Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector

H Chitimira*, E Torerai** and VLM Jana***

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed,
open access online law publications

Authors

Howard Chitimira
Elfas Torerai
Vimbai Lisa Michelle Jana

Affiliation

North-West University,
South Africa

Email

Howard.Chitimira@nwu.ac.za
elfas.torerai@gmail.com
lvjae@yahoo.com

Date Submitted

19 February 2024

Date Revised

17 July 2024

Date Accepted

17 July 2024

Date Published

10 September 2024

Editor

Prof W Erlank

Journal Editor

Prof W Erlank

How to cite this contribution

Chitimira H, Torerai E, and Jana VLM "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector" *PER / PELJ* 2024(27) - DOI http://dx.doi.org/10.17159/1727-3781/2024/v27i0a18024

DOI
http://dx.doi.org/10.17159/1727-3781/2024/v27i0a18024

Abstract

Money laundering and related financial crimes, such as fraud and terrorism financing, pose a significant threat to the integrity and stability of South African financial markets. This article explores the application and use of artificial intelligence (AI) to detect and prevent money laundering in South African banking institutions. The implementation of big data technologies, data processing analytics and AI could enhance the detection and prevention of money laundering activities in South Africa's banking sector. AI should be carefully utilised to improve the detection of suspicious activities and the accuracy of financial intelligence, and to combat evolving money laundering techniques. The article also examines the benefits and challenges of implementing AI as an anti-money laundering (AML) measure in the South African banking sector. These include the need for quality data, integration with existing regulatory systems, regulatory compliance and ethical considerations. The article highlights the potential use of AI in transaction monitoring, customer due diligence, outcomes-based risk assessment and the improved detection of suspicious transactions. This could be done by utilising AI to enhance the effectiveness and efficiency of AML measures. The importance of effective coordination between banking institutions, regulatory authorities and law enforcement bodies is also highlighted as a key component of leveraging AI to combat money laundering and related financial crimes in South Africa's banking sector.

Keywords

Artificial intelligence; money laundering; banking institutions; customer due diligence.

.....

1 Introductory remarks

Money laundering remains a persistent threat that is posing significant challenges to the integrity of global financial markets, especially in the wake of the technological challenges driven by global information and communication networks.[1] This necessitates the need to use advanced technology such as artificial intelligence (AI) to fortify anti-money laundering (AML) measures globally.[2] In 2015, the United Nations (UN) General Assembly established a worldwide framework to address global sustainable development, encompassing seventeen goals commonly known as the Sustainable Development Goals (SDGs).[3] Each of these goals addresses specific social, economic, or environmental concerns, spanning from the eradication of poverty and the fighting of crime. SDG 16 is dedicated to "peace, justice, and strong institutions".[4] This goal includes a sub-target 16.4, which specifically addresses the reduction of illicit financial flows and the combatting of organised crime.[5] Target 16:4 provides that by 2030, there should be a significant reduction in illicit financial flows, strong mechanisms to recover and return stolen assets, and success in combatting all forms of organised crime globally.[6]

Money laundering and other related financial crimes represent a pervasive and escalating threat to the integrity and stability of financial markets,

* Howard Chitimira. LLB *(Cum Laude*), LLM (UFH), LLD (NMMU). Research Professor, Research Director and Professor of Securities and Financial Markets Law, Faculty of Law, North-West University, South Africa. Email: Howard.Chitimira@nwu.ac.za. ORCiD: https://orcid.org/0000-0003-1881-1242.

** Elfas Torerai. BSc (MSU), LLB (Unisa), LLM (NWU), LLD (NWU). Postdoctoral Research Fellow, Faculty of Law, North-West University, South Africa. Email: elfas.torerai@gmail.com. ORCiD: https://orcid.org/0000-0002-9680-5430.

*** Vimbai Lisa Michelle Jana. LLB (Wits), LLM (UWC), LLD (NWU), Faculty of Law, North-West University. ICA certified Money laundering Reporting Officer. Email: lvjae@yahoo.com. ORCiD: https://orcid.org/0000-0002-2509-8919. This article is influenced in part by Jana's LLD thesis titled: *A Comparative Statutory Analysis of the Regulation of Money Laundering in Zimbabwe* (LLD-thesis North-West University 2024) 239-249. In this regard, I wish to acknowledge the expert inputs of Prof Chitimira and Dr Torerai.

1 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 13-14; Whisker and Lokanan 2019 *JMLC* 159-160.

2 Pavlidis 2023 *JMLC* 159; see related comments by Kute *et al* 2021 *IEEE Access* 82301.

3 UN Department of Economic and Social Affairs date unknown https://sdgs.un.org/goals; Carlsen and Bruggemann 2022 *International Journal of Sustainable Development and World Ecology* 229.

4 Goetz and Jenkins 2016 *Gender and Development* 127.

5 UN Department of Economic and Social Affairs date unknown https://sdgs.un.org/goals Target 16:4.

6 UN Department of Economic and Social Affairs date unknown https://sdgs.un.org/goals Target 16:4.

especially the banking sector.[7] This is attributable, in part, to the intricate nature of modern financial transactions, coupled with the rapid evolution of money laundering techniques. Countries such as South Africa require robust and innovative measures in order to effectively combat money laundering and other related crimes.[8] The *Financial Intelligence Centre Act* (*FICA*)[9] provides some non-innovative measures to combat and curb money laundering in South Africa.[10] The same status quo is duplicated in other AML regulations and statutes such as the *Prevention of Organised Crime Act* (*POCA*),[11] the *General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act*,[12] the *Protection of Constitutional Democracy against Terrorist and Related Activities Act*[13] and the Financial Intelligence Centre Regulations. AI is a handy tool for enhancing the efficiency and quality of financial services. However, it comes with risks to the integrity and financial stability of financial markets such as recording false positives and inadequately focussing on data quality assurance.[14] For the purposes of this article, the advent of AI is seen in the broad context of advanced technological innovations that can be effectively used as techniques to enhance the effectiveness of AML measures in the South African banking sector.[15] To this end, AI should be deployed to fortify AML measures in the South African banking sector.

However, the rapid evolution of the money laundering methods, trends, and techniques used by the perpetrators of money laundering offences has impeded the effective combatting of such offences.[16] The current South African AML legal framework does not effectively combat the unique

7 Van Jaarsveld *Aspects of Money Laundering* 7.

8 See related comments by Pavlidis 2023 *JMLC* 159-160; Menon and Guan Siew 2012 *JMLC* 245.

9 *Financial Intelligence Centre Act* 38 of 2001 as amended (*FICA*) ss 21-45; De Koker 2004 *TSAR* 718; Tuba 2012 *Acta Criminologica* 110.

10 See ss 20A-45 of *FICA*, which stipulate that financial institutions are obliged to do client identity verification in order to ascertain the identity of their customers.

11 See *Prevention of Organised Crime Act* 21 of 1998 (*POCA*) s 4; Kersop and Du Toit 2015 *PELJ* 1624; Tuba 2012 *Acta Criminologica* 109.

12 *General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act* 22 of 2022 ss 18-20; National Treasury 2023 https://www.treasury.gov.za/comm_media/press/2023/2023010601%20MEDIA%20STATEMENT-ENACTMENT%20OF%20KEY%20ANTI-MONEY%20LAUNDERING%20AND%20COMBATING%20OF%20TERROR%20FINANCING%20LAWS%20.pdf 2; Moonstone Information Refinery 2022 https://www.moonstone.co.za/did-grey-listing-threat-hasten-sarb-to-act-against-markus-jooste/.

13 *Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004 s 2; see Khumalo 2023 *African Security Review* 1-2; Roach 2005 *SACJ* 130.

14 See Kute *et al* 2021 *IEEE Access* 82304.

15 Nizovtsev *et al* 2021 *JMLC* 299.

16 Enholm *et al* 2022 *Information Systems Frontiers* 1712.

technology-driven risks and threats that are posed to market integrity and financial stability by the perpetrators of money laundering. This is owing to the fact that AI-driven financial transactions fall outside the scope of traditional AML regulations.[17] This flaw could be exacerbated by the dynamic nature of AI systems, making it difficult for the current AML laws and regulations to keep pace with the emerging AI-induced money laundering techniques.[18] Moreover, the lack of clear guidelines on the integration and use of AI by financial institutions to curb money laundering might create ambiguity and hinder the effective enforcement of AML laws, regulations and policies. The South African AML regulatory framework should be revamped to enact provisions that expressly address the intersection between AI and money laundering in order to provide guidelines on the responsible use of AI in the financial sector. These could include measures to ensure the transparency, accountability, and traceability of AI algorithms that are used in financial transactions, as well as the incorporation of AI-specific risk assessments into AML compliance programmes. Strengthening these aspects of the South African AML regulatory framework could enhance the combatting of all money laundering risks that are associated with AI in the banking sector.

