aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

Smart Compliance or Silent Violation? Human Rights Challenges in Indonesia's AI-Based AML Frameworks

Kartini Laras Makmur
University of Warwick-UK

Corresponding author: Kartini.Makmur@warwick.ac.uk

Keywords:
Artificial Intelligence, Human Rights, Money Laundering

Submitted: 13 November 2024
Accepted: 24 June 2025
Published: 27 June 2025

Abstract

Artificial intelligence (AI) is increasingly used by banks to detect and prevent money laundering; however, the adoption of AI-based anti-money laundering (AML) frameworks raises significant concerns regarding human rights protection. This paper examines the ways in which AI enhances AML efforts in the banking sector, the ethical and human rights challenges that arise from its implementation, and the extent to which these strategies comply with the proportionality test under Indonesian human rights law. Using a structured document analysis of relevant regulations and secondary literature, this study finds that AI applications must respect privacy and be proportionate in addressing money laundering offences, as affirmed by the Indonesian constitution and regulatory framework. The findings highlight the urgent need for comprehensive legal frameworks to guide the development and use of AI in AML, ensuring fairness, accountability, and transparency while safeguarding human rights.

***To cite this article*:** Makmur, K. L. 2025. *Smart Compliance or Silent Violation? Human Rights Challenges in Indonesia's AI-Based AML Frameworks. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 3(2):249-270, https://doi.org/10.59593/amlcft.2025.v3i2.251

Introduction

The issue of money laundering presents a significant threat to financial institutions and society as a whole. The effects of money laundering on the economy are well established, as it promotes the growth of illegal businesses, which can destabilise the economy.[1] Illicit financial activities have the potential to undermine economic equilibrium by fostering unemployment and inflation, reducing economic potential, and diverting sources required to fund public goods such as education and health services, national defence and security, infrastructure, and justice.[2]

[1] Ayodeji Aluko and Mahmood Bagheri, "The Impact of Money Laundering on Economic and Financial Stability and on Political Development in Developing Countries: The Case of Nigeria," *Journal of Money Laundering Control* 15, no. 4 (2012): 442–57, https://doi.org/10.1108/13685201211266024.

[2] Kartini Makmur and Ahsanul Minan, "Money Laundering/Financing of Terrorism Risks in the Indonesian Islamic Banking System," in *Proceedings of the 3rd International Conference of Islamic Finance and Business, ICIFEB 2022, 19-20 July 2022* (The 3rd International Conference of Islamic Finance and Business (ICIFEB 2022), Jakarta, Indonesia: EAI, 2023), 10–21, https://doi.org/10.4108/eai.19-7-2022.2328202.

Money laundering is used by individuals involved in unlawful activities to conceal the sources of their illegal profits. The main predicate crimes of money laundering in Indonesia include corruption, organised criminal activity, financial fraud, illicit drug transactions, and funding for terrorist activities.[3] Money laundering encompasses a range of activities, including the movement of illicit funds or assets, the acquisition, transformation, or utilisation of unlawfully obtained profits, and the provision of advice, support, and aid in money laundering efforts.

Although the most comprehensive estimates currently available only cover the period between 1989 and 2017, they indicate that Indonesia experienced cumulative illicit financial inflows of approximately USD 101.49 billion and outflows of around USD 40.58 billion from its top six export commodities.[4] The annual illicit capital outflow in Indonesia constitutes approximately 10% of the nation's state budget, while the influx of illicit capital equates to roughly 29%.[5] More recent data remain unavailable, underscoring the persistent challenges in tracking illicit financial flows with precision

Financial institutions persist as the primary channel for facilitating these unlawful endeavours, with around 50% of financial organisations expressing a willingness to dedicate resources towards improving and optimising technology as a critical element of their investment plan to combat money laundering operations.[6] It is estimated that banks in the Asia Pacific region increased their investment levels towards compliance technology throughout the year 2022.[7] Based on the findings of Lexis Nexis, 49% of banks reported an expectation of budgetary growth, with an additional 34% expressing their expectations of a significant increase.[8] Banks in Indonesia, Australia, Thailand, and the Philippines have indicated their desire to invest significantly in 2023.[9]

AI is expected to become the prevailing technology in the financial sector's efforts to address the issue of money laundering. Banks have been testing AI for several periods, assisting analysts in reviewing compliance and improving the performance of AML frameworks. There are five distinct methods by which AI enhances the existing AML systems. These methods include the automation of data collection, the redistribution of resources through client risk scoring and alert prioritisation, the utilisation of link analysis, segmentation, and the improvement of anomaly detection.[10] These improvements can be attained by identifying suspicious patterns or uncovering novel patterns.[11]

However, the integration of AI in AML efforts has raised concerns regarding the protection of human rights, necessitating robust safeguards. Key issues in this context include ethics, governance, accountability, and privacy, which have gained increased prominence due to the rapid advancement of machine learning technologies. Addressing these complex and interrelated challenges requires aligning AI-based AML strategies with human rights principles,

[3] Kartini Laras Makmur, "Women and Dirty Money: How Women Are Affected by, Involved, and Counter Money Laundering," *Jurnal Hukum Prasada* 9, no. 1 (2022): 35–44, https://doi.org/10.22225/jhp.9.1.2022.35-44.

[4] Widya Kartika et al., "Highlighting Illicit Financial Flow of Indonesia's Top Six Export Commodities," *Prakarsa Policy Brief* 17 (2019): 1–4.

[5] Kartika et al.

[6] Digital Finance, "Asia Banks Spend $45 Billion on Compliance – For What?," *Digital Finance*, March 13, 2024, https://www.digfingroup.com/compliance-lexisnexis/.

[7] Digital Finance.

[8] Digital Finance.

[9] Digital Finance.

[10] Howard Chitimira, Elfas Torerai, and Lisa Jana, "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector," *Potchefstroom Electronic Law Journal* 27 (2024): 1–30, https://doi.org/10.17159/1727-3781/2024/v27i0a18024.

[11] Chitimira, Torerai, and Jana.

particularly in Indonesia, where diverse cultural beliefs add further dimensions to the ethical and regulatory landscape.

This paper offers a distinctive contribution by situating the use of AI in AML within Indonesia's specific legal framework. Unlike prior studies that often focused on European or global contexts and grounded in international standards like the Financial Action Task Force (FATF) recommendations, the European Union General Data Protection Regulation, or the European Convention on Human Rights,[12] his study applies Indonesia's proportionality test under Article 28J of the 1945 Constitution, alongside domestic laws such as Law No. 8 of 2010 on AML and Law No. 19 of 2016 on Electronic Information and Transactions. Bertrand et al., for instance, who also highlight AI's potential to enhance AML through automation of CDD (Customer Due Diligence), KYC (Know Your Customer) and transaction monitoring, critique AI's human rights risks using EU legal standards.[13] In contrast, this paper examines how AI is actually deployed in Indonesian banks and evaluates these practices against ethical and constitutional principles in a context marked by a developing privacy regime and a lack of AI-specific regulation. By offering a constitutionally grounded, localised analysis, it fills a gap in the literature, particularly for Indonesia and other Global South countries facing similar challenges. Since Europe operates within a mature regulatory environment, but Indonesia relies on fragmented laws and industry practices, illustrating a broader global risk that AI-based AML may violate human rights without strong oversight and legal safeguards.

The novelty of this paper lies in its threefold contribution. First, it offers a unique integration of AI, AML frameworks, and Indonesian human rights law by systematically applying the proportionality test that is rooted in European jurisprudence to Article 28J of the Indonesian Constitution, thereby localising a transnational legal tool to assess AI compliance within the Indonesian context. Second, the paper provides a grounded assessment of AI use in Indonesia's AML practices, moving beyond global theoretical discussions to map how specific technologies such as machine learning for transaction monitoring, e-KYC systems, and risk-scoring algorithms that interact with national legal obligations, particularly those imposed by institutions like the Indonesian Financial Transaction Reports and Analysis Center (PPATK), while highlighting their associated legal and ethical risks. Third, it advances a novel legal reform proposal to amend Indonesian AML legislation by introducing post-reporting notification rights for individuals flagged by AI systems, contingent upon law enforcement justification, thus promoting a balance between transparency and investigative integrity in line with constitutional and international human rights standards as an approach not yet addressed in existing AI-AML literature.

