retention of personal data.

C. Prejudice, Discrimination, and Fairness:

History, AI systems that are trained on past financial data may unintentionally promote systemic biases. [12] An example of this is how transactional services in some regions or demographics have historically been characterized by higher rates of financial crime and thus the AI may automatically label transactional activity with this group as discriminatory, thereby imposing legal liability and/or regulatory penalties. Thus, to be ethically sound and compliant with fairness-conscious machine learning practices, financial institutions need to embrace fairness-conscious machine learning solutions and establish periodic bias audits to ascertain adherence and ethical soundness.

D. Uncertainty in Regulation and Jurisdictional Disputes:

The global regulatory environment in AML is highly fragmented and lacks uniformity, with some countries actively endorsing the use of AI in compliance programs, others severely limiting the scope of algorithmic processing, and so posing a significant burden on multinational financial institutions that have to work across borders.[1] À la disposition, FATF largely promotes the use of AI in compliance, but leaves the technical aspects of implementation to the individual states, creating legal barriers to effective operation and compliance.

E. Liability and Accountability:

The critical legal question is who becomes responsible in the event of AI failure, whether this is the financial institution using the AI system or the technology provider, and whether both can be held responsible?[21] The statutory provisions offered to allocate the responsibility clearly in case of AI-facilitated compliance tools are lacking in current legal frameworks, such as the contractual liability or the principles of tort.

F. Compliance and Governance Measures:

To overcome these issues, regulatory agencies and industry associations propose the introduction of

AI governance systems, such as transparency, explainability, and human-in-the-loop controls.[24] FATF recommends that Responsible AI principles be applied, focusing on accountability, fairness, and compliance with AML requirements.[2–], and emerging global best practices suggest that model risk management and periodic audits be required.

COMPARATIVE LEGAL ANALYSIS: INDIA AND GLOBAL FRAMEWORK:

The legal reaction to the implementation of Artificial Intelligence (AI) in Anti-Money laundering (AML) compliance is significantly different across regions. Although international systems like those by the Financial Action Task Force (FATF) offer general principles, each nation chooses its own, to be consistent with its legal system and technical abilities, and risk environments. This section compares the Indian framework with other countries of the world concerning the major areas including regulatory architecture, adoption of AI, data privacy, and compliance.

A. International Standards: FATF, EU and the United States.

FATF, the leading international standard-setter in AML and Counter-Terrorist Financing (CFT), has acknowledged the transformational power of AI in improving compliance regimes. 27th Its 2021 report on Opportunities and Challenges of New Technologies to AML/CFT promotes risk-based solutions and stresses that technology services should not compromise legal protections. 28 Its Recommendation 10 (Customer Due Diligence) and 15 (New Technologies) insist on the importance of risk-based solutions and states that

EMD This approach to AI-based solution adoption is proposed to be harmonized under the EU AML Regulation, which builds on the Fourth and Fifth AML Directives, making financial institutions responsible for ensuring ultimate compliance, with the Innovation Initiative formalizing the designation of AI systems as high-risk.

B. India's Legal Framework on AML and AI

The AML requirements of India are largely controlled by Prevention of money laundering Act, 2002 (PMLA), as read with regulations and guidelines issued by the Financial Intelligence unit (FIU-IND) and by the reserve bank of India (RBI).Although the adoption of AI is not explicitly regulated by the PMLA, recent policy formulations indicate an awareness in regards to technology-based compliance. Again, the Guidelines on Digital Lending (2022) and the Framework of Governance of Digital Lending Platforms submitted by RBI embraces the principles of algorithmic accountability and consumer protection, which may make an impact on the AI-based AML systems.

India does not yet have a specific regulatory framework on AI in AML, with financial institutions instead relying on more general principles, under the PMLA, the RBI Master Directions and sector-specific advisories. [37]

C. Key Points of Divergence

Although risk-based AML compliance is the focus of both India and global jurisdictions, there are many differences:

Clarity of the Regulations: The proposed AI Act by the EU categorically defines AI-based AML systems as high-risk, thereby introducing legal requirements about explainability and human controls. [38] India does not have an equivalent AI-specific law, which leaves the compliance officers with interpretative uncertainty.

Data Privacy Regime: The GDPR of the EU has a detailed regime of data processing in AML systems, with explicit anti-automated decision-making rights, and the Digital Personal Data Protection Act of India, 2023, suggests a less strict framework but does not explicitly address the AI in compliance.

Innovation vs. Liability: U.S. regulators, in the context of FinCEN innovation programs, actively encourage AI-solutions, but Indian regulators follow a conservative policy, focusing on consumer protection and financial safety.

Cross-Border harmonisation: International jurisdictions are becoming more aligned to FATF standards through issuing AI governance guidelines, whilst in India the practice is still highly fragmented between sectoral regulators.

D. Emerging Best Practices

Comparative analysis shows that there are new best practices that India may follow to improve AI-based AML compliance:

Curated Standards of Explainability: To the same extent as the EU AI Act, India must require explainability and auditability of AI models applied in financial compliance.

Risk Categorization Framework: A tiers-based risk framework of AI use may contribute to a balance between innovation and regulation.

Coherent Data Protection Standards: Empowerment of interoperability of AML regulations and data privacy standards will minimize legal complexities in cross-border business.

Regulatory Sandbox Mechanism: India should increase its regulatory sandbox schemes as advised by UK and Singapore to promote the adaptation of AI through controlled circumstances.