Therefore, despite the potential benefits that AI brings to the financial sector, there are notable challenges and limitations that impede its reliability in the fight against money laundering and other financial crimes.[19] The inherent complexity and adaptability challenges of money laundering schemes, which can evolve rapidly as a counter-response to detection methods employed by AI algorithms, affect the combatting of money laundering. Criminals may exploit vulnerabilities in AI systems by using sophisticated techniques to conduct illicit financial activities without detection.[20] Moreover, the reliability of AI models is contingent on the quality and quantity of the data which are received and processed by the relevant AI systems.[21] If the collected data is biased or incomplete, the AI systems are likely to generate inaccurate or incomplete results which would ultimately lead to false positives or negatives in identifying suspicious transactions.[22] Financial crimes often involve subtle patterns and intricate connections that may elude even the most advanced AI systems, particularly when dealing with the novel and/or sophisticated techniques employed by criminals. Additionally, the dynamic nature of financial markets poses a challenge for

17 Njontini 2021 *De Jure* 179.
18 See Njontini 2021 *De Jure* 179.
19 Alhajeri and Alhashem 2023 *Intelligent Information Management* 284.
20 FATF 2021 https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html.
21 Kute *et al* 2021 *IEEE Access* 82304-82305; also see Pavlidis 2023 *JMLC* 157-160.
22 FATF 2021 https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html.

AI systems that may struggle to quickly adapt to emerging threats and regulatory changes through poor calibrations.[23] The poor calibrations and the complexity of some AI systems further complicate their integration into the AML framework, making it difficult for regulators and financial institutions to understand the reasoning behind AI-generated alerts. In addition, it should be noted that South Africa's AML regulatory framework does not expressly provide for the combatting of AI-induced money laundering and other financial crimes.

Accordingly, this article explores the use of AI-related AML measures to curb money laundering in the South African banking sector. The article also discusses shortcomings in the current South African AML regulatory framework. Thereafter, recommendations that could be utilised by policymakers to enhance the South African AML regulatory framework are provided.

2 The definition of key terms

The *FICA* defines money laundering as an act that involves the concealing or disguising of the nature, source, location, disposition or movement of the proceeds of unlawful activities in order to use financial resources derived from criminal activities as if they are from a legitimate and lawful source.[24] This definition shows that money laundering could be described as a process designed to legalise illegal income or assets.[25] Money launderers always seek to disguise their illicit transactions to avoid detection. Money laundering is a multi-layered process which involves several transactions and participants to erase the true nature of the illicit funds which are laundered.[26] It also involves the commission of other crimes to acquire assets, resulting in the blending of these unlawfully obtained funds with legitimate sources, the obscuring of their origin, and the creation of an appearance of legitimacy at the conclusion of the process.[27] Although some commentators argue that the laundered funds should cross various jurisdictions in order to be considered truly “laundered”, money laundering can still occur within a particular jurisdiction or country.[28] However, it is contended that it is not a fundamental prerequisite for money laundering

23 FATF 2021 https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities -challenges-new-technologies-for-aml-cft.html.

24 Section 1 of the *FICA*.

25 Hamman *Impact of Anti-Money Laundering Legislation* 8.

26 The proceeds need not always be cash. They can assume any form, such as diamonds, gold, credit cards slip, stocks and bonds, cashier cheques, airplanes, rare coins, livestock, postal money orders, airline tickets, and wire transfers. Other synonyms, such as "tainted money", "illegal money", "hot money", or "black money" are also used to describe the proceeds of crime.

27 During this process the illicit proceeds of the criminal activities are intermingled with legitimate funds, which means that the "dirty money" is mixed with "clean money".

28 See related comments by Goredema 2007 *ISS Monograph Series* 78.

since money may be laundered without leaving an economic area or crossing jurisdictions. Any money that is acquired through illegal means constitutes "dirty" money that requires a process of "cleaning" before its successful integration into the legitimate economy.[29] AI technologies could enable this cleaning transformation of dirty money to inadvertently empower those with such money to use it freely without fear of legal repercussions. Irrespective of the definition employed, the primary objective of money launderers is to mitigate or eliminate the risk of the funds being seized or forfeited after detection.[30] Ultimately, the overarching goal for money launderers is to enjoy the benefits of their crime without facing legal consequences.

Money laundering is a pressing global issue for regulators and law enforcement authorities. Those engaged in money laundering activities continually seek opportunities to legitimise their unlawfully gained assets.[31] Most forms of criminal activity inherently involve gaining and enjoying monetary benefits. Once criminals acquire cash and other assets from their illegal pursuits, they begin to engage in the process of money laundering to "cleanse" their illegal assets so that they appear legitimate.[32] This is done to transfer illegally obtained money through legitimate people or legitimate accounts so that its original source cannot be traced. Money laundering allows wrongdoers to camouflage and transfer substantial amounts of illicitly gained funds. It empowers criminal enterprises to operate effectively.[33] The typical money laundering process involves three key stages, the first of which is placement, which occurs when illicit funds enter the financial system, often through depositing them into a bank account.[34] The second stage is the layering of the funds, which occurs when a series of transactions are completed with the intention of distancing the funds from their illegal origins.[35] Lastly, the integration stage occurs when the previously tainted funds are disguised as legitimate so that they are seamlessly blended into the financial markets.[36] Against this background, it then becomes imperative to discuss the role of AI in combatting money laundering in South Africa.

---

29 Goredema 2007 *ISS Monograph Series* 78.

30 See Goredema 2007 *ISS Monograph Series* 78.

31 UNODC 2016 https://www.unodc.org/unodc/en/moneylaundering/introduction.html?ref=menuside.

32 Boles 2019 *Am Bus L J* 365.

33 Boles 2019 *Am Bus L J* 365.

34 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 2-4; Ennis 2002 *Law Business Review of the Americas* 637.

35 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 2-4; Financial Institutions Examination Council 2014 https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf.

36 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 2-4; Sultzer 1995 *Tenn L Rev* 143.

AI is an evolving concept that can be broadly defined as the use of powerful algorithms, machines and computer systems to simulate human intelligence, behaviour and capabilities through techniques such as machine learning and logic programming.[37] Using big data, the algorithms, machines and computers are able to perform human-like tasks. This is possible through, *inter alia*, identifying patterns and solving specific problems.[38] In this regard, AI stands a good chance of dismantling the intricate web of money laundering in South Africa's banking sector.

3 Overview background on money laundering crime in South Africa

Money laundering poses significant threats to the stability and integrity of financial markets globally. It is also a constant challenge to South Africa's banking sector. Pecuniary benefits serve as a key motivating factor for criminals when they undertake illegal activities such as human trafficking and money laundering.[39] For instance, human trafficking generates approximately US$150.2 billion per year globally for criminal organisations through activities such as money laundering, forced labour, sexual exploitation and organ harvesting.[40] A lot of dirty money is required to complete and further such criminal enterprises. In cases of human trafficking, money is needed to move the victims across various locations where they are exploited. As part of the criminal operations, money is necessary to bribe and pay the various complicit intermediaries who form part of the trafficking network that aids the criminal activities.[41] Given the strong link between money and crime, most governments pursue initiatives to curtail the movement of money through money laundering among criminal organisations, in an attempt to reduce the criminals' incentive and ability to engage in illicit behaviour. South Africa functions as a prominent financial hub in Africa, boasting a robust banking and financial services sector along with a substantial cash-based market.[42] This makes South Africa an attractive destination for criminals wanting to conduct illicit activities such as money laundering.[43] Although South Africa is historically known as a vibrant and diverse economy, it is also susceptible to money laundering and related

37 Ncube *et al* "Setting out the Challenges" 1.
38 Ncube *et al* "Setting out the Challenges" 1-2.
39 Byrne 2011 *Journal of Business Ethics* 498.
40 FATF 2018 https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.
41 Ball *et al Private Security State?* 23-34.
42 See related comments by Bara and Le Roux 2017 *Journal of Economic and International Finance* 71.
43 Marakalala and Mokwena 2023 *International Journal of Social Science Research and Review* 529. British authorities have admitted that South Africa is being targeted as a money-laundering hotspot, and local authorities are fighting to make money laundering as difficult as possible.

crimes. In this regard, it is important to note that South Africa has a very low prosecution rate for serious financial crimes. This is partly because it has a weak primary AML legislative framework.[44] The low prosecution rate of money laundering crime implies that there is an ineffective application of the AML/CTF framework in South Africa.[45] Former Finance Minister, Trevor Manuel, estimated that South Africa lost between R21 billion and R85 billion through money laundering in the early 2000s.[46] It is possible that the level of money laundering has increased over the years.