This paper is a descriptive-normative legal study that examines the use of AI technologies in AML systems, focusing on their integration into banking compliance functions like CDD, KYC, and transaction monitoring. It discusses both the operational benefits and the legal-ethical challenges of AI deployment, including concerns about privacy, algorithmic bias, and human rights. Using the proportionality test as a constitutional framework, the paper argues for regulatory safeguards to ensure AI-based AML strategies align with Indonesia's 1945 Constitution and human rights standards.

This paper employs a desk study methodology to investigate AI-based money laundering detection compatibility in the Indonesian banking industry with human rights principles. The

[12] See Martin Jullum et al., "Detecting Money Laundering Transactions with Machine Learning," *Journal of Money Laundering Control* 23, no. 1 (2020): 173–86, https://doi.org/10.1108/jmlc-07-2019-0055; Astrid Bertrand, Winston Maxwell, and Xavier Vamparys, "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?," *SSRN Electronic Journal* (2020): 1–27, https://doi.org/10.2139/ssrn.3647420.

[13] Bertrand, Maxwell, and Vamparys, "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?"

document analytical method is used to examine the regulatory dimension of AI-based anti-money laundering techniques. The study focuses on understanding the source of legal statutes and thoroughly examines what the limitation clause means by using the proportionality test.

The paper aims to explore how the proportionality test can be employed to address the issue of AI-based money laundering prevention in the Indonesian banking industry while ensuring the protection of human rights. The proportionality test ensures that AI-based AML frameworks in Indonesia do not violate fundamental human rights, such as privacy and due process, by requiring that any restrictions be lawful, necessary, and minimally intrusive. As AI technologies in AML become more powerful and pervasive, the proportionality test provides a legal and ethical framework to assess whether their use is justified and balanced.

The results of this study could enhance the efficacy of anti-money laundering efforts in the Indonesian banking industry. This paper offers a valuable conceptual and legal analysis of how AI is employed in AML practices and how these technologies intersect with human rights concerns. However, several research gaps remain, notably the absence of empirical data on how AI-based AML tools function in practice, how algorithmic decisions are made, and how flagged individuals are affected. The study also lacks perspectives from rights-holders themselves, leaving unexplored the lived experiences of those potentially subjected to discriminatory profiling or surveillance. Moreover, while this paper highlights Indonesia's regulatory gaps, it does not fully investigate the institutional and political dynamics shaping AI governance, nor does it offer a comparative view of how other countries with similar contexts are addressing these challenges. Lastly, although the proportionality test is introduced as a key legal standard, this paper does not explore how it is enforced or interpreted by Indonesian courts.

AI Utilisation in AML Strategies

In 1955, Dartmouth College math professor John McCarthy introduced the groundbreaking term "artificial intelligence," setting the stage for a transformative field.[14] AI is a specialised field of computer science that focuses on developing algorithms and systems that enable machines to exhibit cognitive abilities like humans.[15] The development of "intelligent" machines capable of exhibiting human-like thinking, communication, and behaviour has proven to be effective.

AI encompasses several significant subfields, one of which is machine learning. Machines possess the capability to acquire knowledge by processing and assimilating data autonomously. Machine learning facilitates the autonomous acquisition of pattern recognition capabilities and predictive abilities by a system.[16] One crucial element of supervised machine learning is human intervention in the utilisation of a labelled dataset, which includes attributes such as age, payment, time, and locations to train the model.[17] Subsequently, the database should be appropriately categorised to get the intended effect, such as facilitating the approval process for credit card applications.[18] On the contrary, unsupervised learning is a technique that involves the construction of a machine learning model without the utilisation of labelled training data or human intervention.[19]

Financial institutions have incorporated AI technology into their systems to identify and mitigate criminal activities, including money laundering. The efficacy of the banking system

[14] Gil Press, "Artificial Intelligence (AI) Defined," *Forbes*, August 27, 2017, https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/.

[15] Chitimira, Torerai, and Jana, "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector."

[16] Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."

[17] Jullum et al.

[18] Jullum et al.

[19] Jullum et al.

is contingent upon the veracity of the information provided by consumers, which is utilised to oversee both lawful and potentially illicit transactions. The AI examines clients and transactions to identify potentially suspicious behaviour. The examination is characterised by automation, which incorporates specific approaches based on predetermined rules. Subsequently, a human operator thoroughly examines the concerns and takes the necessary measures, which may involve manual intervention such as approving, denying, or obstructing the transaction. The manual process of analysing transactions can be a significant challenge for human operators, particularly in cases where a system generates a high number of false positives.

AI-Based Customer Due Diligence

As required by Indonesian AML Law, bank employees are responsible for verifying the authenticity and credibility of the documents submitted by clients during the registration process. To gain comprehensive knowledge about the individuals they engage with, banks employ CDD procedures. CDD procedures help to identify and assess any potential risks associated with the clients. KYC procedures to verify the authenticity of the client's claims, official documents like ID cards, birth certificates, driving licences, passports, proof of address, or other relevant credentials are required by banks.[20]

CDD also assists banks in understanding the business nature of their clients and the source of their income or assets. This feature enables easy monitoring and detection of potentially hazardous behaviours, such as alterations in transaction networks, frequency, and quantities. According to the guidelines set forth by the FATF, it is advised that banks carry out CDD procedures when clients establish new business relationships or partake in transactions above a predetermined threshold.[21] Renewing CDD when there is a change in operations enables banks to update and maintain accurate profiles of their clients, facilitating continuous monitoring of potentially problematic behaviours or activities.

The FATF has outlined key characteristics to monitor in each transaction, including client movements and destinations, the types of currency exchanges involved, as well as the transaction limits, frequency, amounts and values.[22] Currently, many banks rely on manual, non-standardised processes for scoring customer risk, a method that is time-consuming and highly subjective. Compliance officers collect information on factors like industry, jurisdiction, and products, often leading to assessments influenced by individual judgment rather than standardised criteria. This approach burdens both the compliance officers and the customers, as officers are often tasked with extensive inquiries into documents like bank statements and tax filings without a clear framework. This subjective method results in inconsistent risk grading, as ratings can vary widely between compliance officers, making the process unreliable and inefficient.

Machine learning models offer an alternative, data-driven approach to CDD, enhancing the predictive power of risk assessments. Unlike officer scorecards, these models rely on historical data and behavioural patterns, yielding more accurate insights into potential financial crimes.[23] Machine learning models undergo development and testing to refine their predictive accuracy, which allows financial institutions to identify high-risk customers more effectively. By using machine learning, banks can potentially automate parts of the onboarding CDD, making it more efficient and reducing the workload on compliance staff.

[20] AML Law Number 8 Tahun 2010, Art. 19.

[21] FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," FATF-GAFI, last modified 2023, https://www.fatf-gafi.org/content/dam/fatf-gafi/Recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

[22] FATF.

[23] Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."

Ongoing due diligence is also essential, as banks gather more behavioural data post-onboarding. Information such as transaction volume, payment methods, and business counterparts adds valuable insights to update the customer's risk rating dynamically. Statistical models can convert this transaction data into updated risk scores, predicting the likelihood of financial crime. This ongoing monitoring can also segment customers into risk categories based on behavioural patterns, allowing more targeted monitoring of high-risk segments. These models help identify potential money laundering, tax evasion, or terrorism financing, enhancing the institution's ability to respond proactively to emerging threats.

Integrating machine learning outcomes into smart AI-based systems can further optimise the CDD process. The AI program generates periodic reports that include risk ratings, transaction locations, transaction directions (inward or outward), and the percentage of transactions categorised by type.[24] By automating decision-making, these AI systems can improve accuracy, speed, and cost-efficiency in customer risk assessment. Digital transformation and AI save resources and reduce compliance costs, making CDD a scalable and sustainable process. As business and regulatory pressures increase, the transition to automated and AI-powered compliance solutions is inevitable, positioning financial institutions for more effective and efficient compliance in the future.