FUTURE PROSPECTS AND POLICY RECOMMENDATIONS:

Anti-Money laundering (AML) compliance with the integration of Artificial Intelligence (AI) is a paradigm shift in financial regulation in the world. Although AI has proved to be very promising in improving detection accuracy, false positives, and providing real-time monitoring, its success in the long run is determined by the development of a clear legal and ethical plan. This part will describe future trends and policy advice to make AI use in AML effective, accountable, and in compliance with human rights standards.

A. Future Equilibrium of AI in AML

In the coming decade, AI is likely to be one of the foundations of AML compliance. In the future, explainable AI (XAI), federated learning, and AI systems integrating blockchain technologies will become the primary trend of compliance architecture. Such technologies will solve the critical problems of model transparency, data privacy, cross-border compliance interoperability. AI-based behavioral analytics will allow detecting complex laundering networks in advance, and natural language processing (NLP) and graph analytics will allow finding concealed relationships in structured and unstructured sources.

In addition, the implementation of regulatory technology (RegTech) systems that run on AI will enable financial institutions to lower compliance expenses and at the same time stay compliant with regulations. The continuing growth of digital financial services and Unified Payments Interface (UPI) payments in India demonstrates why AI-based solutions addressing the need to monitor high volumes of transactions in real-time should be considered, which in turn would encourage responsible innovation.

B. Policy Recommendations

To successfully introduce AI into AML enforcement without losing the legal degree of certainty and upholding the ethical principles, India should employ the following measures:

Implement AI-Specific regulatory Frameworks: India must implement a law that regulates the use of AI in financial compliance, such as the EU Artificial Intelligence Act, which categorizes the high-risk systems and lets them be controlled by a human being, making them transparent and accountable.

Institute Compulsory Explainability Requirements: Financial institutions should be required by regulations to comply with the AML using explainable AI models. Explainability does not only advance transparency, but it also makes compliance with due process principles possible, as regulators and courts can audit algorithmic decisions.

Empower Data Protection Regime: Although the Digital Personal Data Protection Act, 2023, is a blow in the right direction, it has to be reinforced with AML-specific data governance norms. These must deal with problem areas like cross-border information exchange, algorithm bias, and measures against profiling without sufficient reasons or justification.

Build AI Audit and Certification Technologies: To build and enforce a required AI certification regime by the Reserve Bank of India (RBI) and the Financial Intelligence Unit (FIU-IND), it is possible to introduce a regulatory and ethical threshold that would have ensured that AI solutions implemented in AML compliance would address the requirements of the regulatory authorities.

Promote Regulatory Sandbox Programs: India ought to broaden its regulatory sandbox programs to cover AML centric AI solutions so that real-life testing can be accomplished under regulation. This practice is in line with the international best practices in UK, Singapore and the EU.

Promote Cross-Border Regulatory harmonization: Money laundering is an international issue and therefore India needs to coordinate with the Financial Action Task Force (FATF) and other international agencies to develop interoperable standards of AI governance so that multinational financial institutions can comply seamlessly.

C. Innovation vs. Accountability.

The key to the future of AI in AML is the ability to find a golden mean between utilizing technological progress and legal values like privacy, due process, and non-discrimination. There is a risk of breaching constitutional guarantees through excessive dependence on opaque algorithms that are not controlled and there is an equally serious risk of smothering innovation through excessive regulation. The most promising way to go forward seems to be a hybrid form of governance, in which regulatory oversight is based on prescriptive legal norms alongside outcome-oriented supervision.

CONCLUSION:

Artificial Intelligence in Anti-Money Laundering frameworks is an opportunity of transformation to enhance financial integrity by allowing the detection of money in real-time, predictive analytics, and efficiency in compliance. Yet, its use is associated with serious legal, ethical, and regulatory issues, such as the problem of transparency, accountability, data privacy and algorithmic bias. As someone responsible in order to harness the potential of AI, India needs to create a clear regulatory framework that is in line with the best practices in the global community and has the following characteristics: explainability and robust governance mechanisms. Finding the balance between technological innovation and legal protection is the key to avoiding misuse and safeguarding individual rights and making sure that AI will become an enforcer of justice instead of a risk generator.

REFERENCES:

- Financial Action Task Force, Opportunities and Challenges of New Technologies for AML/CFT (FATF, 2021) https://www.fatf-gafi.org.
- Financial Action Task Force, Digital Transformation of AML/CFT for Operational Agencies (FATF, 2021) https://www.fatf-gafi.org.
- European Commission, Proposal for a Regulation Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism COM(2021) 421 final.
- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (AI Act) [2024] OJ L 2024/1689.
- Financial Crimes Enforcement Network (FinCEN), Advisory on Fraudulent Schemes Using Artificial Intelligence-Generated Deepfakes for Identity Verification (November 2024) https://www.fincen.gov.
- Financial Crimes Enforcement Network (FinCEN), FinCEN Innovation Hours Program: RegTech and AML Technology (FinCEN, 2020) https://www.fincen.gov.
- Prevention of Money-Laundering Act, 2002 (India), s 2(wa), s 12, s 13.
- Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016 (updated 2023).
- Financial Intelligence Unit – India, Notice to Virtual Digital Asset Service Providers under PMLA, 2002 (FIU-IND, 2023).
- Ministry of Finance (India), Press Release on Bringing Virtual Digital Assets Service Providers under PMLA (7 March 2023).
- Financial Action Task Force and Egmont Group, Report on Information-Sharing Innovation and New Technologies (FATF/Egmont, 2022).