Consequently, there is a need for a paradigm shift in the choice of AML strategies. AI technology should be recognised as an integral tool to use in effectively combatting money laundering in South Africa. While South Africa currently employs the traditional AML measures, there is a concern that they may fall short in combatting sophisticated money laundering threats that are technologically aided.[47] Hence, the rationale in advocating the use of AI technology-driven innovation in AML measures is underscored by the limitations of the existing rule-based systems in coping with the dynamic nature of money laundering.[48] This necessitates the adoption of a proactive and technology-driven approach to detect, prevent, and mitigate the risks associated with illicit financial activities such as money laundering. Moreover, the use of AI can produce measurable outcomes rather than following a limited rule-based approach which is increasingly becoming a tick-box exercise which does not effectively curb money laundering.

Against this backdrop, the integration of AI technologies into South Africa's AML regulatory framework presents a promising avenue to strengthen the resilience of banking institutions. The incorporation of AI technologies, particularly big data analytics, presents a paradigm shift in the fight against money laundering.[49] AI offers the capability to analyse vast datasets with speed and accuracy far beyond the scope and depth of traditional or manual AML methods.[50] AI systems can discern patterns, anomalies and trends which may be indicative of potential money laundering activities by leveraging machine learning algorithms. Thus, AI technologies will not only enhance the efficiency of AML processes, but they will also provide a proactive approach to identifying AML risks and emerging threats to the

44 See ss 4-8 of the *POCA*; De Koker 2003 *JMLC* 32; Basdeo 2013 *AJICL* 308-309.
45 See related comments by Chitimira 2021 *JMLC* 799; Schlenther 2013 *JMLC* 127.
46 Schlenther 2014 *JMLC* 21-22; Goredema 2007 *ISS Monograph Series* 78.
47 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 15-16; also see Goredema 2007 *ISS Monograph Series* 78.
48 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 15-16; Goredema 2007 *ISS Monograph Series* 78.
49 Mckinsey and Company 2022 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer.
50 Kute *et al* 2021 *IEEE Access* 82301.

South African banking sector.[51] In addition, the adaptability of AI technological systems allows them to evolve in line with the fast-changing nature of money laundering techniques, ensuring a sustainable and effective defence against such illicit financial activities.[52]

4 The use of artificial intelligence to combat money laundering in South Africa

AI proves highly pertinent in this age of big data, given its capacity to process substantial amounts of data, including unstructured inputs like images and speeches.[53] AI measures such as machine learning algorithms are responsible for processing data inputs.[54] Machine learning utilises the computational process that aims to identify patterns in the dataset where the rules link inputs to outputs.[55] In addition, AI relies on predetermined rules that enable the computational process to apply these rules to input data in order to generate an output.[56] Nonetheless, AI and machine learning measures are not yet utilised in AML regulatory measures under the *POCA* and the *FICA* in South Africa.

Machine learning encompasses diverse types of computational processes, each tailored to address and solve specific problems such as detecting money laundering patterns in a particular jurisdiction.[57] The human supervised machine learning matches scenarios with known inputs and outputs.[58] In this regard, the human analyst manipulates identified money laundering detection datasets, separating and labelling data as either input or output. The AI algorithms detect patterns connecting inputs to outputs and formulate rules applicable to future instances of the problem.[59] Conversely, unsupervised machine learning, where distinguishing between inputs and outputs is unknown, could give rise to mistakes and false conclusions.[60] The human analyst furnishes the computer with an

51 Han *et al* 2020 *Digital Finance* 213.
52 Han *et al* 2020 *Digital Finance* 213.
53 Big data refers to extremely large and complex sets of information that traditional data processing methods struggle to manage efficiently. It involves the collection, storage, and analysis of vast amounts of data, often characterised by the three Vs: volume (large amounts of data), velocity (rapid data generation and processing), and variety (diverse types of data, such as text, images, and videos). Big data analytics involves using specialised techniques and technologies to extract valuable insights, patterns and trends from these massive datasets, enabling better decision-making and problem-solving; Kietzmann, Paschen and Treen 2018 *Journal of Advertising Research* 264.
54 Skiena *Algorithm Design Manual* 5.
55 Canhoto 2021 *Journal of Business Research* 442.
56 Canhoto 2021 *Journal of Business Research* 442-443.
57 See related comments by Kute *et al* 2021 *IEEE Access* 82304-82305.
58 Canhoto 2021 *Journal of Business Research* 442.
59 Canhoto 2021 *Journal of Business Research* 442.
60 Canhoto 2021 *Journal of Business Research* 442.

unlabelled dataset, manipulating the algorithm by determining optimal data point groupings and formulating rules to elucidate their relationships.[61] An intermediary technique, reinforced machine learning suits problems where specific actions yield superior results, like playing a game.[62] In this context, the human analyst supplies the computer with a dataset, a goal and associated rewards or penalties for actions taken.[63] The algorithms should identify the optimal action to achieve the goal, sifting through potential data combinations and analysing rewards for different permutations to identify possible money laundering patterns.[64] The selection of the algorithm type should ideally align with the nature of the problem at hand.[65] However, in practice, this decision is often influenced by pragmatic considerations such as the human analyst's expertise, compatibility between programming languages[66] and/or the available processing power.[67] However, AI algorithms and related measures are still not used to detect and combat money laundering in South Africa under the *POCA* and the *FICA*.

Big data plays a pivotal role in the development of machine learning algorithms and the overall performance of algorithms. Without data, algorithms are likened to mathematical fictions.[68] Depending on the technical specifications, data can encompass structured data (numeric data) or extend to unstructured data like images or voice.[69] Datasets should be carefully utilised to detect suspicious activity that may be indicative of money laundering activities. These datasets are derived from historical databases such as shipping addresses or the types of internet protocol (IP) address connections which are used by a client when communicating with a financial institution.[70] Real-time data to analyse transaction patterns may be collected through physical sensors or online tracking or knowledge data such as the acceptance or rejection of previous financial product recommendations.[71] Furthermore, data to create a clear client activity profile can be obtained internally or externally.[72] Deciding which type of data to use or how much data to incorporate is often constrained by the necessity for systems compatibility across various elements of AI measures that are

61 Kute *et al* 2021 *IEEE Access* 82304-82307.
62 Mnih et al 2013 https://arxiv.org/pdf/1312.5602.pdf.
63 See related comments by Kute *et al* 2021 *IEEE Access* 82304-82308.
64 Mnih et al 2013 https://arxiv.org/pdf/1312.5602.pdf.
65 See Skiena *Algorithm Design Manual* 5.
66 Calvard 2016 *Management Learning* 67.
67 See related comments by Agarwal and Dhar 2014 *Information Systems Research* 445-446.
68 Constantiou and Kallinikos 2015 *Journal of Information Technology* 46.
69 Paschen, Pitt and Kietzmann 2020 *Business Horizons* 150.
70 O'Hear 2016 https://techcrunch.com/2017/01/16/fraugster/.
71 Stervinou 2015 https://www.kansascityfed.org/Payments%20Conferences/documents/7490/PSCP2015_StervinouPaper.pdf.
72 Jacob and Summers 2008 https://www.chicagofed.org/publications/chicago-fed-letter/2008/july-252.

employed.[73] While the standardisation of AI technologies across institutions enhances the ability to utilise multiple and fragmented data sources for the regulator, it simultaneously diminishes the AI measures' flexibility and restricts contextual richness and competition amongst AI providers.[74] Another critical consideration involves the quality of the harvested dataset, specifically how the data were gathered, their age and whether they are an accurate representation of the broader population's transactional patterns.[75] Therefore, the challenge of the quality of the harvested data becomes pertinent in the case of externally controlled or acquired data, where firms may face challenges in accessing and evaluating the underlying assumptions and data sources driving an AML process for a financial institution.[76] Unfortunately, big data and other AI-related measures are not yet used by regulatory authorities to curb money laundering in the South African financial sector under the *POCA* and the *FICA*.