AI-Based Know Your Customer

In the context of AML compliance, KYC and CDD are complementary but distinct regulatory processes that financial institutions are legally required to implement. KYC involves the initial identification and verification of a customer's identity at the point of onboarding, using official documents such as ID cards, passports, or proof of address. Its primary aim is to prevent anonymous or fraudulent access to the financial system, ensuring that only traceable, legitimate entities can transact. In Indonesia, KYC procedures are mandated by Law No. 8 of 2010 and are increasingly facilitated by electronic systems (e-KYC) that integrate with government databases to streamline identity verification. In contrast, CDD goes beyond identity checks to assess a customer's risk profile through an ongoing evaluation of their financial activity, business relationships, and potential links to high-risk entities or jurisdictions. It enables banks to monitor behaviour over time and apply enhanced due diligence to higher-risk clients. The distinction between KYC and CDD is essential to understanding how AI reshapes compliance while raising new concerns about human rights violations.

Law No. 8 of 2010 on Countermeasure and Eradication of Money Laundering and a series of national regulations require banks to do several things, such as KYC procedures, identifying politically exposed persons, identifying transactions in high-risk countries, and reporting suspicious or unusual transactions.[25] Banks are obligated to proactively identify potentially suspicious transactions and promptly notify the PPATK, which serves as the designated financial intelligence unit (FIU).[26] It is important to note that such reporting obligations do not necessitate the disclosure of these activities to the customers involved. Compliance laws, such as anti-corruption laws, require the implementation of mechanisms like whistleblowing to identify and disclose illicit conduct occurring within corporate entities. In contrast, AML laws mandate banks to assume the role of government informants, potentially conflicting with their customary obligation of maintaining customer confidentiality.

However, financial entities such as banks, payment processors, credit institutions, and insurance companies have these obligations for critical reasons. First, the sophistication of money laundering techniques demands vigilant oversight and only financial institutions have

[24] Jullum et al.

[25] AML Law Number 8 Tahun 2010, Art. 23.

[26] AML Law Number 8 Tahun 2010, Art. 23.

the depth of information needed to detect suspicious transactions within customer relationships.[27] Second, banks face substantial financial incentives to overlook illicit funds. Without legal requirements to identify and report suspicious activity, the potential economic gains could drive banks to accept deposits of unlawful money, except in the most blatantly criminal cases.[28]

Financial institutions primarily gather data from prospective clients to enhance the provision of their services. Banks utilise client data to assess the risks associated with loans, detect instances of money laundering, and identify potential fraudulent actions. Banks are obligated to collaborate with authorities in instances involving money laundering to furnish pertinent information that may serve as evidentiary material in legal processes. Customer-centric data acquisition is of significant importance within the banking industry, particularly in light of the expanding realm of online banking and the prevalence of fraudulent actions.

AI technology is utilised within banking institutions to facilitate customer identification, verification, and authorisation processes. The KYC method operates similarly to CDD, enabling banks to understand their clientele more deeply. Financial institutions are required to gather information from both domestic and international customers, as well as non-profit entities, businesses, and governmental bodies. This data is essential for conducting financial audits. However, the sheer magnitude of daily transactions poses a challenge for banks in effectively monitoring this extensive dataset and accurately detecting all potentially fraudulent activities or questionable transfers.

The introduction of electronic Know Your Customer (e-KYC) technology has greatly aided compliance professionals by allowing financial institutions to access customer information directly from government portals.[29] With customer consent, financial institutions can retrieve and autofill necessary details from reliable databases, reducing the need for extensive documentation. This shift to digital information gathering streamlines the onboarding process, minimises errors, and enhances compliance, making it a more efficient alternative to conventional KYC methods.

In addition to e-KYC, automated alert systems notify bank personnel and customers when documents, such as IDs, are nearing expiration and need renewal. This system of automated alerts helps financial institutions maintain up-to-date records while improving compliance with regulatory requirements.[30] By proactively reminding customers about renewals, financial institutions can reduce cases of outdated documentation and minimise potential compliance breaches.

Automation in information extraction further enhances the KYC process, allowing banks to efficiently scan, organise, and extract relevant information from emails and documents. This technology can save significant time and resources, as it reduces manual processing demands. However, the effectiveness of automated extraction relies on the accuracy of the algorithms used.[31] Poorly designed algorithms may lead to errors, requiring additional human intervention, so maintaining algorithmic precision is essential for optimal efficiency.

AI systems possess the capability to browse through vast quantities of data points, scrutinise transactions that appear suspicious, and identify any discernible trends or patterns that may suggest the presence of harmful activities.[32] AI, particularly computer vision, enables

[27] Peter Yeoh, "Banks' Vulnerabilities to Money Laundering Activities," *Journal of Money Laundering Control* 23, no. 1 (2019): 122–35, https://doi.org/10.1108/jmlc-05-2019-0040.
[28] Yeoh.
[29] Yeoh.
[30] Md. Abdul Hannan et al., "A Systematic Literature Review of Blockchain-Based e-KYC Systems," *Computing* 105, no. 10 (2023): 2089–2118, https://doi.org/10.1007/s00607-023-01176-8.
[31] Hannan et al.
[32] Hannan et al.

banks to verify the consistency of uploaded documents by cross-checking customer-provided information against official records.[33] Computer vision can detect discrepancies, such as mismatches in ID numbers, and raise alerts for further investigation.[34] This AI-based approach supports quality assurance across all transactions, increasing accuracy and trust in the system. Overall, the integration of e-KYC, automated alerts, and AI enhances compliance processes, reduces costs, and improves the customer experience.

AI-Based Beneficial Owner Detection

Money laundering activities involve cross-border financial transactions, which make it difficult to trace the source of funds. The process consists of a series of transactions to conceal illicit funds from authorities, making it challenging to identify the actual beneficial owner. The complexity of the process is compounded by the use of multiple levels of data documentation, which makes it challenging to retrieve records, especially across different jurisdictions and regulatory frameworks. Moreover, corporations and foundations can appoint shareholders and board members without revealing the identities of the true beneficial owners, making it even more challenging to identify the rightful owners of illicitly acquired funds.

The lack of transparency provided by corporations and trusts enables the concealment of the identities of those involved in financial crimes, making it difficult to prosecute the offenders. Implementation of regulations to combat money laundering has been undertaken by many countries by requiring trusts and companies to digitize their registers and make information about beneficial owners publicly accessible.[35] However, a significant portion of the data is unstructured or in handwritten notes, making it challenging to comprehend the information and identify the beneficial owner.[36]

AI can help create digitised and organised data records that are easily searchable, assuming that such information is included in shareholder filings.[37] The AI procedure can help to enhance transparency regarding beneficial ownership and ensure compliance with the regulations, reducing the liability of the organisation and its executives. The registration of beneficial owners is mandatory, and their information must be made publicly accessible through appropriate technological means.

AI-Based Transactions Monitoring

Traditional transaction monitoring relies on rule-based systems that generate alerts based on predefined scenarios. However, this approach has limitations, especially at the scale of trillions of global transactions. Rule-based methods often yield a high rate of false positives, leading to resource-intensive investigations. As a result, banks are increasingly adopting advanced alert optimisation methods and exploring AI-based monitoring to manage alerts more efficiently.

A key aspect of transaction monitoring is real-time counterparty screening, particularly to prevent funds from reaching sanctioned entities. In real-time payments, banks must verify the recipient's information before transaction approval to ensure compliance.[38] This type of screening, especially sanctions screening, is critical in instant settlements where any delay in

[33] Hannan et al.

[34] Hannan et al.

[35] S. Alexandra Bieler, "Peeking into the House of Cards: Money Laundering, Luxury Real Estate, and the Necessity of Data Verification for the Corporate Transparency Act's Beneficial Ownership Registry," *Fordham Journal of Corporate and Financial Law* 27 (2022): 193.

[36] Bieler.

[37] Bieler.