After the machine learning algorithm processes data for AML, the AML system generates an output whose nature and independence can vary.[77] Machine learning autonomously acts based on computational results, like self-driving cars.[78] However, the system's output can be as straightforward as a score, lacking performative value until a human analyst acts upon it.[79] This output can also be reintroduced into the AML dataset to further refine the algorithm's capabilities of detecting suspicious activity or unusual transactions such as money laundering.[80] This capability indicates that machine learning algorithms can learn and adapt over time to changes in their environment.[81] Nevertheless, this adaptability can lead to complex and incomprehensible self-reinforcing feedback loops such as those generated by Facebook's AI negotiation bots, which create their own language.[82] These loops can propagate biases and errors, as seen in AI-powered bots disseminating unverified information and automatic trading algorithms causing stock market flash crashes.[83] This issue becomes particularly significant in predictive analytics, where assessing output quality before implementation and scaling is challenging for human analysts.[84] AI and

73 Gates and Jacob 2009 *Economic Perspectives* 7-15.
74 Alaimo and Kallinikos 2017 *Information Society* 175.
75 Hudson 2017 https://fivethirtyeight.com/features/technology-is-biased-too-how-do-we-fix-it/.
76 Khan *et al* 2020 https://www.digitalistmag.com/executive-research/algorithms-the-new-means-of-production.
77 Canhoto *et al* 2017 *Journal of Strategic Marketing* 386.
78 Goodall 2016 *Applied Artificial Intelligence* 810.
79 Silver *et al* 2017 *Nature* 354-359.
80 Silver *et al* 2017 *Nature* 354-359.
81 Russell *Artificial Intelligence* 5.
82 Lewis *et al* 2017 https://code.facebook.com/posts/1686672014972296/deal-or-no-deal-training-ai-bots-to-negotiate.
83 Ferrara *et al* 2016 *Communications of the ACM* 97.
84 Mittelstadt *et al* 2016 *Big Data & Society*.

machine learning are capable of performing mechanical, analytical, intuitive or even empathetic tasks.[85] However, this is not yet being utilised in South Africa.

5 Leveraging AI to detect money laundering in the South African banking sector

Financial institutions should embrace AI technological measures to detect and prevent financial crimes such as insider trading, money laundering, terrorist financing and fraud in the South African banking sector. AI technological measures could enable banks to easily categorise customers and transactions as high or low risk so as to combat money laundering and related financial crimes.[86] AI algorithms automatically analyse transaction input and output to detect anomalies in the data provided to curb money laundering through predictive and predefined binary rules.[87] Computer scientists are making continuous efforts to enhance algorithm accuracy and reliability in order to reduce false alerts through meticulous record analysis.[88]

AML measures follow a linear workflow in the banking sector, which is connected to a big data source.[89] In this context, human data analysts and programmers incorporate specific parameters to identify risky transactions, customers or communications which may suggest the occurrence of fraudulent behaviour.[90] A typical AML system comprises four layers, namely a data layer for collecting, managing, and storing data; a screening and monitoring layer for analysing clients and transactions for suspicious activities; an alert and event layer for raising alarms in case of suspected transactions; and an operational layer for further action.[91] Financial institutions with effective AML regulatory frameworks rely not only on internal employee data but also on information collected from the fraud and sanctions watchlists of regulatory authorities.[92] The data records undergo analysis using various AI and machine learning techniques such as natural language processing, enhancing computers' ability to comprehend and derive meaning from human languages and providing insights that establish connections between clients and transactions.[93]

85 Huang and Rust 2018 *Journal of Service Research* 159.
86 Allam and Dhunny 2019 *Cities* 89.
87 Alhajeri and Alhashem 2023 *Intelligent Information Management* 284.
88 Jensen 1997 https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf 34.
89 Jensen 1997 https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf 34.
90 Jensen 1997 https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf 34.
91 Truskauskas and Taujanskaitė 2022 *Business and Management* 435.
92 Gaviyau and Sibindi 2023 *JMLC* 225-226.
93 Han *et al* 2020 *Digital Finance* 215.

The screening and monitoring layer employs automated rule-based techniques using expert skills to identify potential money launderers.[94] Rule-based systems use pre-defined parameters and thresholds to detect suspicious trading activities. Striking a balance between being too strict (leading to multiple false alerts) and less strict (allowing illicit transactions), is crucial.[95] This layer retrieves user information from the data layer to screen customers and transactions. The alert and event layer signals the occurrence of a suspected transaction upon identifying suspicious activities.[96] Human AML analysts who are positioned in the first line of defence against money laundering in a financial institution then review the issues raised, taking manual actions such as allowing, rejecting, or blocking transactions.[97] However, the manual review process can overwhelm human AML analysts, creating backlogs in the client due diligence process, especially when the AI-powered system produces numerous false positives.[98]

The effective integration of AI and data mining techniques will curb the challenge of numerous false alerts that could hinder the combatting of money laundering. Thus, the use of an outlier detection method enables the identification of fraud and/or money laundering activities on client profiles.[99] This method empowers human analysts to establish various parameters for a client profile by scrutinising its transaction patterns. The analysis requires a vast dataset comprising hundreds of thousands of records spanning months to years, facilitating the classification of data into distinct clusters or groups. This approach has been acknowledged to be effective because it recognises similarities and differences in transaction patterns and classifies them into activity or pattern groups.[100] Once grouped as such, accounts or client profiles may be clearly differentiated between the levels of risks identified. Furthermore, given the evolving nature of money laundering techniques, AI can detect outliers and changes in behavioural patterns. Hence, AI and machine learning techniques excel in identifying suspicious transactions or irregular networks of money transfers not predefined in the outlier parameters.

94 Kute *et al* 2021 *IEEE Access* 82300.
95 Han *et al* 2021 https://doras.dcu.ie/23358/.
96 Labib, Rizka and Shokry "Survey of Machine Learning" 74.
97 Bellomarini, Laurenza and Sallinger 2020 http://hdl.handle.net/20.500.12708/58323 134.
98 Goecks *et al* 2022 *Intelligent Systems in Accounting, Finance and Management* 71-85.
99 Goecks *et al* 2022 *Intelligent Systems in Accounting, Finance and Management* 71-85.
100 Truskauskas and Taujanskaitė 2022 *Business and Management* 430.

5.1 Benefits of implementing AI in South African banking institutions

There are several benefits that AI can bring in combatting money laundering in the South African banking sector. Some of the benefits are discussed below.

5.1.1 AI enhances customer due diligence and know-your-customer measures

Effective data management is crucial for the streamlined delivery of financial services in the banking sector. AI is a key technology for enhancing data management, improving the speed, efficiency and accuracy of the services provided.[101] Algorithms powered by AI can be developed to effectively detect and prevent money laundering and fraudulent activities by comprehending customer behaviours such as transaction frequency, amounts and network usage.[102] Given the detrimental socio-economic effects of money laundering, banks should remain vigilant. AI technologies may play a pivotal role in proper customer identification to combat money laundering.[103]

The primary defence against money laundering involves a thorough understanding of clients through the Know Your Client (KYC) and Client Due Diligence (CDD) processes.[104] These processes entail that financial institutions should gather sufficient evidence to verify the identity and legal existence of individuals who seek to engage in a business dealing or entering into a business relationship with them.[105] The verification process includes scrutinising customers' official documents such as passports, identity cards, and proofs of names and addresses.[106] The CDD process enables banks to comprehend the nature of a client's business and sources of income to enable the effective monitoring of accounts for potential risks of money laundering. However, challenges arise in the digital era with electronic payment services and anonymous transactions. Therefore, there is a need for more robust and substantive outcomes-based approaches to AML, including harnessing AI technologies to detect illicit financial activities.[107]

---

101 Životić, Ristić and Mirković 2022 *Oditor* 95.
102 See Životić, Ristić and Mirković 2022 *Oditor* 95.
103 Životić, Ristić and Mirković 2022 *Oditor* 95.
104 Životić, Ristić and Mirković 2022 *Oditor* 95.
105 Johari *et al* "Money Laundering" 130.
106 Xu *et al* 2021 *Journal of Forensic and Investigative Accounting* 274-275.
107 Raweh, Cao and Shihadeh 2017 https://scholar.ptuk.edu.ps/handle/123456789/639.

5.1.2 Integrating AI into the CDD processes of South African banks aids the detection of money laundering activities

Financial institutions such as banks collect customer data to assess loan risks, detect money laundering and combat fraudulent activities.[108] AI technology should be employed to enhance customer identification and verification and to promote the principles of CDD so as to curb money laundering.[109] KYC regulations are designed to aid financial institutions in monitoring and combatting money laundering globally.[110] Autonomous AI systems help to process vast amounts of data, identify suspicious transactions, and detect patterns that could be indicative of money laundering transactions.[111]

6 Challenges of using AI in the banking sector

Despite the positive acclaim around AI's efficacy in combatting money laundering, certain limitations impact its reliability. Malicious users can exploit AI systems to pose threats to both digital and physical security in the financial sector.[112] AI could pose a digital security threat through the poor use of machine and data analytics.[113] Spear phishing attacks may be employed to gather critical details about individuals or to pilfer money or personal information, with attackers posing as trustworthy government or financial department entities.[114] Therefore, AI can learn the specific habits of bank users to detect and curb money laundering. The accuracy of data sets in AML processes is crucial for AI to effectively detect money laundering and related illicit activities.[115] Consequently, human interference can compromise the efficiency of AI-based AML systems through data poisoning attacks.[116] The AI programs may learn from these manipulated inputs, enabling attackers to exploit the learned mistakes by introducing fake records during the calibration of AI systems.[117] Given the automated nature of the process, it becomes challenging for humans to discern certain flaws, allowing money launderers to operate with impunity.[118]

Despite the obvious advantages of AI’s big data analysis capabilities, implementing AI technologies in the South African banking sector to combat

---

108 Chen 2020 *Applied Soft Computing* 1-7.
109 Saha, Bose and Mahanti 2016 *Decision Support Systems* 78.
110 See related comments by Gaviyau and Sibindi 2023 *JMLC* 234.
111 Bhatore, Mohan and Reddy 2020 *Journal of Banking and Financial Technology* 111.
112 Brundage *et al* 2018 https://arxiv.org/pdf/1802.07228.
113 Oseni *et al* "Security and Privacy for Artificial Intelligence: Opportunities and Challenges".
114 Huang *et al* 2021 *ACM Computing Surveys* 8.
115 Mirsky *et al* 2023 *Computers and Security*.
116 Mirsky *et al* 2023 *Computers and Security*.
117 See Mirsky *et al* 2023 *Computers and Security*.
118 Mirsky *et al* 2023 *Computers and Security*.

AML also presents multifaceted challenges. Firstly, there is a need for robust data infrastructure management. Many South African financial institutions struggle with fragmented data sources owing to their inability to cope with emerging technologies, making it challenging to build comprehensive AI models for detecting patterns of money laundering.[119] A cohesive and integrated data framework is crucial for the effective functioning of AI-based AML systems.[120]

Secondly, regulatory compliance poses a significant challenge to the combatting of money laundering in South Africa. The integration of AI in AML processes requires alignment with existing regulatory frameworks and ongoing collaboration between banks and regulatory bodies to ensure outcomes-based compliance while leveraging the benefits of AI.[121] Additionally, for an AML system to be effective, the AI that it employs should be capable of interpreting huge datasets accurately without being impeded by false positives inadvertently created by rigid rules-based regulations. The lack of interpretability can hinder substantive regulatory implementation by South African banking institutions and this may pose challenges in justifying AI-driven AML decisions to the regulatory authorities.[122] To this end, the evolving nature of money laundering tactics requires the continuous adaptation of the AI-powered AML models and processes which are adopted by a financial institution. Criminals are constantly changing their strategies. Therefore, AI systems need to be agile enough to rapidly detect new money laundering trends, patterns and methods. This necessitates ongoing investment in research and development to ensure that AI-based AML systems remain effective against all money laundering activities in South African banks.[123]

7 The utilisation of AI in the South African AML regulatory framework

7.1 Cybercrimes Act *19 of 2020*

Money laundering is considered a cybercrime when criminals exploit digital channels, online platforms and digital financial systems to conceal the origins of their illicit funds.[124] In the context of cyber-enabled financial crimes, criminals may leverage various techniques such as online fraud,

119 Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management* 15-16.

120 FATF 2006 https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html.

121 Huang and Rust 2018 *Journal of Service Research* 157.

122 Huang and Rust 2018 *Journal of Service Research* 157.

123 D'Amico *et al* 2020 *Sensors* 1-24.

124 Sections 2-12 of the *Cybercrimes Act* 19 of 2020 (*Cybercrimes Act*); Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494.

phishing, hacking or the use of virtual currencies to manipulate or infiltrate digital financial systems.[125] For instance, cybercriminals may engage in sophisticated schemes involving the illicit transfer of funds through digital channels, making detection and tracking very challenging for enforcement authorities.[126] The convergence of traditional money laundering practices and digital technologies underscores the need for the implementation of robust cybersecurity measures by financial institutions to prevent unauthorised access, data breaches and fraudulent activities.[127] As financial transactions increasingly occur in the digital space, the intersection of money laundering and cybercrime highlights the importance of making comprehensive efforts to combat both money laundering and cyber threats through the utilisation of AI in order to safeguard the integrity of the global financial system.[128] The *Cybercrimes Act* seeks to safeguard individuals, corporations, banks and financial institutions from cybercriminals, terrorists and individuals exploiting computers, the Internet and advanced technologies to commit cybercrimes in the country.[129] This Act prohibits any unauthorised access to data and the illicit acquisition of data by individuals. It seeks to address cyber threats and provide comprehensive protection against unlawful activities conducted through digital means.[130] Under the *Cybercrimes Act*, any person engaging in illegal interference with data or a computer program using either software or hardware tools commits a crime.[131] This Act expressly prohibits activities that involve unauthorised tampering with, disruption of or interference with data or computer programmes, whether achieved through software manipulation or hardware tools.[132] It seeks to establish legal boundaries and deter individuals from engaging in any form of illicit activities that compromise the integrity, security, or functionality of data and computer programs.[133]

The *Cybercrimes Act* plays a crucial role in shaping the landscape for the use of AI in combatting money laundering in South Africa. It establishes a legal framework to address cyber threats that may intersect with financial crimes, such as money laundering, by explicitly outlawing illegal interference with data and computer programmes. AI is a powerful tool in

125 Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494.
126 Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494.
127 Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494.
128 Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494.
129 Sections 2 and 3 of the *Cybercrimes Act*.
130 Sections 4 and 5 of the *Cybercrimes Act*.
131 See ss 4 and 5 of the *Cybercrimes Act*.
132 Sections 4 and 5 of the *Cybercrimes Act*.
133 Sections 4 and 5 of the *Cybercrimes Act*.

analysing vast data sets and detecting patterns indicative of money laundering activities which can benefit from the legal provisions which are set out in the *Cybercrimes Act*. The *Cybercrimes Act* provides a foundation for the secure and lawful implementation of AI systems in financial institutions, allowing them to leverage advanced technologies to identify and prevent cyber-enabled financial crimes such as money laundering. This synergy between the *Cybercrimes Act* and the use of AI reinforces the regulatory environment, fostering a proactive approach to addressing emerging threats at the intersection of cybersecurity and financial crime prevention in South Africa. It is key to note that the *Cybercrimes Act* does not expressly provide for the use of AI to combat money laundering.

7.2 Electronic Communications and Transactions Act 25 of 2002

After years of legal ambiguity regarding the regulation of cybercrime, the enactment of the *Electronic Communications and Transactions Act* (*ECTA*) represents a crucial step towards combatting cybercrimes such as money laundering. The *ECTA* stands as the first legislative statute directly addressing cybercrime in South Africa.[134] While it refrains from explicitly defining "cybercrime", it provides a comprehensive definition of "access", covering actions where individuals, upon noticing data, are aware of their lacking authorisation yet persist in accessing it.[135] This statute prohibits unauthorised access to, interception of or interference with data.[136] Importantly, these provisions not only establish a foundation for addressing cyber-related offences but also create an environment which is supportive of leveraging AI in AML measures in South Africa. AI has analytical capabilities and it can detect patterns in extensive datasets, making it instrumental in identifying instances of unauthorised data access, interception or interference, which aligns with the objectives of the *ECTA*. Furthermore, the *Cybercrimes Act*'s prohibition of producing, selling or possessing devices or computer programmes which are designed to bypass data protection security measures is particularly relevant to ensuring secure AI implementation in combatting cyber-related offences. Additionally, the *ECTA* expressly addresses computer-related extortion, fraud and forgery, providing a legal foundation to combat cybercrimes.[137] The *Cybercrime Act*'s provisions encompass individuals attempting to commit cybercrimes, reinforcing the legal framework's efficacy in addressing evolving threats in the digital landscape. However, the *ECTA* does not expressly provide for the use of AI to detect and combat money laundering.