[38] Bieler.

detection could allow illegal funds to transfer, causing potential harm and regulatory violations.[39]

In addition to real-time monitoring, scheduled transaction reviews identify potential money laundering by regularly assessing transaction patterns. Banks set specific thresholds for transactions, such as high-value cash withdrawals within a set timeframe.[40] If a transaction exceeds these parameters, it triggers alerts for further scrutiny. Scheduled monitoring helps detect longer-term patterns in suspicious transactions that real-time monitoring may miss.[41]

Machine learning offers a promising solution to address challenges in monitoring transactions. Machine learning algorithms can analyse transaction patterns, adjust to emerging trends in financial crimes, and refine alert thresholds to improve accuracy.[42] For banks with limited access to machine learning, threshold finetuning, which is adjusting the values that trigger alerts, can provide an alternative means of refining transaction monitoring systems and reducing false positives.[43]

Furthermore, productivity rate metrics aid in evaluating monitoring systems. The metrics focus on alert effectiveness across multiple levels, from transactions to specific customer behaviours. Additionally, metrics like SAR coverage, which tracks the proportion of SARs captured within a scenario, and overlap ratio, which monitors multi-scenario alerts for the same customer, help streamline investigations and focus resources on high-risk cases.[44]

Segmenting customers by behaviour and risk profile is a foundational step in threshold finetuning. Traditionally, static segmentation groups customers by background factors, such as company type or exposure levels.[45] However, dynamic segmentation using machine learning-based unsupervised learning allows for more responsive grouping, aligning thresholds with each segment's distinct transaction patterns.[46] Dynamic segmentation using machine learning helps reduce false positives and enhances the accuracy of detecting suspicious activities.[47]

Threshold finetuning follows a structured approach, starting with analysing scenario parameters to ensure thresholds align with business and regulatory objectives.[48] This is followed by replicating scenario logic in test environments to establish baseline productivity and SAR coverage.[49] Resolving discrepancies collaboratively with compliance teams ensures that threshold adjustments are optimised and understood before implementation.

Above-the-line (ATL) and below-the-line (BTL) testing allow banks to assess alert sensitivity by modifying thresholds.[50] Lower thresholds increase alerts and SAR coverage, while higher thresholds reduce both.[51] Through iterative testing, banks seek to maximise detection without overburdening the system with false positives.[52] This iterative optimization

[39] Bieler.
[40] Bieler.
[41] Bieler.
[42] Jullum et al., "Detecting Money Laundering Transactions with Machine Learning."
[43] Jullum et al.
[44] Jullum et al.
[45] Guneet Kaur, "Trust the Machine and Embrace Artificial Intelligence (AI) to Combat Money Laundering Activities," in *Disruptive Technologies and Digital Transformations for Society 5.0*, ed. Sandeep Kautish et al. (Singapore: Springer Nature Singapore, 2024), 63–81, https://doi.org/10.1007/978-981-99-5354-7_4.
[46] Kaur.
[47] Kaur.
[48] Abhishek Gupta, Dwijendra Nath Dwivedi, and Ashish Jain, "Threshold Fine-Tuning of Money Laundering Scenarios through Multi-Dimensional Optimization Techniques," *Journal of Money Laundering Control* 25, no. 1 (2022): 72–78, https://doi.org/10.1108/jmlc-12-2020-0138.
[49] Gupta, Dwivedi, and Jain.
[50] Gupta, Dwivedi, and Jain.
[51] Gupta, Dwivedi, and Jain.
[52] Gupta, Dwivedi, and Jain.

is critical in high-frequency transaction scenarios, such as ATM withdrawals, where detection sensitivity must be balanced against operational efficiency.

Cross-scenario optimization further enhances monitoring by addressing the overlap ratio. This case is where customers trigger multiple alerts across different types of transactions.[53] Reducing overlap through programming methods helps banks streamline investigations and focus resources more effectively.[54]

Lastly, accurately tagging suspicious behaviours is critical for refining threshold finetuning. By documenting the specific behaviours that trigger alerts, banks enhance their monitoring systems and strengthen their ability to respond to evolving financial crime trends. This proactive, data-driven approach ultimately safeguards banks from regulatory risks and enhances compliance while focusing resources on genuine threats to financial integrity.

Ethical Challenges

While AI has been positively accepted for its role in combating financial fraud, significant limitations affect its reliability. Malicious individuals can exploit AI technologies to compromise the security and integrity of financial systems, creating serious threats to both digital and physical safety. AI can potentially pose a significant danger to digital security through various means, including leveraging machine learning algorithms and data analytics to exploit vulnerable individuals.[55] AI can acquire and analyse certain behavioural patterns exhibited by individuals who utilise banking services. By illicitly obtaining their login information, AI can create detailed profiles of these individuals, which are subsequently exploited to engage in money laundering activities.[56] Spear phishing assaults are employed to acquire crucial personal information or engage in fraudulent activities, such as monetary theft, by masquerading as reputable government or financial entities to deceive unsuspecting individuals.[57]

Ethical AI practices have been evolving for years, particularly in industries such as financial services.[58] These practices emphasise transparency, with clear guidelines on what factors should or should not be used in making decisions.[59] Instances like Amazon's biased AI tool and culturally specific advertisements on social media highlight the potential for AI to get it wrong and perpetuate biases in ways that are unintended or harmful.[60]

In the realm of AML compliance, AI applications often rely on profiling, where certain demographics are classified as high-risk.[61] Historically, such profiling has been based on demographic factors, raising concerns about its ethical implications. The key issue is whether such profiling constitutes bias against particular groups. While profiling can be useful in detecting potential risks, there is a fine line between risk management and discriminatory practices that unfairly target certain communities and reinforce harmful stereotypes.[62]

[53] Gupta, Dwivedi, and Jain.
[54] Gupta, Dwivedi, and Jain.
[55] Abhishek Gupta, Dwijendra Nath Dwivedi, and Jigar Shah, *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance*, Future of Business and Finance (Singapore: Springer Nature Singapore, 2023), https://doi.org/10.1007/978-981-99-2571-1.
[56] Gupta, Dwivedi, and Shah.
[57] Gupta, Dwivedi, and Shah.
[58] Faraz Ahmed, "Ethical Aspects of Artificial Intelligence in Banking," *Journal of Research in Economics and Finance Management* 1, no. 2 (2022): 55–63, https://doi.org/10.56596/jrefm.v1i2.7.
[59] Ahmed.
[60] Ahmed.
[61] Sheshadri Chatterjee and N. S. Sreenivasulu, "Artificial Intelligence and Human Rights: A Comprehensive Study from Indian Legal and Policy Perspective," *International Journal of Law and Management* 64, no. 1 (2022): 110–34, https://doi.org/10.1108/ijlma-02-2021-0049.
[62] Chatterjee and Sreenivasulu.

Privacy concerns are another critical challenge. AI systems often process vast amounts of unstructured data, such as transaction history or network interactions, which can infringe on individuals' privacy.[63] In Indonesia, privacy regulations are still evolving, leaving room for uncertainty about how personal data should be handled. While there have been no major incidents reported, the risk of AI being misused to discriminate against customers remains a genuine concern.

AI systems are also prone to various types of biases, which can be introduced through human decisions, data selection, and model design.[64] Human biases often influence the development of AI systems, whether consciously or subconsciously. These biases can be based on past experiences or preconceived notions about certain demographic groups.[65] For instance, decision-makers may associate specific professions with particular behaviours, which can influence the data selected for training AI models.[66] Data-driven biases are another common source of AI errors.[67] Poorly classified or misrepresented data can lead to skewed outcomes.[68] In areas like KYC processes, biases can disproportionately affect certain groups, leading to unfair treatment. For instance, an AI system might flag a particular group as high-risk based on historical patterns, but these patterns may not reflect current realities.

As AI becomes more sophisticated, it is essential to ensure that ethical standards evolve alongside these advancements to protect customer trust and ensure the stability of financial markets. While AI algorithms can outperform humans in processing data, they often perpetuate human biases unless preventive measures are implemented.[69] The use of Big Data in AI analysis can infringe on privacy, which is threatening human rights.

Indeed, AI has introduced significant risks to human rights, exacerbating existing issues and creating new challenges in areas like algorithmic decision-making.[70] While traditional statistical models are straightforward and less likely to impact human rights, AI's complex decision-making processes can unintentionally violate human rights by perpetuating biases, such as in criminal justice, employment, and surveillance.[71] AI systems can also lead to discrimination, misinformation, and unequal treatment, disproportionately affecting vulnerable groups.[72] These risks raise concerns about power imbalances and how AI can reinforce oppression, making it crucial to address these issues through effective human rights protections.