---

134 Section 1 read with ss 10-89 of the Electronic Communications and Transaction Act 25 of 2002 (*ECTA*).

135 Section 1 read with ss 10-89 of the *ECTA*.

136 Section 1 read with ss 10-89 of the *ECTA*.

137 Section 1 read with ss 10-89 of the *ECTA*.

7.3 ICASA and the Regulation of AI

The Independent Communications Authority of South Africa (ICASA) functions as an autonomous regulatory body which oversees the communications, broadcasting, and postal services sectors in the country.[138] It was established in 2000 through the *ICASA Act*. Its primary mandate is to regulate the telecommunications and broadcasting sectors in the public interest.[139] This role was assumed from the Independent Broadcasting Authority and the South African Telecommunications Regulatory Authority, a merger driven by the imperative to adapt to the rapid technological advancements occurring globally. ICASA is authorised to issue licences, monitor licensee compliance, and formulate regulations for consumer protection in terms of the *Public Finance Management Act*,[140] the *ECTA*, the *Postal Services Act* 24 of 1998,[141] the *Broadcasting Act* 4 of 1999 and the *ICASA Act*. However, the ICASA and the *ICASA Act* do not specifically provide for the use of AI measures to detect, investigate, prevent and curb money laundering in South African banks and other financial institutions.

7.4 The POCA and the FICA

Although both the *POCA* and the *FICA* have some provisions that outlaw money laundering activities, they do not expressly provide for the use of AI measures to curb such activities. Thus, the *POCA* and the *FICA* do not require banks, financial institutions, enforcement authorities and other role-players to employ AI measures to combat money laundering activities in the South African banking sector.

8 Concluding remarks

The challenges to implementing AI technologies for AML processes in the South African banking sector underline the need for the adoption of a comprehensive and adaptable AI-powered outcomes-based approach to combatting money laundering. Despite its technological limitations, regulatory uncertainties and ethical considerations, there is a promising trajectory which is driven by potential positive shifts in both technology and AML regulatory framework in South Africa. Advancements in AI technologies, including the development of more sophisticated algorithms and enhanced machine learning models, hold the promise of improved capabilities in detecting intricate money laundering schemes and other illicit financial activities in South Africa. In this regard, the relevant regulatory

138 *Independent Communications Authority of South Africa Act* 13 of 2000, as amended (*ICASA Act*) ss 3 and 4.

139 See ss 3 and 4 of the *ICASA Act*.

140 *Public Finance Management Act* 1 of 1999.

141 *Postal Services Act* 24 of 1998.

bodies should be statutorily obliged to incorporate AI measures into their AML measures. Such measures should be clear and adequate. Moreover, regulators, financial institutions and technology experts should be statutorily obliged to collaborate and develop appropriate measures to curb money laundering in the South African banking sector. Banks and regulatory bodies should embrace and leverage AI technologies to combat money laundering and other financial crimes. The relevant AML statutes, such as the *POCA* and the *FICA*, should be carefully amended to oblige banks, financial institutions and other enforcement authorities to utilise AI measures to detect and curb financial crimes such as money laundering and fraud. Severe penalties should be imposed on all the perpetrators of money laundering and related financial crimes. Lastly, a robust and AI-AML integrated system that adapts to emerging threats and technological advancements should be adopted to safeguard the integrity of the South African financial sector against money laundering and related financial crimes.

Bibliography

Literature

Agarwal and Dhar 2014 *Information Systems Research*
Agarwal R and Dhar V "Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research" 2014 *Information Systems Research* 443-448

Alaimo and Kallinikos 2017 *Information Society*
Alaimo C and Kallinikos J "Computing the Everyday: Social Media as Data Platforms" 2017 *Information Society* 175-191

Alhajeri and Alhashem 2023 *Intelligent Information Management*
Alhajeri R and Alhashem A "Using Artificial Intelligence to Combat Money Laundering" 2023 *Intelligent Information Management* 284-305

Allam and Dhunny 2019 *Cities*
Allam Z and Dhunny ZA "On Big Data, Artificial Intelligence and Smart Cities" 2019 *Cities* 80-91

Ball *et al Private Security State?*
Ball K *et al The Private Security State? Surveillance, Consumer Data and the War on Terror* (Copenhagen Business School Press Copenhagen 2015)

Bara and Le Roux 2017 *Journal of Economic and International Law*
Bara A and Le Roux P "International Financial Centres, Global Finance and Financial Development in the Southern Africa Development Community (SADC)" 2017 *Journal of Economic and International Finance* 68-79

Basdeo 2013 *AJICL*
Basdeo V "The Legal Challenges of Criminal and Civil Asset Forfeiture in South Africa: A Comparative Analysis" 2013 *AJICL* 303-326

Bhatore, Mohan and Reddy 2020 *Journal of Banking and Financial Technology*
Bhatore S, Mohan L and Reddy YR "Machine Learning Techniques for Credit Risk Evaluation: A Systematic Literature Review" 2020 *Journal of Banking and Financial Technology* 111-138

Boles 2015 *Am Bus L J*
Boles JR "Financial Sector Executives as Targets for Money Laundering Liability" 2015 *Am Bus L J* 365-433

Byrne 2011 *Journal of Business Ethics*
Byrne EF "Business Ethics Should Study Illicit Businesses: To Advance Respect for Human Rights" 2011 *Journal of Business Ethics* 497-509

Calvard 2016 *Management Learning*
Calvard TS "Big Data, Organizational Learning, and Sensemaking: Theorizing Interpretive Challenges under Conditions of Dynamic Complexity" 2016 *Management Learning* 65-82

Canhoto 2021 *Journal of Business Research*
Canhoto AI "Leveraging Machine Learning in the Global Fight against Money Laundering and Terrorism Financing: An Affordances Perspective" 2021 *Journal of Business Research* 441-452

Canhoto *et al* 2017 *Journal of Strategic Marketing*
Canhoto AI *et al* "The Role of Customer Management Capabilities in Public-Private Partnerships" 2017 *Journal of Strategic Marketing* 384-404

Carlsen and Bruggemann 2022 *International Journal of Sustainable Development and World Ecology*
Carlsen L and Bruggemann R "The 17 United Nations' Sustainable Development Goals: A Status by 2020" 2022 *International Journal of Sustainable Development and World Ecology* 219-229

Chen 2020 *Applied Soft Computing*
Chen TH "Do You Know Your Customer? Bank Risk Assessment Based on Machine Learning" 2020 *Applied Soft Computing* 1-7

Chitimira 2021 *JMLC*
Chitimira H "An Exploration of the Current Regulatory Aspects of Money Laundering in South Africa" 2021 *JMLC* 789-805

Constantiou and Kallinikos 2015 *Journal of Information Technology*
Constantiou ID and Kallinikos J "New Games, New Rules: Big Data and the Changing Context of Strategy" 2015 *Journal of Information Technology* 44-57

D'Amico *et al* 2020 *Sensors*
D'Amico G *et al* "Understanding Sensor Cities: Insights from Technology Giant Company Driven Smart Urbanism Practices" 2020 *Sensors* 1-24

De Koker 2003 *JMLC*
De Koker L "Money Laundering Trends in South Africa" 2003 *JMLC* 27-41

De Koker 2004 *TSAR*
De Koker L "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 715-746

Enholm *et al* 2022 *Information Systems Frontiers*
Enholm IM *et al* "Artificial Intelligence and Business Value: A Literature Review" 2022 *Information Systems Frontiers* 1709-1734

Ennis 2002 *Law and Business Review of the Americas*
Ennis J "Cleaning up the Beaches: The Caribbean Response to the FATF's Review to Identify Non-Cooperative Countries of Territories" 2002 *Law and Business Review of the Americas* 637-665