Human rights laws play a critical role in mitigating the harm caused by AI, but determining the "good" and "bad" impacts of AI is complex and requires ethical considerations. Ethical principles such as fairness, justice, accountability, and transparency guide AI development and use, helping define boundaries between acceptable and harmful practices. Major tech companies like Microsoft, IBM, and Google have developed their own AI ethics guidelines, though these principles are not always clearly defined.[73] Nevertheless, human rights principles

[63] Sinta Dewi and Mohammad Wildan Hidayat, "Protection of Data Privacy in the Era of Artificial Intelligence in the Financial Sector in Indonesia," *Journal of Central Banking Law and Institutions* 1, no. 2 (2022): 353–66, https://doi.org/10.21098/jcli.v1i2.18.

[64] Chatterjee and Sreenivasulu, "Artificial Intelligence and Human Rights."

[65] Chatterjee and Sreenivasulu.

[66] Chatterjee and Sreenivasulu.

[67] Chatterjee and Sreenivasulu, "Artificial Intelligence and Human Rights."

[68] Chatterjee and Sreenivasulu.

[69] Chatterjee and Sreenivasulu.

[70] Chatterjee and Sreenivasulu.

[71] Chatterjee and Sreenivasulu.

[72] Chatterjee and Sreenivasulu.

[73] Morgan Sullivan, "Big Tech's Evolving Role in AI Governance: Shaping Ethical Standards," *Transcend*, March 21, 2024, https://transcend.io/blog/big-tech-ai-governance.

are universally recognised and provide a foundation for holding AI systems accountable. When AI is perceived as unethical, it not only violates individual rights but also undermines the core principles of human rights law.

Global Frameworks

International norms and directives that govern specific areas also possess a degree of universality. Take, for example, the Japanese Society for Artificial Intelligence's Ethical Guidelines, which recommend government-led algorithm audits.[74] This idea soon gained traction and was adopted by the U.S. Senate Intelligence Committee as a means of promoting fair and unbiased decision-making.[75]

Similarly, the European Union's GDPR was designed to protect data privacy for individuals within the EU, extending its influence to any organisation handling data on EU citizens.[76] Organisations like the Organisation for Economic Co-operation and Development (OECD) and the European Union's Artificial Intelligence High-Level Expert Group (AI HLEG) work closely with regional bodies to develop principles that champion trustworthy, ethical AI systems.[77] Both have put forth guidelines that highlight essential values such as transparency, accountability, privacy, and the broader social impacts of AI.[78] The OECD guidelines, in particular, underscore the need for AI to support inclusive growth, sustainability, and well-being.[79] However, these principles are generally high-level and do not provide specific technical guidance, leaving room for interpretation and evolution as AI advances.

One key OECD principle calls for transparency around AI systems, emphasising the importance of enabling users to challenge AI-based decisions.[80] In sectors like AML, transparency does not necessarily mean notifying flagged individuals. Instead, it means that AI models must be understandable and explainable to oversight bodies, allowing for proper scrutiny of the algorithms used. This requirement is also tied to the need for reproducible and reliable results, which ensures that similar inputs lead to consistent outputs, reinforcing the reliability of AI systems in these high-stakes applications.

Security and ongoing risk evaluation are other focal points, emphasised in OECD Principle 4.[81] AI systems are expected to operate safely, even in challenging or unforeseen conditions. This principle aligns with the EU's risk-based approach to AI regulation, currently laid out in the proposed AI Act.[82] This legislation, unveiled in April 2022, aims to establish enforceable AI standards across the EU, addressing areas such as transparency, human oversight, data protection, and cybersecurity. The act includes a tiered risk framework, where high-risk applications like medical devices and AI used in hiring processes undergo rigorous evaluation, while low-risk applications like chatbots require users to be informed that they are interacting

[74] Japanese Society for Artificial Intelligence, "The Japanese Society for Artificial Intelligence Ethical Guidelines," Japanese Society for Artificial Intelligence, last modified 2017, https://www.ai-gakkai.or.jp/ai-elsi/wp-content/uploads/sites/19/2017/05/JSAI-Ethical-Guidelines-1.pdf.

[75] The Senate of The United States, "Bill to Provide a Framework for Artificial Intelligence Innovation and Accountability, and for Other Purposes," congress.gov, last modified November 15, 2023, https://www.congress.gov/118/bills/s3312/BILLS-118s3312is.pdf.

[76] The European Parliament and The Council, *2016/679 General Data Protection Regulation* (The European Parliament and The Council, 2016).

[77] Alexandru Circiumaru, "Towards European AI: Part I - Setting the Context," Queen Mary University of London, last modified October 18, 2019, https://www.qmul.ac.uk/euplant/blog/items/towards-european-ai-part-i---setting-the-context-.html.

[78] Circiumaru.

[79] OECD, "AI Principles," OECD, last modified 2024, https://www.oecd.org/en/topics/sub-issues/ai-principles.html.

[80] OECD.

[81] OECD.

[82] Circiumaru, "Towards European AI."

with AI.[83] This approach seeks to balance regulatory oversight with the flexibility needed to foster innovation in AI, minimising regulatory burdens for lower-risk technologies.

The EU AI Act, however, represents a landmark move as it introduces enforceable regulations that apply directly to AI applications within the digital single market.[84] While many of the EU's member states also support FATF and OECD guidelines, the AI Act goes further, establishing mandatory rules for all AI technologies, especially those in high-risk sectors such as AML. In these areas, AI tools have a substantial role in analysing extensive data sets to detect criminal activities.[85] With AI's involvement, AML efforts gain an analytical edge, allowing teams to focus on high-risk cases while AI handles the preliminary work of data aggregation.

The EU AI Act mandates continuous human oversight for high-risk AI applications in AML, ensuring that operators can pause or review automated decisions at any time.[86] Continuous human oversight for high-risk AI applications in AML supports the principle of model explainability, which allows users to understand how and why AI systems produce specific outcomes, which is an essential feature for detecting potential biases or errors. To comply, regulated entities must implement strong data security protocols, maintain detailed audit trails, and establish governance frameworks that may include new roles such as AI compliance officers. Although this transition presents practical challenges, it is widely viewed as a necessary step toward building public trust and ensuring that AI is applied ethically and responsibly in critical domains such as financial crime prevention.

The EU AI Act is a substantial step toward harmonising AI regulation, setting a global benchmark that may influence AI standards worldwide.[87] As its implementation unfolds, the focus will remain on fostering a balance between innovation and oversight, ensuring AI serves humanity in ways that are transparent, fair, and responsible.

Law necessitates a harmonious equilibrium between safeguarding human rights and proportionally imposing restrictions. Therefore, the limitation clause should be employed as a criterion for addressing the challenges of AI-based AML procedures. The proportionality test is a commonly employed method in democratic societies to restrict rights.[88]

The proportionality test has emerged as a widely employed constitutional law principle within democratic societies, serving to strike a balance between individual rights and the lawful restrictions imposed upon them. Generic constitutional law refers to the basic principles, theories, practices, and doctrines of constitutional law that apply broadly, without being tied to any specific jurisdiction.[89] It suggests that when an approach, practice, or principle has been consistently employed throughout multiple jurisdictions, it attains the status of generic constitutional law. The examination has been implemented in numerous jurisdictions adhering to civil and common law systems.[90]

Moreover, it has also been implemented by regional human rights courts, including the European Court of Human Rights, the Inter-American Court of Human Rights, and the European Court of Justice.[91] The underlying principle of the proportionality test is to achieve a

[83] Circiumaru.
[84] Circiumaru.
[85] Circiumaru.
[86] Circiumaru.
[87] Circiumaru.
[88] Circiumaru.
[89] Circiumaru.
[90] Circiumaru.
[91] Emil Śliwiński, "Principle of Proportionality as a Threat to Criminal-Law-Related Fundamental Rights," *New Journal of European Criminal Law* 14, no. 3 (2023): 327–44, https://doi.org/10.1177/20322844231158323.