Ferrara *et al* 2016 *Communications of the ACM*
Ferrara E *et al* "The Rise of Social Bots" 2016 *Communications of the ACM* 96-104

Gates and Jacob 2009 *Economic Perspectives*
Gates T and Jacob K "Payment's Fraud: Perception Versus Reality — A Conference Summary" 2009 *Economic Perspectives* 7-15

Gaviyau and Sibindi 2023 *JMLC*
Gaviyau W and Sibindi AB "Anti-Money Laundering and Customer Due Diligence: Empirical Evidence from South Africa" 2023 *JMLC* 224-238

Gaviyau and Sibindi 2023 *Journal of Risk and Financial Management*
Gaviyau W and Sibindi AB "Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique" 2023 *Journal of Risk and Financial Management* 1-21

Goecks *et al* 2022 *Intelligent Systems in Accounting, Finance and Management*
Goecks LS *et al* "Anti-Money Laundering and Financial Fraud Detection: A Systematic Literature Review" 2022 *Intelligent Systems in Accounting, Finance and Management* 71-85

Goetz and Jenkins 2016 *Gender and Development*
Goetz AM and Jenkins R "Gender, Security, and Governance: The Case of Sustainable Development Goal 16" 2016 *Gender and Development* 127-137

Goodall 2016 *Applied Artificial Intelligence*
Goodall NJ "Away from Trolley Problems and toward Risk Management" 2016 *Applied Artificial Intelligence* 810-821

Goredema 2007 *ISS Monograph Series*
Goredema C "Confronting Money Laundering in South Africa: An Overview of Challenges and Milestones" 2007 *Confronting the Proceeds of Crime in Southern Africa: An Introspection. ISS Monograph Series* 73-92

Hamman *Impact of Anti-Money Laundering Legislation*
Hamman AJ *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* (LLD/PhD-thesis University of the Western Cape 2015)

Han *et al* 2020 *Digital Finance*
Han J *et al* "Artificial Intelligence for Anti-Money Laundering: A Review and Extension" 2020 *Digital Finance* 211-239

Huang and Rust 2018 *Journal of Service Research*
Huang MH and Rust RT "Artificial Intelligence in Service" 2018 *Journal of Service Research* 155-172

Huang *et al* 2021 *ACM Computing Surveys*
Huang H *et al* "A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools" 2021 *ACM Computing Surveys* 1-42

Jana *Comparative Statutory Analysis*
Jana VLM *A Comparative Statutory Analysis of the Regulation of Money Laundering in Zimbabwe* (LLD-thesis North-West University 2024)

Johari *et al* "Money Laundering"
Johari RJ *et al* "Money Laundering: Customer Due Diligence in the Era of Cryptocurrencies" Paper presented at the *1st International Conference on Accounting, Management and Entrepreneurship* (2020) 130-135

Kersop and Du Toit 2015 *PELJ*
Kersop M and Du Toit SF "Anti-Money Regulations and the Effective Use of Mobile Money in South Africa - Part 1" 2015 *PELJ* 1603-1636

Kietzmann, Paschen and Treen 2018 *Journal of Advertising Research*
Kietzmann J, Paschen J and Treen E "Artificial Intelligence in Advertising: How Marketers Can Leverage Artificial Intelligence along the Consumer Journey" 2018 *Journal of Advertising Research* 263-267

Khumalo 2023 *African Security Review*
Khumalo K "The Problem with the Removal of the Motive Requirement from the Offence of Terrorism-A Short Commentary" 2023 *African Security Review* 1-5

Kute *et al* 2021 *IEEE Access*
Kute DV *et al* "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering: A Critical Review" 2021 *IEEE Access* 82300-82317

Labib, Rizka and Shokry "Survey of Machine Learning"
Labib NM, Rizka MA and Shokry AEM "Survey of Machine Learning Approaches of Anti-Money Laundering Techniques to Counter Terrorism Finance" in *Internet of Things—Applications and Future: Proceedings of ITAF 2019 Singapore* (Springer Singapore 2020) 73-87

Marakalala and Mokwena 2023 *International Journal of Social Science Research and Review*
Marakalala MC and Mokwena RJ "Forensic Investigation: The Impact of Money-Laundering during Lockdown in South Africa" 2023 *International Journal of Social Science Research and Review* 523-532

Menon and Guan Siew 2012 *JMLC*
Menon S and Guan Siew T "Key Challenges in Tackling Economic and Cyber Crimes: Creating a Multilateral Platform for International Co-operation" 2012 *JMLC* 243-256

Mirsky *et al* 2023 *Computers and Security*
Mirsky Y *et al* "The Threat of Offensive AI to Organizations" 2023 *Computers and Security* https://doi.org/10.1016/j.cose.2022.103006

Mittelstadt *et al* 2016 *Big Data & Society*
Mittelstadt BD *et al* "The Ethics of Algorithms: Mapping the Debate" 2016 *Big Data & Society* https://doi.org/10.1177/2053951716679679

Ncube *et al* "Setting out the Challenges"
Ncube CB *et al* "Setting out the Challenges and Opportunities of Artificial Intelligence for Africa" in Ncube CB *et al Artificial Intelligence and the Law in Africa* (LexisNexis Durban 2023) 1-20

Nizovtsev *et al* 2022 *JMLC*
Nizovtsev YY *et al* "Mechanisms of Money Laundering Obtained from Cybercrime: The Legal Aspect" 2022 *JMLC* 297-305

Njontini 2021 *De Jure*
Njontini MN "Disruptive Technologies and the Future of Regulations: ICT Regulatory Structure(s) Determined" 2021 *De Jure* 174-193

Paschen, Pitt and Kietzmann 2020 *Business Horizons*
Paschen U, Pitt C and Kietzmann J "Artificial Intelligence: Building Blocks and an Innovation Typology" 2021 *Business Horizons* 147-155

Pavlidis 2023 *JMLC*
Pavlidis G "Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era" 2023 *JMLC* 156-166

Roach 2005 *SACJ*
Roach K "A Comparison of South African and Canadian Anti-Terrorism Legislation" 2005 *SACJ* 127-150

Russell *Artificial Intelligence*
Russell SJ *Artificial Intelligence: A Modern Approach* (Pearson Education Inc Harlow 2010)

Saha, Bose and Mahanti 2016 *Decision Support Systems*
Saha P, Bose I and Mahanti A "A Knowledge-based Scheme for Risk Assessment in Loan Processing by Banks" 2016 *Decision Support Systems* 78-88

Schlenther 2013 *JMLC*
Schlenther B "The Taxing Business of Money Laundering: South Africa" 2013 *JMLC* 126-141

Schlenther 2014 *JMLC*
Schlenther B "Is the South African Effort toward Reducing Money Laundering Optimal?" 2014 *JMLC* 17-33

Silver *et al* 2017 *Nature*
Silver D *et al* "Mastering the Game of Go without Human Knowledge" 2017 *Nature* 354-359

Skiena *Algorithm Design Manual*
Skiena SS *The Algorithm Design Manual* (Springer New York 1998)

Sultzer 1995 *Tenn L Rev*
Sultzer S "Money Laundering: The Scope of the Problem and Attempts to Combat It" 1995 *Tenn L Rev* 143-238

Truskauskas and Taujanskaite 2022 *Business and Management*
Truskauskas G and Taujanskaitė K "Efficiency of Anti-Money Laundering: The Case of Northern European Countries" 2022 *Business and Management* 430-440

Tuba 2012 *Acta Criminologica*
Tuba MD "Prosecuting Money Laundering the FATF Way: An Analysis of Gaps and Challenges in South African Legislation from a Comparative

Perspective" 2012 *Acta Criminologica: African Journal of Criminology and Victimology* 103-122

Van Jaarsveld *Aspects of Money Laundering*
Van Jaarsveld IL *Aspects of Money Laundering in South African Law* (LLD/PhD-thesis University of South Africa 2011)

Whisker and Lokanan 2019 *JMLC*
Whisker J and Lokanan ME "Anti-Money Laundering and Counter-Terrorist Financing Threats Posed by Mobile Money" 2019 *JMLC* 158-172

Xu *et al* 2021 *Journal of Forensic and Investigative Accounting*
Xu C *et al* "How Can a Blockchain-based Anti-Money Laundering System Improve Customer Due Diligence Process?" 2021 *Journal of Forensic and Investigative Accounting* 273-287