harmonious equilibrium between the methods employed and the outcome.[92] When considering the balance between forms and the final result, the means employed must be beneficial, essential, suitable, and above all, proportionate. In his work, Bernhard Schlink provides an illustrative anecdote with a disabled individual who endeavours to protect his property, specifically a collection of apples, from a toddler who pilfers one from a tree.[93] The child demonstrates a lack of compliance with the spoken instruction to refrain from taking his apple. The sole method available to him involves utilising a firearm within his immediate vicinity to discharge a projectile to cause harm to the youngster. In this instance, Schlink expounds on the efficacy and necessity of employing lethal force to safeguard the man's apples, which are considered his property.[94]

Nevertheless, shooting a child to obtain apples is widely regarded as wrong or morally unbalanced due to the inherent disparity between the value of a child's life and the relatively trivial worth of a few apples. Schlink offered a specific example from a case before the German Federal Constitutional Court.[95] The Court raised inquiries regarding the permissibility of the state's extraction of a defendant's cerebrospinal fluid to assess their cognitive abilities.[96] The court rendered a decision affirming the legitimacy of the objective of ascertaining mental ability. However, the court recognised the distress and risk involved in the extraction process. As a result, it ruled that such extraction is justified only in cases of substantial severity.

The potential restriction of human rights is explicitly outlined in Article 29 of the Universal Declaration of Human Rights (UDHR), which asserts:

> "The exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order, and the general welfare in a democratic society."[97]

Compatibility with Human Rights Law in Indonesia

In Indonesia, there is still no regulation on the utilisation of AI. The Indonesian legal system suggests regulating prospective AI regulation and human rights compatibility by determining the principle of responsible AI. These legal principles shall be the guidelines to prevent the harms and the risks of AI technology and to strengthen the effort of mitigating money laundering.

Undoubtedly, human rights, as well as other legal rights, are subject to limitations.[98] So, there is a necessity to investigate the potential of utilising the 1945 Constitution and Indonesian AML Law to address the dilemma. Article 28 J of the 1945 Constitution. A comparable tone to Article 29 of the UDHR exhibits the limitation provision in the 1945 Constitution. The restriction provision outlined in Article 28J of the 1945 Constitution specifies:

> "In exercising rights and freedoms, every person shall be subject to limitations as are determined by law solely for securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, religious values, security, public order, in a democratic society."[99]

[92] Śliwiński.

[93] Bernhard Schlink, "Proportionality in Constitutional Law: Why Everywhere but Here?," *Duke Journal of Comparative & International Law* 22 (2012): 291.

[94] Schlink.

[95] Schlink.

[96] Schlink.

[97] United Nations, "Universal Declaration of Human Rights," United Nations, last modified 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[98] Schlink, "Proportionality in Constitutional Law."

[99] Constitutional Court of the Republic of Indonesia, "The 1945 Constitution of the Republic of Indonesia," MKRI, last modified 2020, https://en.mkri.id/library/constitution.

The idea of the necessity of certain restrictions on human rights is supported by the Constitutional Court of Indonesia (MK). In court decision number 14/PUU-VI/2008, the Court recognises that, at times, it is unavoidable to limit rights, even when the 1945 Constitution does not include explicit limitation clauses.[100]

In this regard, the proportionality test ensures that government powers granted by a specific law do not excessively infringe on fundamental rights, such as the right to privacy, non-discrimination, a fair trial, or freedom of expression. The application of the proportionality test is observed in two distinct contexts within the legal framework of Indonesia. Firstly, it is employed as a proportionality requirement stipulated in the constitution.[101] Secondly, it is utilised as a statutory proportionality requirement found in national laws.[102]

Regardless of whether individual laws explicitly mention proportionality, the notion of proportionality is inherently embedded within statutory frameworks.[103] A statute that fails to adhere to the principle of proportionality at the constitutional level shall be deemed null and void.[104] One of the most relevant provisions for AML is Article 26 of Law No. 19/2016 on Electronic Information and Transactions, which protects privacy rights.

The proportionality test comprises three sequential steps that must be collectively fulfilled. The initial stage involves inquiring whether the policy has been stipulated in a law or regulation that is specific, comprehensible, and has been enacted by democratic procedures.[105] The second step involves evaluating whether the policy in question is aligned with a valid purpose, such as protecting fundamental rights or addressing a significant societal concern.[106] The third phase inquires about the necessity of the measure within the context of a democratic society.[107] The third phase in this process presents the most significant level of difficulty and encompasses multiple subtests. These subtests assess the measure's effectiveness, its level of intrusiveness compared to other existing standards, a fair balance between the rights involved, and sufficient protections.

The first stage of the proportionality test, as required by law, demands that any rights-limiting measure be clearly defined in legislation. This legislation must specify the features of the technology used, the type of data it processes, and the safeguards in place. Such clarity allows citizens and political stakeholders to understand the measure, assess its implications, and hold the government accountable for its implementation.[108] There is significant flexibility in interpreting AML regulations regarding transaction monitoring. The primary stipulations entail the necessity for systems to exhibit complete efficacy in obstructing payments directed towards entities subject to international sanctions.[109] Additionally, the systems must be designed to identify suspicious transactions by considering meticulously defined risk scenarios.

In practical terms, regulatory bodies anticipate that banks will adhere to industry standards when implementing systems. These standards are subject to continuous evolution as vendors of AML technologies introduce increasingly advanced and invasive procedures. It is worth noting

[100] Constitutional Court of the Republic of Indonesia, "Decision Number 14/PUU-VI/2008," MKRI, 2020, https://en.mkri.id/court/decision?search=14%2FPUU-VI%2F2008.

[101] Jan Sieckmann, "Proportionality as a Universal Human Rights Principle," in *Proportionality in Law*, ed. David Duarte and Jorge Silva Sampaio (Cham: Springer International Publishing, 2018), 3–24, https://doi.org/10.1007/978-3-319-89647-2_1.

[102] Sieckmann.

[103] Sieckmann.

[104] Sieckmann.

[105] Sieckmann.

[106] Sieckmann.

[107] Sieckmann.

[108] Sieckmann.

[109] Sieckmann.

that legal frameworks do not establish explicit upper limits in this regard. The current upward trajectory is driven by the perception of banks that increasing investments in technology and compliance personnel will mitigate the likelihood of regulatory penalties. Banks tend to consider AML sanctions, which encompass measures such as the cancellation of a banking licence, as more consequential risks than data protection risks. This notion can cause banks to make mistakes in using more advanced compliance systems.

The second element of proportionality, which involves pursuing a valid objective and addressing a pressing social need, can be easily fulfilled in the case of AML strategies. AML strategies are inherently linked to broader efforts to combat severe criminal activities and terrorism. Article 26 of Law No. 19 of 2016 explicitly states that the legitimate grounds for encroaching upon privacy rights include cases related to AML, provided that such interference is proportionate.

The Siracusa Principle draws attention to the pervasive issue of governmental abuse in employing human rights restriction clauses to curtail fundamental human rights unilaterally.[110] There are nine key principles to guide how states can lawfully impose restrictions on human rights using limitation clauses.[111] In principle, it underscores the essential elements involved in restricting rights. The term "necessary" suggests that the limitation and other requirements must be commensurate with the objective of the constraint.[112]

Another important document, General Comment No. 31 (2004) from the Human Rights Commission, explains that states must justify any restrictions on rights under the International Covenant on Civil and Political Rights (ICCPR).[113] It states that these restrictions must be necessary and proportionate to the legitimate objectives they aim to achieve, ensuring that the rights protected by the Covenant remain effectively safeguarded.[114]

An essential component of the third proportionality stage entails evaluating the extent to which a particular technique is truly efficacious in attaining the intended goal while also being the least invasive way available.[115] However, what methodologies can be employed to assess the efficacy of AML strategies? As previously said, banks set their success solely by relying on historical reports. In the context of banking, the efficacy of warnings is heightened when they have a resemblance to scenarios that bank compliance teams have previously identified as problematic. However, financial institutions lack knowledge regarding the efficacy of their suspicious activity reports in facilitating law enforcement efforts. The confirmation or denial of any potential connection between the suspicious activity observed by the bank and criminal conduct is currently being withheld by law enforcement authorities.

One essential aspect is transparency, wherein persons must be notified of their identification as potential threats to engage in illegal behaviour.[116] Nevertheless, the legislation about AML restricts such actions due to the potential compromising of criminal investigations that may arise from tipping off an individual. The issue of effectively communicating surveillance activities to the subjects under monitoring poses a significant challenge for various surveillance systems, particularly those employed in national security and anti-terrorism operations, when maintaining confidentiality is of utmost importance. The prevailing stance

[110] Sieckmann.

[111] Alex Conte, "Limiting Rights Under International Law," in *Human Rights in the Prevention and Punishment of Terrorism*, ed. Alex Conte (Berlin, Heidelberg: Springer Berlin Heidelberg, 2010), 283–314, https://doi.org/10.1007/978-3-642-11608-7_10.

[112] Conte.

[113] UN Human Rights Committee, "General Comment No. 31 [80], the Nature of the General Legal Obligation Imposed on States Parties to the Covenant," Refworld, last modified May 26, 2004, https://www.refworld.org/legal/general/hrc/2004/en/52451.

[114] UN Human Rights Committee.

[115] Schlink, "Proportionality in Constitutional Law."

[116] Schlink.

adopted by courts is that persons should be promptly notified while ensuring that such notification does not jeopardise the ongoing inquiry. This proposal posits that there is a need to amend the AML legislation to grant banks the ability to inform customers who have been the subject of a SAR at a certain point in time after the transmission of the SAR to the FIU unless the FIU explicitly determines that such notification would impede an ongoing investigation. Law enforcement authorities bear the burden of proving that informing a specific customer would compromise an ongoing investigation. Keeping such information permanently hidden, especially when SARs are never acted upon, appears unjust.

The proportionality test stipulates that any infringement upon private rights or other limitations on rights must adhere to the principle of proportionality.[117] Therefore, it is imperative to establish regulations within the framework of governmental interventions. When faced with a query concerning transaction monitoring, the initial step would involve assessing the extent to which human rights are impacted. The AML detection methods are inherently intrusive as they encompass the comprehensive analysis of transaction data from all clients, regardless of the presence of machine learning techniques.

Policy Recommendation

The regulation of systemic risks associated with AI-based AML strategies highlights critical areas needing attention to ensure human rights protection, particularly in governance, accountability, and ethics.[118] Current regulatory efforts focus on ensuring that both financial institutions and AI developers maintain robust internal controls to monitor and manage risks throughout the AI development lifecycle.[119] Key to these controls is the principle of shared accountability, where both developers and users bear responsibility for any systemic risks posed by AI technologies.[120] This accountability should be upheld at the highest levels for AI applications with significant financial implications, ensuring that human oversight remains intact. Transparency in the decision-making processes of AI systems is paramount so that these systems can be explained and controlled by human operators when necessary.

Although these regulatory efforts represent a solid foundation for managing AI risks in the banking industry, they rely heavily on the preparedness and accountability of AI developers and banks. For regulation to be effective, banks must have the capability to monitor and explain AI behaviour reliably. Achieving this requires regulators to engage skilled personnel and develop or acquire AI-linked technologies that allow them to verify AI systems' functionalities independently. The complexity of AI, combined with the need for specialised skills, makes full regulatory engagement challenging, especially in cases of AI systems with potential systemic importance. Consequently, regulators may find it more feasible to focus their efforts on high-risk cases, where the potential impacts on financial stability are greatest.

Flexibility and adaptability are central to AI regulation, especially given the rapid pace of AI advancements and the informational gaps that often exist between regulators and the market.[121] The proportionality test acknowledges the need for legal frameworks that can evolve alongside technological developments. This flexibility, however, must not lead to a regulatory vacuum, where AI systems operate with insufficient oversight. A risk-based regulatory approach offers a balanced solution by establishing broad guidelines that prioritise data privacy,

[117] Conte, "Limiting Rights Under International Law."

[118] Ondrej Bajgar and Jan Horenovsky, "Negative Human Rights as a Basis for Long-Term AI Safety and Regulation," *Journal of Artificial Intelligence Research* 76 (2023): 1043–75, https://doi.org/10.1613/jair.1.14020.

[119] Bajgar and Horenovsky.

[120] Bajgar and Horenovsky.

[121] Alberto Quintavalla and Jeroen Temperman, *Artificial Intelligence and Human Rights* (Oxford, UK: Oxford University Press, 2023).

consumer protection, and safety measures. Such an approach provides a stable regulatory perimeter while allowing adjustments as needed to address emerging risks.

Regulations should require that system-enabling features be disabled if the system begins to operate beyond expected limits to keep AI technology under human control.[122] Additionally, a clearer regulatory framework is needed to define the compliance requirements for AI developers and banks, as the legal landscape surrounding AI regulation is currently evolving. By setting concrete standards, regulators can help prevent ambiguities that may lead to inconsistent compliance practices or loopholes in AI risk management.

The challenge for regulators is exacerbated by the pace of market developments, which often outstrips the speed at which regulatory measures can be implemented. While this gap is commonly accepted as part of a market dynamic, it can pose severe risks to financial stability if regulators are unprepared to respond to systemic AI-related issues. Regulators must stay informed about rapid AI advancements to reduce the delay between AI developments and regulatory responses. Investing in AI technologies themselves could enhance regulators' capacity to monitor developments in real time, offering a way to bridge the informational divide and better anticipate potential issues.[123]

In the context of AML detection, regulators may need broader emergency powers to respond swiftly and effectively. Since AI-related challenges can significantly affect individual rights, regulatory frameworks should be flexible enough to enable timely interventions. The shift could also reshape the regulatory landscape, potentially reducing the role of traditional legal systems and courts as regulators take on a more central role in managing AI-related emergencies. A proactive regulatory stance, with robust emergency powers, would enable regulators to address AI risks efficiently and maintain stability in an increasingly AI-based AML strategy.

Conclusion

AI focuses on creating systems that enable machines to perform cognitive tasks like human-like thinking, communication, and behaviour. A major subfield of AI, machine learning, allows machines to acquire knowledge from data autonomously. AI has found applications across many sectors, including finance, where it is used to detect and prevent criminal activities like money laundering by analysing transactions and customer behaviour. In the banking industry, machine learning improves CDD processes by analysing historical data and customer behaviors, allowing banks to identify high-risk individuals and suspicious activities more effectively. AI also automates decision-making, generates risk reports, and continuously monitors transactions, reducing compliance costs and enhancing proactive responses to emerging threats. AI technologies in e-KYC, automated alerts, and document verification systems have streamlined compliance procedures, improving the efficiency and accuracy of customer identification, especially in the face of growing online banking risks and fraud. AI systems also enhance transparency and compliance with beneficial ownership regulations. AI-based transaction monitoring systems improve efficiency and adapt to emerging financial crime trends.

However, AI also introduces ethical challenges, including the risk of exploitation by irresponsible individuals to compromise security, such as through spear phishing. Ethical concerns surrounding AI in financial services, especially in AML compliance, are increasingly significant. AI systems can perpetuate bias, particularly through profiling based on ethnicity or profession, raising concerns about discrimination. Privacy is another major issue, especially in countries like Indonesia, where privacy regulations are still evolving.

[122] Quintavalla and Temperman.

[123] Quintavalla and Temperman.

The proportionality test with Article 28J of the 1945 Constitution provides a framework for limiting rights in a way that respects public order and morality. For AI-based AML strategies, the test ensures that privacy rights are not unduly infringed upon and that measures are necessary and proportionate to combating criminal activities. Practically, this means AI systems must be transparent, effective, and minimally invasive. Challenges arise, particularly with the surveillance of suspicious activities, as current AML/CFT laws prevent the notification of individuals who may be under investigation. Legal amendments are needed to increase transparency while safeguarding investigations and ensuring that AI technologies are used responsibly and ethically. Laws must guide AI development to ensure fairness, accountability, and transparency, protecting individuals' rights while fostering trust in AI technologies.