Životić, Ristić and Mirković 2022 *Oditor*
Životić I, Ristić K and Mirković Z "The Impact of Security Management in the Detection of Money Laundering with Consequences on the Economy" 2022 *Oditor* 91-108

Legislation

Broadcasting Act 4 of 1999

Cybercrimes Act 19 of 2020

Electronic Communications and Transaction Act 25 of 2002

Financial Intelligence Centre Act 38 of 2001

General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022

Independent Communications Authority of South Africa Act 13 of 2000

Postal Services Act 24 of 1998

Prevention of Organised Crime Act 121 of 1998

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Public Finance Management Act 1 of 1999

Internet sources

Bellomarini, Laurenza and Sallinger 2020 http://hdl.handle.net/20.500.12708/58323
Bellomarini L, Laurenza E and Sallinger E 2020 *Rule-based Anti-Money Laundering in Financial Intelligence Units: Experience and Vision* http://hdl.handle.net/20.500.12708/58323 accessed 25 October 2023

Brundage *et al* 2018 https://arxiv.org/pdf/1802.07228
Brundage M *et al* 2018 *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* https://arxiv.org/pdf/1802.07228 accessed 4 July 2024

FATF 2006 https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html
Financial Action Task Force 2006 *Trade-Based Money Laundering* https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html accessed 20 October 2023

FATF 2018 https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf
Financial Action Task Force 2018 *Financial Flows from Human Trafficking* https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf accessed 5 June 2024

FATF 2021 https://www.fatf-gafi.org/en/publications/Digital transformation/Opportunities-challenges-new-technologies-for-aml-cft.html
Financial Action Task Force 2021 *Opportunities and Challenges of New Technologies for AML/CFT* https://www.fatf-gafi.org/en/publications/Digital transformation/Opportunities-challenges-new-technologies-for-aml-cft.html accessed 13 October 2023

Financial Institutions Examination Council 2014 https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf
Financial Institutions Examination Council 2014 *Bank Secrecy Act/Antimoney Laundering Examination Manual* https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf accessed 20 October 2023

Han *et al* 2021 https://doras.dcu.ie/23358/
Han J *et al* 2021 *NextGen AML: Distributed Deep Learning-based Language Technologies to Augment Anti Money Laundering Investigation* https://doras.dcu.ie/23358/ accessed 20 October 2023

Hudson 2017 https://fivethirtyeight.com/features/technology-is-biased-too-how-do-we-fix-it/
Hudson L 2017 *Technology is Biased Too. How Do We Fix It?* https://fivethirtyeight.com/features/technology-is-biased-too-how-do-we-fix-it/ accessed 20 October 2023

Jacob and Summers 2008 https://www.chicagofed.org/publications/chicago-fed-letter/2008/july-252
Jacob K and Summers BJ 2008 *Assessing the Landscape of Payments Fraud* https://www.chicagofed.org/publications/chicago-fed-letter/2008/july-252 accessed 19 October 2023

Jensen 1997 https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf
Jensen D 1997 *Prospective Assessment of AI Technologies for Fraud Detection: A Case Study* https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf accessed 4 July 2024

Khan *et al* 2020 https://www.digitalistmag.com/executive-research/algorithms-the-new-means-of-production
Khan I *et al* 2020 *Algorithms: The New Means of Production* https://www.digitalistmag.com/executive-research/algorithms-the-new-means-of-production accessed 30 October 2023

Lewis *et al* 2017 https://engineering.fb.com/2017/06/14/ml-applications/deal-or-no-deal-training-ai-bots-to-negotiate/
Lewis M *et al* 2017 *Deal or No Deal? Training AI Bots to Negotiate* https://engineering.fb.com/2017/06/14/ml-applications/deal-or-no-deal-training-ai-bots-to-negotiate/ accessed 23 October 2023

Mckinsey and Company 2022 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer
Mckinsey and Company 2022 *The Fight against Money Laundering: Machine Learning is a Game Changer* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer accessed 23 October 2023

Mnih *et al* 2013 https://arxiv.org/pdf/1312.5602.pdf
Mnih V *et al* 2013 *Playing Atari with Deep Reinforcement Learning* https://arxiv.org/pdf/1312.5602.pdf accessed 21 October 2023

Moonstone Information Refinery 2022 https://www.moonstone.co.za/did-grey-listing-threat-hasten-sarb-to-act-against-markus-jooste/
Moonstone Information Refinery 2022 *Did Grey-Listing Threat Hasten SARB to Act against Markus Jooste?* https://www.moonstone.co.za/did-grey-listing-threat-hasten-sarb-to-act-against-markus-jooste/ accessed 22 April 2023

National Treasury 2023 https://www.treasury.gov.za/comm_media/press/2023/2023010601%20MEDIA%20STATEMENT-ENACTMENT%20OF%20KEY%20ANTI-MONEY%20LAUNDERING%20AND%20COMBATING%20OF%20TERROR%20FINANCING%20LAWS%20.pdf
National Treasury 2023 *Media Statement: Enactment of Key Anti-Money Laundering and Combating of Terror Financing Laws* https://www.treasury.gov.za/comm_media/press/2023/2023010601%20MEDIA%20STATEMENT-ENACTMENT%20OF%20KEY%20ANTI-

MONEY%20LAUNDERING%20AND%20COMBATING%20OF%20TERROR%20FINANCING%20LAWS%20.pdf accessed 5 June 2024

O'Hear 2016 https://techcrunch.com/2017/01/16/fraugster/
O'Hear S 2016 *Fraugster: A Startup that Uses AI to Detect Payment Fraud, Raises $5m* https://techcrunch.com/2017/01/16/fraugster/ accessed 19 October 2023

Oseni *et al* 2021 https://arxiv.org/pdf/2102.04661
Oseni A *et al* 2021 *Security and Privacy for Artificial Intelligence: Opportunities and Challenges* https://arxiv.org/pdf/2102.04661 accessed 4 July 2024

Raweh, Cao and Shihadeh 2017 https://scholar.ptuk.edu.ps/handle/123456789/639
Raweh B, Cao E and Shihadeh F 2017 *Review the Literature and Theories on Anti-Money Laundering* https://scholar.ptuk.edu.ps/handle/123456789/639 accessed 20 October 2023

Sanction Scanner date unknown https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494
Sanction Scanner date unknown *What is Cyber-laundering?* https://sanctionscanner.com/blog/cyber-laundering-and-cyberterrorism-494 accessed 5 June 2024

Stervinou 2015 https://www.kansascityfed.org/Payments%20Conferences/documents/7490/PSCP2015_StervinouPaper.pdf
Stervinou A 2015 *Monitoring Payment Fraud: A Key Piece to the Puzzle* https://www.kansascityfed.org/Payments%20Conferences/documents/7490/PSCP2015_StervinouPaper.pdf accessed 19 October 2023

UN Department of Economic and Social Affairs date unknown https://sdgs.un.org/goals
United Nations Department of Economic and Social Affairs date unknown *Sustainable Development: The 17 Goals* https://sdgs.un.org/goals accessed 5 June 2024

UNODC 2016 https://www.unodc.org/unodc/en/moneylaundering/introduction.html?ref=menuside
United Nations Office on Drugs and Crime 2016 *Introduction to Money-Laundering*
https://www.unodc.org/unodc/en/moneylaundering/introduction.html?ref=menuside accessed 14 October 2023

List of Abbreviations

AI	artificial intelligence
AJICL	African Journal of International and Comparative Law
Am Bus L J	American Business Law Journal
AML	anti-money laundering
CDD	Client Due Diligence
ECTA	Electronic Communications and Transaction Act 25 of 2002
FATF	Financial Action Task Force
FICA	Financial Intelligence Centre Act 38 of 2001
ICASA	Independent Communications Authority of South Africa
ICASA Act	Independent Communications Authority of South Africa Act 13 of 2000
JMLC	Journal of Money Laundering Control
KYC	Know Your Client
PELJ	Potchefstroom Electronic Law Journal
POCA	Prevention of Organised Crime Act 121 of 1998
SACJ	South African Journal of Criminal Justice
SDGs	Sustainable Development Goals
Tenn L Rev	Tennessee Law Review
TSAR	Tydskrif vir die Suid-Afrikaanse Reg
UN	United Nations
UNODC	United Nations Office on Drugs and Crime