References

Ahmed, Faraz. "Ethical Aspects of Artificial Intelligence in Banking." *Journal of Research in Economics and Finance Management* 1, no. 2 (2022): 55–63. https://doi.org/10.56596/jrefm.v1i2.7.

Aluko, Ayodeji, and Mahmood Bagheri. "The Impact of Money Laundering on Economic and Financial Stability and on Political Development in Developing Countries: The Case of Nigeria." *Journal of Money Laundering Control* 15, no. 4 (2012): 442–57. https://doi.org/10.1108/13685201211266024.

Bajgar, Ondrej, and Jan Horenovsky. "Negative Human Rights as a Basis for Long-Term AI Safety and Regulation." *Journal of Artificial Intelligence Research* 76 (2023): 1043–75. https://doi.org/10.1613/jair.1.14020.

Bertrand, Astrid, Winston Maxwell, and Xavier Vamparys. "Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?" *SSRN Electronic Journal* (2020): 1–27. https://doi.org/10.2139/ssrn.3647420.

Bieler, S. Alexandra. "Peeking into the House of Cards: Money Laundering, Luxury Real Estate, and the Necessity of Data Verification for the Corporate Transparency Act's Beneficial Ownership Registry." *Fordham Journal of Corporate and Financial Law* 27 (2022): 193.

Chatterjee, Sheshadri, and N. S. Sreenivasulu. "Artificial Intelligence and Human Rights: A Comprehensive Study from Indian Legal and Policy Perspective." *International Journal of Law and Management* 64, no. 1 (2022): 110–34. https://doi.org/10.1108/ijlma-02-2021-0049.

Chitimira, Howard, Elfas Torerai, and Lisa Jana. "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector." *Potchefstroom Electronic Law Journal* 27 (2024): 1–30. https://doi.org/10.17159/1727-3781/2024/v27i0a18024.

Circiumaru, Alexandru. "Towards European AI: Part I - Setting the Context." Queen Mary University of London. Last modified October 18, 2019. https://www.qmul.ac.uk/euplant/blog/items/towards-european-ai-part-i---setting-the-context-.html.

Constitutional Court of the Republic of Indonesia. "Decision Number 14/PUU-VI/2008." MKRI. Last modified 2020. https://en.mkri.id/court/decision?search=14%2FPUU-VI%2F2008.

———. "The 1945 Constitution of the Republic of Indonesia." MKRI. Last modified 2020. https://en.mkri.id/library/constitution.

Conte, Alex. "Limiting Rights Under International Law." In *Human Rights in the Prevention and Punishment of Terrorism*, edited by Alex Conte, 283–314. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-11608-7_10.

Dewi, Sinta, and Mohammad Wildan Hidayat. "Protection of Data Privacy in The Era of Artificial Intelligence in The Financial Sector in Indonesia." *Journal of Central Banking Law and Institutions* 1, no. 2 (2022): 353–66. https://doi.org/10.21098/jcli.v1i2.18.

Digital Finance. "Asia Banks Spend $45 Billion on Compliance – for What?" *Digital Finance*, March 13, 2024. https://www.digfingroup.com/compliance-lexisnexis/.

FATF. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." FATF-GAFI. Last modified 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/Recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

Gupta, Abhishek, Dwijendra Nath Dwivedi, and Ashish Jain. "Threshold Fine-Tuning of Money Laundering Scenarios through Multi-Dimensional Optimization Techniques." *Journal of Money Laundering Control* 25, no. 1 (2022): 72–78. https://doi.org/10.1108/jmlc-12-2020-0138.

Gupta, Abhishek, Dwijendra Nath Dwivedi, and Jigar Shah. *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance*. Future of Business and Finance. Singapore: Springer Nature Singapore, 2023. https://doi.org/10.1007/978-981-99-2571-1.

Hannan, Md. Abdul, Md. Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad Shahriar Rahman. "A Systematic Literature Review of Blockchain-Based e-KYC Systems." *Computing* 105, no. 10 (2023): 2089–2118. https://doi.org/10.1007/s00607-023-01176-8.

Japanese Society for Artificial Intelligence. "The Japanese Society for Artificial Intelligence Ethical Guidelines." Last modified 2017. https://www.ai-gakkai.or.jp/ai-elsi/wp-content/uploads/sites/19/2017/05/JSAI-Ethical-Guidelines-1.pdf.

Jullum, Martin, Anders Løland, Ragnar Bang Huseby, Geir Ånonsen, and Johannes Lorentzen. "Detecting Money Laundering Transactions with Machine Learning." *Journal of Money Laundering Control* 23, no. 1 (2020): 173–86. https://doi.org/10.1108/jmlc-07-2019-0055.

Kartika, Widya, Rahmanda M. Thaariq, Dwi Rahayu Ningrum, and Herni Ramdlaningrum. "Highlighting Illicit Financial Flow of Indonesia's Top Six Export Commodities." *Prakarsa Policy Brief* 17 (2019): 1–4.

Kaur, Guneet. "Trust the Machine and Embrace Artificial Intelligence (AI) to Combat Money Laundering Activities." In *Disruptive Technologies and Digital Transformations for Society 5.0*, edited by Sandeep Kautish, Prasenjit Chatterjee, Dragan Pamucar, N. Pradeep, and Deepmala Singh, 63–81. Singapore: Springer Nature Singapore, 2024. https://doi.org/10.1007/978-981-99-5354-7_4.

Makmur, Kartini Laras. "Women and Dirty Money: How Women Are Affected by, Involved, and Counter Money Laundering." *Jurnal Hukum Prasada* 9, no. 1 (2022): 35–44. https://doi.org/10.22225/jhp.9.1.2022.35-44.

Makmur, Kartini, and Ahsanul Minan. "Money Laundering/Financing of Terrorism Risks in the Indonesian Islamic Banking System." In *Proceedings of the 3rd International Conference of Islamic Finance and Business, ICIFEB 2022, 19-20 July 2022*, 10–21. Jakarta, Indonesia: EAI, 2023. https://doi.org/10.4108/eai.19-7-2022.2328202.

OECD. "AI Principles." OECD. Last modified 2024. https://www.oecd.org/en/topics/sub-issues/ai-principles.html.

Press, Gil. "Artificial Intelligence (AI) Defined." *Forbes*, August 27, 2017. https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/.

Quintavalla, Alberto, and Jeroen Temperman. *Artificial Intelligence and Human Rights*. Oxford, UK: Oxford University Press, 2023.

Schlink, Bernhard. “Proportionality in Constitutional Law: Why Everywhere but Here?” *Duke Journal of Comparative & International Law* 22 (2012): 291.

Sieckmann, Jan. “Proportionality as a Universal Human Rights Principle.” In *Proportionality in Law*, edited by David Duarte and Jorge Silva Sampaio, 3–24. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-89647-2_1.

Śliwiński, Emil. “Principle of Proportionality as a Threat to Criminal-Law-Related Fundamental Rights.” *New Journal of European Criminal Law* 14, no. 3 (2023): 327–44. https://doi.org/10.1177/20322844231158323.

Sullivan, Morgan. “Big Tech’s Evolving Role in AI Governance: Shaping Ethical Standards.” *Transcend*, March 21, 2024. https://transcend.io/blog/big-tech-ai-governance.

The European Parliament and The Council. *2016/679 General Data Protection Regulation*. The European Parliament and The Council, 2016.

The Senate of The United States. “Bill to Provide a Framework for Artificial Intelligence Innovation and Accountability, and for Other Purposes.” congress.gov. Last modified November 15, 2023. https://www.congress.gov/118/bills/s3312/BILLS-118s3312is.pdf.

UN Human Rights Committee. “General Comment No. 31 [80], the Nature of the General Legal Obligation Imposed on States Parties to the Covenant.” Refworld. Last modified May 26, 2004. https://www.refworld.org/legal/general/hrc/2004/en/52451.

United Nations. “Universal Declaration of Human Rights.” Last modified 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Yeoh, Peter. “Banks’ Vulnerabilities to Money Laundering Activities.” *Journal of Money Laundering Control* 23, no. 1 (2019): 122–35. https://doi.org/10.1108/jmlc-05-2019-0040.